UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO DE INTEGRACIÓN CURRICULAR

previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

“Ingeniería social en una institución de educación superior aplicando técnicas computacionales y no computacionales”

AUTOR

Peñafiel Suárez Marcelo Rodrigo

PROFESOR TUTOR

Ing. Lídice Haz López, Msi.

LA LIBERTAD – ECUADOR

PAO: 2022-1

APROBACIÓN DEL TUTOR

En mi calidad de tutora del trabajo de titulación denominado: **"Ingeniería social en una institución de educación superior aplicando técnicas computacionales y no computacionales"**, elaborado por el Sr. Peñafiel Suárez Marcelo Rodrigo, de la carrera de Tecnología de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

La Libertad, 03 de agosto del 2022

Ing. Lídice Haz López, Msi.

DECLARACIÓN

El contenido del presente componente práctico del trabajo de titulación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

_____

Peñafiel Suárez Marcelo Rodrigo

AGRADECIMIENTO

Agradezco a mis padres, por acompañarme siempre durante este proceso educativo, brindándome su apoyo emocional, convirtiéndose en mi inspiración para poder culminar mi carrera universitaria.

Expreso mi agradecimiento a todas las autoridades de la institución donde realicé mi proyecto, a los docentes que en este camino de aprendizaje han compartido conmigo sus conocimientos adquiridos. A mi docente tutor y así mismo a mi docente de integración curricular, gracias por su supervisión, dedicatoria, y paciencia, fueron parte fundamental para el desarrollo de este proyecto.

Marcelo Rodrigo Peñafiel Suárez

DEDICATORIA

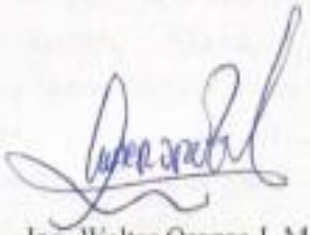
A mi familia, amigos, a todas las personas que creyeron en mí y me brindaron su apoyo fundamental durante este proceso educativo. sobre todo, a mis padres por ser mi inspiración e inculcarme valores para ser una mejor persona cada día.

Marcelo Rodrigo Peñafiel Suárez

TRIBUNAL DE GRADO

Ing. Jaime Orozco, Mgt

DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN



Ing. Walter Orozco I, Mgt

DOCENTE ESPECIALISTA

Ing. Lidia Haz López, Msi

DOCENTE TUTOR

Ing. Marjorie Coronel, MgT

DOCENTE GUÍA UIC

RESUMEN

La ingeniería social es una de las técnicas más utilizadas por cibercriminales, la cual busca atacar a las personas que pertenecen a una institución respectivamente, manipulando a la misma mediante habilidades sociales y técnicas psicológicas, con la finalidad de cumplir un objetivo malicioso. Este método aparece frecuentemente como un correo electrónico o un mensaje de texto que a simple vista parece inofensivo, pero que tiene por debajo un ataque cibernético.

Debido a la pandemia del covid19, las instituciones públicas y privadas, optaron por utilizar herramientas tecnológicas de manera fundamental, ya que, era una necesidad para poder desempeñar las actividades que realizaban en su lugar de trabajo de manera presencial, esto se volvió algo habitual, tanto así que el uso de plataformas informáticas aumentó considerablemente. Teniendo en cuenta esto, nos debemos preocupar de la seguridad que recibe la información que posee y como está siendo tratada. De este modo, dichas herramientas digitales son un blanco fácil para los ciberdelincuentes, que tienen mayor acceso a robar datos importantes y vulnerarlos con fines maliciosos.

Por esta razón, el presente proyecto propone determinar las posibles vulnerabilidades a través de la recopilación de información, mediante ingeniería social, empleando técnicas computacionales y no computacionales en una institución de educación superior de la provincia de Santa Elena, con el objetivo de generar un informe acerca de los datos encontrados y complementando con una guía de buenas prácticas para las personas de dicha entidad.

La metodología de investigación empleada para elaborar el presente informe es de tipo exploratoria y diagnóstica, las cuales ayudaron a recolectar información acerca de la institución de educación superior, realizando una encuesta a los estudiantes y docentes de la entidad. Así mismo, se utilizó una metodología genérica, adaptada con el fin de identificar las vulnerabilidades mediante ataques de ingeniería social, que se divide en las fases: identificación y selección de técnicas de ingeniería social, implementación de técnicas de ingeniería social, análisis de resultados e informe de resultados.

Finalmente, se realizaron los ataques de ingeniería social, teniendo éxito y mostrando las vulnerabilidades encontradas en dicha institución, así mismo, se planteó una guía de buenas prácticas, que será de gran ayuda para las personas que desconocen del tema.

ABSTRACT

Social engineering is one of the techniques most commonly used by cybercriminals, which seeks to attack people belonging to an institution respectively, manipulating them through social skills and psychological techniques, in order to fulfill a malicious objective. This method often appears as an email or text message that at first glance seems harmless, but has a cyber-attack underneath.

Due to the covid19 pandemic, public and private institutions opted to use technological tools in a fundamental way, since it was a necessity to be able to carry out the activities they performed in their workplace in person, this became commonplace, so much so that the use of computer platforms increased considerably. Taking this into account, we must be concerned about the security of the information you have and how it is being treated. In this way, such digital tools are an easy target for cybercriminals, who have greater access to steal important data and violate them for malicious purposes.

For this reason, this project proposes to determine the possible vulnerabilities through the collection of information, through social engineering, using computational and non-computational techniques in an institution of higher education in the province of Santa Elena, with the aim of generating a report about the data found and complementing it with a guide of good practices for the people of that entity.

The research methodology used to prepare this report is exploratory and diagnostic, which helped to collect information about the higher education institution, conducting a survey of students and teachers of the entity. Likewise, a generic methodology was used, adapted in order to identify vulnerabilities through social engineering attacks, which is divided into the following phases: identification and selection of social engineering techniques, implementation of social engineering techniques, analysis of results and report of results.

Finally, the social engineering attacks were carried out, being successful and showing the vulnerabilities found in this institution, likewise, a guide of good practices was proposed, which will be of great help for people who are not familiar with the subject.

TABLA DE CONTENIDO

ÍNDICE DE FIGURA

ÍNDICE DE TABLA

LISTA DE ANEXOS

INTRODUCCIÓN

En Ecuador, muchas entidades públicas y privadas han sido víctimas de ataques informáticos y robo de datos, dichos casos no han sido denunciados ni reportados, porque pierden credibilidad como empresa, por ende, no son muy conocidos como crímenes cibernéticos en el país. Así mismo, son pocas las instituciones que revelan haber sufrido pérdidas de información, perdiendo prestigio con los clientes en base a la protección de datos que brindan como entidad.

En la actualidad, las instituciones manejan espacios grandes de almacenamiento digital, recopilando toda la información importante allí, incluyendo datos personales, estados financieros, lista de los clientes, entre otros. Llamando la atención de cibercriminales malintencionados, buscando instituciones con el propósito de recolectar datos sensibles y utilizarlos de forma fraudulenta. Cualquier entidad puede ser un blanco de ataque hoy en día, ya que los hackers utilizan un conjunto de técnicas que les permiten usurpar la información.

Es por esto, que se propone determinar las posibles vulnerabilidades mediante la recopilación de información a través de ingeniería social utilizando métodos computacionales y no computacionales en una institución de educación superior de la provincia de Santa Elena, con el fin de generar un informe con respecto a los datos encontrados y complementando con una guía de buenas prácticas para las personas de dicha entidad.

Las fases que se utilizarán en el presente proyecto son: Identificación y selección de técnicas de ingeniería social, implementación de técnicas de ingeniería social, análisis de resultados e informe de resultados.

Para la determinación de requerimientos se utilizaron las metodologías de investigación diagnóstica y exploratoria, haciendo una revisión de trabajos similares al presente proyecto y realizando una encuesta a los docentes y estudiantes de la institución antes mencionada. Así mismo, se utiliza una metodología adaptada, con el fin de identificar vulnerabilidades a través de ataques de ingeniería social.

Se emplearon herramientas de código libre para el desarrollo del proyecto, tales como: Kali Linux y Social Engineering Toolkit, permitiendo crear los ataques de ingeniería social, que serán enviados a las personas de la institución.

Los vectores de ataque empleados en el presente trabajo se dividen en computacionales y no computacionales, siendo estos:

- Website attack Vectors
- Infectious media Generator
- QRCode Generator attack vector
- Shoulder surfing
- Vishing.

Después de realizar correctamente todos los ataques descritos anteriormente, se analizaron las vulnerabilidades encontradas y se elaboró una guía de buenas prácticas que ayudará en gran medida a la institución.

Este trabajo, está estructurado como se detalla a continuación:

El capítulo I, contiene los antecedentes, descripción del proyecto, objetivos, justificación y metodología del proyecto.

Así mismo, el capítulo II está conformado por el marco contextual, marco conceptual, marco teórico y componentes de la propuesta.

Finalmente, el capítulo III, abarca la propuesta, los resultados de la encuesta con cuadros estadísticos, la metodología de ataques de ingeniería social, identificación de técnicas de ingeniería social computacionales y no computacionales, implementación de técnicas de ingeniería social, análisis de resultados, conclusiones y recomendaciones.

1. FUNDAMENTACIÓN

1.1 ANTECEDENTES

En la actualidad las instituciones manejan espacios de almacenamiento digital, donde recopilan información relevante, donde pueden incluir datos personales, estados financieros, lista clientes, entre otros [1]. Esto llama la atención de entes mal intencionados, los mismos que pueden ser competidores dentro del mercado, o los conocidos ciberdelincuentes informáticos, que recolectan y utilizan datos sensibles para extorsionar, robar información, manipular, entre otros crímenes, que afectan al desarrollo de la organización [1]. Los hackers utilizan un conjunto de técnicas que les permiten usurpar la información [1].

La ingeniería social es uno de los métodos más utilizados por cibercriminales, la cual se enfoca en atacar a las personas que pertenecen a una entidad, manipulando a la misma a través de habilidades sociales y técnicas psicológicas con el fin de cumplir un objetivo malicioso [2]. Esta técnica frecuentemente aparece como un mensaje de texto, de correo electrónico o de voz de una fuente que parece inofensiva a simple vista, pero por debajo contiene un tipo de ataque cibernético [2].

Entre los ataques más conocidos está el phishing, que se lleva a cabo mediante el correo electrónico, donde persuade a la víctima a ingresar al enlace insertado en el mensaje para que revele sus datos personales o financieros [3]. Así mismo, existen otras técnicas como instalar software malicioso o malware de forma inadvertida en los dispositivos electrónicos; utilizar un keylogger que captura las contraseñas que introducen los usuarios, o emplear prácticas como la personificación, la cual asume la identidad de otra persona con el fin de obtener información confidencial [3].

En el año 2016 la compañía de seguridad informática ESET informó que 49% de los ataques son dirigidos a instituciones pequeñas y un 30% a instituciones grandes o medianas, pero el sector que presenta más vulnerabilidades es el sector público, debido que no realizan estudios para identificar los riesgos y por lo tanto no se puede tomar medidas preventivas de ciberseguridad [4] [Anexo1].

En Ecuador, muchas instituciones han sido víctimas de ataques informáticos y robo de información, pero son casos que no han sido denunciados o reportados, ya que pierden prestigio como entidad, por lo tanto, no son conocidos muchos de los crímenes cibernéticos que ha habido en el país y son pocas las instituciones que revelan, puesto que

han sufrido pérdidas de clientes debido a la baja credibilidad de protección de datos que poseen, por lo que las personas ya no confían en seguir con la institución [5].

En el país, un 43% de los ciudadanos tiene acceso a internet, sin embargo, la mayoría de estos, no conocen temas de vulnerabilidades informáticas o medidas que deben tomar para disminuir el riesgo de infección por algún tipo de malware [6], esto se debe al bajo nivel de educación informática [Anexo2], elevando la posibilidad de ser víctimas de estos delincuentes, por otro lado, las políticas y normas de seguridad no se cumplen de forma rigurosa.

Diversas instituciones son víctimas de ciberataques, según el estudio realizado por ITRC Data Breach Reports el 23,7% son ataques realizados al sector de la salud, un 8,0% a la educación e instituciones gubernamentales presentan un 4,7% [6].

A nivel mundial en el periodo 2018-2019 se registró un aumento del 33% en ataques informáticos tipo phishing [7]. En el año 2020 entre los meses de enero a septiembre se registraron 1.3 millones de intentos de ataques con ransomware [Anexo3]. Los atacantes aprovechan las vulnerabilidades del sistema, contraseñas débiles, softwares no actualizados o programas crackeados para realizar la infección [8].

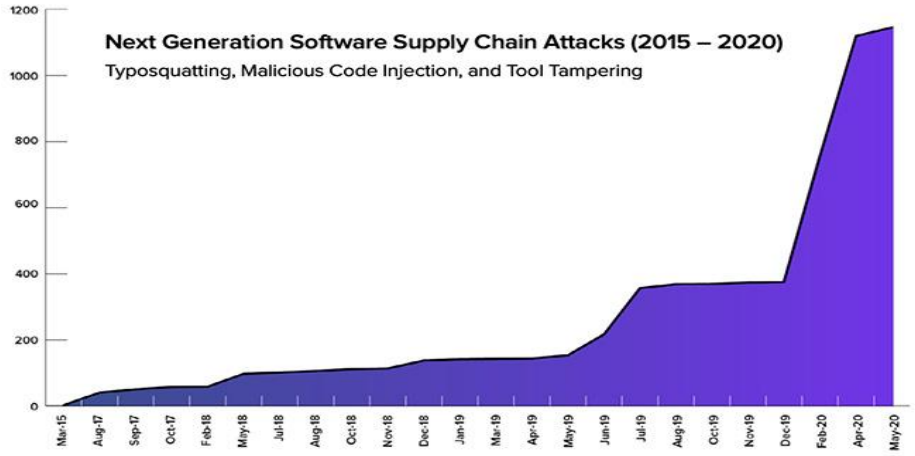


Figura 1. Aumento de ataques informáticos entre el año 2015-2020

Debido a la pandemia del covid19 en el mundo las empresas, instituciones públicas y privadas, personas se vieron obligados a utilizar herramientas tecnológicas de forma esencial para desempeñar las actividades que realizaban en su lugar de trabajo, esto se volvió habitual e indispensable, tanto así que el uso de plataformas informáticas aumentó del 70% a 300% [8]. No obstante, nos deberíamos de preocupar de la seguridad que recibe nuestra información y como está siendo tratada [Anexo4].

Del mismo modo, con la virtualidad durante la pandemia, se trabajó con herramientas digitales de aprendizaje remoto, donde los ciberdelincuentes tenían mayor acceso a robar datos importantes y vulnerarlos con fines maliciosos [8]. Si comparamos el ambiente de funcionamiento de una institución educativa con una financiera, no tiene los mismos niveles de seguridad que se requieren para administrar la información, siendo un blanco fácil para cibercriminales y dejando a un lado la protección de los datos [8].

El presente trabajo propone determinar las posibles vulnerabilidades mediante la recopilación de información a través de ingeniería social utilizando técnicas computacionales y no computacionales en una institución de educación superior de la provincia de Santa Elena, con la finalidad de generar un informe acerca de los datos encontrados y complementando con una guía de buenas prácticas para los estudiantes de dicha entidad.

1.2 DESCRIPCIÓN DEL PROYECTO

El presente proyecto propone determinar las vulnerabilidades en una institución de educación superior, a través de la recopilación de información, mediante ingeniería social aplicando técnicas computacionales y no computacionales, con el objetivo de generar un informe acerca de los datos recabados, complementando con una guía de buenas prácticas para dicha entidad.

Diversas instituciones son víctimas de ciberataques, según el estudio realizado por ITRC Data Breach Reports el 23,7% son ataques realizados al sector de la salud, un 8,0% a la educación y empresas gubernamentales presentan un 4,7% [9]. A nivel mundial en el periodo 2018-2019 se registró un aumento del 33% en ataques informáticos tipo phishing [9], los ataques con técnicas de ingeniería social son cada vez más comunes dentro de la sociedad. En el año 2021 la tendencia de crecimiento de ataques informáticos en Ecuador aumentó significantemente un 75% con relación a años anteriores [9]. En estas estadísticas se puede observar que las instituciones de educación se encuentran como una de las víctimas preferidas de estos delincuentes informáticos.

Por motivos del crecimiento de ataques informáticos en el país, se desea realizar un análisis de ingeniería social en una institución de educación superior, los resultados servirán para analizar estos inconvenientes que se presentan en el lugar, dar recomendaciones para disminuir la posibilidad de un futuro ataque, mitigar el daño que

puede generar el mismo y evitar que la falta de seguridad informática sea aprovechada por estos ciber atacantes.

Las fases que se utilizarán en el presente proyecto son: Identificación y selección de técnicas de ingeniería social, implementación de técnicas de ingeniería social, análisis de resultados e informe de resultados.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Aplicar ingeniería social mediante el diseño de ataques de seguridad informática, con técnicas computacionales y no computacionales, para evaluar el nivel de conocimiento de los usuarios, respecto al uso seguro de los sistemas informáticos.

1.3.2 OBJETIVOS ESPECÍFICOS

- Investigar acerca de los distintos tipos de métodos empleados en ingeniería social, escogiendo las técnicas adecuadas, para identificar las vulnerabilidades a las que están expuestas los usuarios.

- Recopilar información, mediante métodos de recolección de datos, para tener una base de conocimientos previos de las habilidades de los usuarios respecto al uso seguro de los sistemas informáticos.

- Emplear técnicas computacionales y no computacionales a través de ingeniería social, para analizar las vulnerabilidades a las que están expuestas los usuarios por falta de conocimiento en seguridad informática.

- Elaborar un informe final con los resultados obtenidos, para evidenciar el diseño de los ciberataques y sus consecuencias.

- Proponer una guía de buenas prácticas de seguridad de la información, basada en la norma ISO 27001, que permita mejorar el nivel de conocimiento de los usuarios respecto al uso seguro de los sistemas informáticos.

1.4 JUSTIFICACIÓN

La seguridad informática ha experimentado un profundo cambio en los últimos años. La misma, pasó de ser un gasto innecesario a una inversión aislada con el objetivo de fortalecer la protección de datos en puntos muy concretos, por esta razón las inversiones en este sector han crecido de forma exponencial para cuidar lo más valioso que tiene la entidad, que es resguardar los procesos que posee y la información del personal [10]. El 70% de las instituciones consideran que la ciberseguridad es prioridad en sus agendas, ya que esto ayuda a mitigar los ataques que se pueden presentar en el lugar [10].

En el año 2019 el ESET reportó los incidentes de seguridad basándose en países de Latinoamérica donde se puede observar que el país con más inconvenientes de este tipo es México con el 72%, seguido por Perú con el 71%, Paraguay 67% y Ecuador con el 65% de ataques registrados, las medidas que fueron implementadas por diversas instituciones lograron reducir un 10% de ataques con Ransoware con respecto a los años anteriores [11].

En los últimos años se han implementado nuevos procesos que permiten mitigar los ataques informáticos, para evitar el hurto de información, suplantación de identidad, DDOS, etc. Los trabajos de investigación lograron construir diversas metodologías que permiten reducir el impacto de un futuro ataque, utilizando los análisis de vulnerabilidades cuya aplicación permite disminuir el riesgo a equipos y redes, precautelando la información y servicios de las organizaciones [8].

Con el flujo constante de personas en las instituciones, especialmente usuarios nuevos y salientes, se puede decir que enseñar a cada miembro de una organización las mejores prácticas de ciberseguridad, es un proceso interminable [8].

Mientras comienzan desde la incorporación y la inducción, los empleados nuevos y existentes necesitan recordatorios constantes y actualizaciones sobre los pasos que deben tomar diariamente para proteger a la entidad de la gran cantidad de amenazas cibernéticas emergentes muchas veces provenientes de método hábiles de ingeniería social [12].

La virtualización de sistemas operativos y procesos sirve principalmente para compartir los recursos y optimizar el uso de procesadores [11]. Virtual Box es un software que nos ayuda a recrear estos sistemas operativos para utilizar las herramientas disponibles que estos S.O nos ofrecen para trabajar de una mejor forma.

Al realizar el análisis de vulnerabilidades utilizaremos varias herramientas que están disponibles en el S.O Kali Linux, el resultado obtenido por ambos sistemas serán comparados y esto permitirá elegir la información más sensible para realizar el estudio.

La finalidad de este trabajo investigativo es presentar un informe, donde se establezcan todas las vulnerabilidades existentes. Además, se elaborará una guía de buenas prácticas con recomendaciones que se puedan ejecutar, para mitigar los riesgos de un futuro ataque y reforzar la seguridad informática de dicha entidad de educación superior.

Este proyecto está direccionado al plan de creación de oportunidades.

Objetivo 10. Garantizar la Soberanía nacional, integridad territorial y seguridad del estado.

Tomando en cuenta el redimensionamiento político de los temas de seguridad con una orientación cooperativa y coordinada, considerando la soberanía, la independencia y el planteamiento de la política de los Estados [13].

Políticas.

10.1 Fortalecer al Estado para mantener la confidencialidad, integridad y disponibilidad de la información frente a amenazas provenientes del ciberespacio y proteger su infraestructura crítica [13].

Lineamiento territorial 10.1. Promover el mejoramiento de la calidad de vida de las personas que habitan las zonas de frontera, en un entorno de respeto a los derechos humanos [13].

Metas al 2025

10.1.1 Incrementar el índice de ciberseguridad global de 26.3 a 51.3 [13].

Objetivos del eje Económico

Objetivo 5. Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social [13].

Política 5.5: Mejorar la conectividad digital y el acceso a nuevas tecnologías [13].

1.5. METODOLOGÍA DEL PROYECTO

1.5.1. METODOLOGÍA DE LA INVESTIGACIÓN

El proyecto de investigación realizado a esta institución tomó de referencia documentos que contengan análisis hechos a otras instituciones, por eso el tipo de metodología empleado será exploratorio [14]. La investigación que se realizará a esta institución, no se ha realizado con anterioridad, con recolección de información mediante técnicas de ingeniería social [14].

Se recopiló información con diferentes herramientas y métodos de ciberataques, así mismo, la búsqueda de trabajos similares respecto al presente tema de investigación, en base a la metodología aplicada, la cual es de tipo diagnóstica [14]. Teniendo como objetivo, disminuir el porcentaje de información sensible entregada a terceros por parte del personal [14].

1.5.2. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Las técnicas utilizadas para la recolección de información se dieron mediante ingeniería social, en una encuesta realizada en Google form para recolectar información acerca del conocimiento de dichos ataques y procedimientos que se van a realizar en la entidad (Ver Anexo 7), en relación al presente proyecto.

1.5.3. RECOPILACIÓN DE INFORMACIÓN

Es una actividad que se basa en agrupar datos importantes sobre un contenido en específico, de tal forma, es importante conocer la opinión de las personas para el correcto desarrollo del trabajo. Por este motivo, se realiza la recolección de información en la institución de educación superior de la provincia de Santa Elena, realizando una encuesta general [Anexo7] al personal docente y estudiantes de la entidad, a través de la herramienta Google form, con el objetivo de saber si tienen conocimientos acerca de ataques cibernéticos e ingeniería social.

Esta fase se considera como la parte más importante del proyecto, ya que aquí se determina la situación actual en la institución y los conocimientos que poseen las personas, permitiendo almacenar y analizar la información sobre los individuos, teniendo una base de donde partir para el desarrollo de este proyecto.

1.5.4. DATOS DE LA INSTITUCIÓN

La institución donde se hará el ataque, cuenta con un departamento de TI, el cual está encargado de la administración de las redes en todo el campus, dichas redes están divididas de manera híbrida dentro de cada departamento con conexiones por cableado y en todo el campus a través de wifi de largo alcance, que se expande en varias redes para personal específico, entre estudiantil y administrativo, el cual es privado y encriptado mientras que el otro se mantiene de manera libre para los usuarios.

De la misma forma mantiene una página web interactiva, que consta con varios aplicativos webs para estudiantes, docentes y administrativos, motivo por el cual, en conjunto se maneja un aula virtual en donde interactúa el docente con los estudiantes, empleando un usuario y contraseña individual, el cual es el principal medio de ataque que se estudiará. Como esta institución se divide en múltiples sectores se comenzará este ataque ético desde una zona en la, cual se piensa será el punto más vulnerable de toda esta institución.

1.5.5. METODOLOGÍA DE DESARROLLO

Este trabajo se realizó mediante una metodología genérica, adaptada con el fin de identificar vulnerabilidades mediante ataques de ingeniería social. Se divide en las siguientes fases: Identificación y selección de técnicas de ingeniería social, implementación de técnicas de ingeniería social, análisis de resultados e informe de resultados.

Esta metodología se enfoca en 4 fases, las cuales se explican a continuación:

- **Identificación y selección de técnicas de ingeniería social:** Se reúne información acerca de las principales técnicas de ingeniería social computacionales y no computacionales, mostrándolas en un cuadro comparativo.

- **Implementación de técnicas de ingeniería social:** En esta fase se diseñan y ejecutan los diversos ataques de ingeniería social, creando un prototipo experimental para infectar al individuo de manera computacional, proponiendo una forma de ingeniería social para determinar la posible extracción de cuentas y contraseñas. Además, se realiza la identificación de vulnerabilidades, obteniendo acceso a los sistemas y evaluando los mismos.

- **Análisis de resultados:** Se evalúan todos los resultados de la ejecución de ataques de ingeniería social computacionales y no computacionales, aplicados en la fase anterior, para obtener información concreta de las vulnerabilidades encontradas.

- **Informe de resultados:** Se crea un informe de los ataques generados para constatar de qué modo se pudo extraer más información, así mismo, el documento abarca un análisis completo de cada infección recolectada en el transcurso de la fase 2. De la misma forma, se propone una guía de buenas prácticas, que ayude al usuario con un amplio contenido de información, sobre la prevención de posibles ataques dentro de la institución.

La metodología que se utilizará en el presente proyecto se adaptó teniendo en cuenta los requerimientos recopilados en la institución, la cual está diseñada para evaluar la entidad, realizar los ataques, analizar los resultados y posteriormente, crear una guía de buenas prácticas. Esta metodología ayuda a proyectar de la mejor manera cada fase, siguiendo una secuencia de los procesos en cada ítem.

2. LA PROPUESTA

2.1 MARCO CONTEXTUAL

2.1.1. INSTITUCIONES DE EDUCACIÓN SUPERIOR

Las instituciones de educación superior son entidades que cuentan con un orden de normas legales, con el reconocimiento oficial siendo prestadoras de servicio público de la educación superior [15]. Dichas instituciones son pluralistas, están abiertas a todas las formas del pensamiento universal expuestas de manera científica [15]. Dirigen su actividad a la formación integral de las personas para contribuir al desarrollo del país y al logro de la justicia social [15].

2.1.2. SEGURIDAD INFORMÁTICA EN INSTITUCIONES DE EDUCACIÓN SUPERIOR

Asegurar la confidencialidad, integridad y disponibilidad de la información en un mundo tecnológico se han convertido en los ejes principales a garantizar al interior de cualquier organización, de hecho, actualmente, el sector educativo tiene el desafío de evitar la vulnerabilidad, fortalecer el acceso, monitorear y garantizar la adecuada gestión de los equipos, reduciendo las posibilidades de ser víctimas de ataques cibernéticos [16].

Los diferentes riesgos van de la mano con la seguridad de la información, desafiando las seguridades físicas tradicionales, como en un campus universitario, un edificio o alumnos y empleados de un ente educativo superior, esto se ha convertido en una necesidad para implementar protocolos de seguridad para la información mediante pasos de autentificación, estructuración, secuencia y encriptado de datos organizacionales [17].

Las instituciones de educación superior han mostrado recientemente un creciente interés por lograr una mayor eficiencia en la gestión, dependiendo de una escala más alta sobre la seguridad de estas gestiones. Debiendo trabajar para enfrentar los desafíos creados por las necesidades internas y externas de seguridad tanto para empleados administrativos, personal general, docentes y estudiante, sobre todo con personas que se conectan a las redes gratuitas de la institución [18].

Por otro lado, se dice que las instituciones de educación superior presentan grandes desafíos como son la integración de la seguridad informática en el establecimiento, así mismo, las capacitaciones que se deben impartir acerca de este tema, continuamente a los docentes y estudiantes que conforman la entidad [18].

APLICACIÓN DE SEGURIDAD INFORMÁTICA EN EL ÁMBITO TECNOLÓGICO

Los piratas informáticos están evolucionando y sus tecnologías se están volviendo cada vez más sofisticadas, por lo que las organizaciones ya no pueden confiar en un enfoque propietario de la seguridad [19]. Las amenazas continúan evolucionando y cambiando a diario, y las empresas de todos los tamaños deben esforzarse por ser resilientes, trabajar regularmente para desarrollar y perfeccionar estrategias de seguridad tan polifacéticas como la infraestructura que las protege [19].

Sabiendo que las redes universitarias deben respetar la diversidad de estas funciones, la planificación es necesaria para garantizar la eficacia del servicio, así como su seguridad [19]. Ante esto, Pablo Ramos, Especialista en Seguridad de la Información de ESET Latinoamérica, dice que planificar y diseñar infraestructura educativa no es una tarea para nada sencilla, ya que, la protección de la infraestructura de TI es el procedimiento de implementar medidas que ayuden a salvaguardar el entorno tecnológico de la institución, abarcando toda el área de TI, incluyendo las redes, software relevantes y componentes de hardware [19].

“Primero hay que pensar en el tráfico que hay que manejar, así como en el comportamiento de los estudiantes y docentes, que en la mayoría de los casos va más allá de las buenas prácticas de seguridad informática, ya que la información se maneja dentro de una institución educativa, es necesario desde el comienzo para considerar los segmentos de la red que también deben tratarse hasta los programas y políticas de seguridad. [20]”.

Referentemente en una de sus revistas Universitaria, se menciona que por el impacto de las TIC en diversos sectores de la sociedad, incluyendo la educación y la cultura, donde se necesita apoyo para resolver problemas a través de planes de transformación; Se presentó un trabajo de diseño arquitectónico y modelo tecnológico de componentes para la creación de un campus universitario virtual y el desarrollo de estudios en línea en el contexto de la educación superior en el Ecuador [21]. Para ello, se toma como referencia el marco normativo vigente en el Ecuador y las principales recomendaciones que las instituciones de educación superior deben ser aprobadas por las instituciones de educación superior [21]. Ofreciendo oportunidades de carrera en métodos en línea o aquellos que necesitan un campus virtual para aumentar su productividad [21].

APLICACIÓN DE SEGURIDAD INFORMÁTICA EN LA COMUNIDAD ACADÉMICA

Si bien el proceso de integración de la seguridad informática en las ideas y acciones de la sociedad avanza poco a poco, las dificultades que implica presentar esta información en la comunidad estudiantil también son cada vez más complejas de entender y manejar [22]. Según Security Scorecard, un tercio de los ataques cibernéticos en 2018 se dirigieron a instituciones de educación superior [22]. Así lo confirmó el director de Seguridad de la Universidad de Pensilvania, Donald Welch, quien afirmó que cuando se trata de ciberseguridad en las instituciones de educación superior, solo se dedica un pequeño porcentaje del tiempo al desarrollo de una estrategia para prevenir amenazas y mitigar futuras violaciones [22]. Hay que entender que las universidades son instituciones que tienen casi todo tipo de datos importantes, críticos y confidenciales [22].

FINES Y PRINCIPIOS DEL SISTEMA DE EDUCACIÓN SUPERIOR

Art. 1.- Ámbito. - Esta Ley regula el sistema de educación superior en el país, a los organismos e instituciones que lo integran; determina derechos, deberes y obligaciones de las personas naturales y jurídicas, y establece las respectivas sanciones por el

incumplimiento de las disposiciones contenidas en la Constitución y la presente Ley [23].

Art. 2.- Objeto. - Esta Ley tiene como objeto definir sus principios, garantizar el derecho a la educación superior de calidad que propenda a la excelencia interculturalidad, al acceso universal, permanencia, movilidad y egreso sin discriminación alguna y con gratuidad en el ámbito público hasta el tercer nivel [23].

Art. 3.- Fines de la Educación Superior. - La educación superior de carácter humanista, intercultural y científica constituye un derecho de las personas y un bien público social que, de conformidad con la Constitución de la República, responderá al interés público y no estará al servicio de intereses individuales y corporativos [23].

Art. 4.- Derecho a la Educación Superior. - El derecho a la educación superior consiste en el ejercicio efectivo de la igualdad de oportunidades, en función de los méritos respectivos, a fin de acceder a una formación académica y profesional con producción de conocimiento pertinente y de excelencia [23]. Las ciudadanas y los ciudadanos en forma individual y colectiva, las comunidades, pueblos y nacionalidades tienen el derecho y la responsabilidad de participar en el proceso educativo superior, a través de los mecanismos establecidos en la Constitución y esta Ley [23].

2.1.3. NECESIDAD DE HERRAMIENTAS TECNOLÓGICAS EN LA COMUNIDAD ACADÉMICA

En la actualidad la tecnología avanza notablemente, y el desarrollo de herramientas tecnológicas ha adoptado el ritmo en la vida cotidiana [24]. En el contexto educativo, es bastante común que los estudiantes utilicen varias herramientas para realizar tareas académicas o facilitar el trabajo en el proceso enseñanza – aprendizaje [24]. Ahora realizan las actividades en el menor tiempo posible, por ejemplo: Buscar un libro por internet y no tener que ir físicamente a una biblioteca [24].

A continuación, se detallan las herramientas tecnológicas que los estudiantes más utilizan en la era actual:

- **Gmail:** Servicio de correo electrónico, permitiendo acceder a servicios de la nube y sus beneficios [25].
- **Microsoft Word:** Procesador de textos, que permite manipular, guardar, imprimir y compartir información [26].
- **Adobe Acrobat:** Es una familia de aplicaciones informáticas, diseñados para visualizar, crear y modificar archivos en formato PDF [27].
- **Google Chrome:** Es un navegador web rápido y seguro [28].
- **Google:** Es un motor de búsqueda, que permite recibir millones de consultas cada día a través de sus distintos servicios [29].
- **Power Point:** Es un programa de presentación, utilizado en diversos campos de la enseñanza, los negocios, entre otros [30]. Permite las animaciones de texto e imágenes prediseñadas [30].
- **Microsoft Excel:** Es un programa de software de hojas de cálculo y una herramienta avanzada de análisis y visualización de datos [31].
- **Avast:** Es un antivirus inteligente, que detecta virus, malware, spyware, ransomware, phishing, entre otras amenazas [32].
- **Facebook:** Es una red social, que permite vínculos virtuales y ofrece servicios para redes y medios de carácter social, en línea [33].
- **WhatsApp:** Aplicación de chat para teléfonos móviles de última generación, los llamados smartphones, que sirve para enviar mensajes de texto y multimedia [34].
- **Zoom:** Servicio de videoconferencia basado en la nube que se utiliza para reunirse virtualmente con otras personas [35].
- **Moodle:** Plataforma de aprendizaje diseñada para proporcionar a docentes y estudiantes, un sistema para crear ambientes de aprendizaje personalizado [36].
- **Drive:** Servicio de almacenamiento de datos, guardados en la nube [37].

2.1.4. BASE LEGAL

La Ley Orgánica de Protección de Datos Personales, es una norma jurídica que tiene como objetivo garantizar y proteger el tratamiento de datos personales, libertades públicas y derechos fundamentales de las personas físicas, especialmente en su honor e intimidad personal y familiar [38].

Según la Ley Orgánica de Protección de Datos Personales (LOPD), se consideran los artículos más relevantes en el presente trabajo [38]:

Capítulo I.- Ámbito de aplicación integral

Art 1.- Objeto y finalidad. – El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección [38]. Para dicho efecto regula, prevé y desarrolla principios, derecho, obligaciones y mecanismos de tutela [38].

Artículo 5.- Integrantes del sistema de protección de datos personales. – Son parte del sistema de protección de datos personales, los siguientes [38]:

1. Titular;
2. Responsable del tratamiento;
3. Encargado del tratamiento;
4. Destinatario;
5. Autoridad de protección de datos personales; y,
6. Delegado de protección de datos personales.

Artículo 25.- Categorías especiales de datos personales. – Se considerarán categorías especiales de datos personales, los siguientes [38]:

a) Datos sensibles;
b) Datos de niñas, niños y adolescentes;
c) Datos de salud; y,
d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.

Artículo 37.- Seguridad de datos personales. – El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos [38].

Artículo 38.- Medidas de seguridad en el ámbito del sector público. – El mecanismo gubernamental de seguridad de información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones,

destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales [38].

2.2 MARCO CONCEPTUAL

2.2.1. INGENIERÍA SOCIAL

Es un conjunto de técnicas que utilizan los hackers para engañar a sus víctimas y que les envíen datos sensibles, infectando sus computadoras con malware o abriendo enlaces a sitios infectados [3]. Del mismo modo, los ciberdelincuentes pueden tratar de aprovecharse por la falta de conocimiento de los usuarios, ya que, la mayoría de personas no son conscientes del valor que tienen los datos personales y no saben la manera de proteger correctamente su información [3].

2.2.2. TÉCNICAS DE INGENIERÍA SOCIAL

Entre las técnicas más conocidas en ingeniería social para manipular a una persona, y que la misma, realice aquello que el hacker le propone, se dividen en computacionales y no computacionales. A continuación, se presentan las técnicas más importantes:

Técnicas de ingeniería social	
COMPUTACIONALES	**Vector de ataque**
	Spear-Phishing Attack Vectors
	Website Attack Vectors
	Infectious Media Generator
	Create a Payload and Listener
	Mass Mailer Attack
	Arduino-Based Attack Vector
	Wireless Access Point Attack Vector
	QRCode Generator Attack Vector
	Powershell Attack Vectors
	Third Party Modules
	Smishing
	Vishing
	Spear phishing
	Dumpster Diving
	Shoulder surfing

NO COMPUTACIONALES	Tailgating
	Eliciting information
	Identity Fraud
	Invoice Scams
	Reconnaissance
	Hoax

Tabla 1. Técnicas de ingeniería social

2.2.3. HERRAMIENTAS UTILIZADAS EN LA APLICACIÓN DE INGENIERÍA SOCIAL

2.2.3.1. KALI LINUX

Es una distribución de Linux, que se basa en Debian de código abierto, que tiene como objetivo realizar pruebas de penetración avanzadas y auditorías de seguridad [39]. Kali Linux posee múltiples herramientas destinadas a distintas tareas de seguridad de la información, tales como: pruebas de penetración, informática forense, investigación de seguridad e ingeniería inversa [39]. Es una solución multiplataforma, disponible y accesible de manera gratuita para profesionales y aficionados en la seguridad de la información [39].

Se lanzó el 13 de marzo de 2013, vista como una reconstrucción completa de BackTrack Linux y se adhiere de forma completa a los estándares de desarrollo de Debian [39].

2.2.3.2. SOCIAL ENGINEERING TOOLKIT

Se utilizará una suite completa de ingeniería social, permitiendo automatizar tareas desde el envío de mensajes de texto falsos (mensajes de texto), donde se pueden reemplazar números de teléfono enviando mensajes, clonar cualquier sitio web, configurar y ejecutar un servidor de phishing en segundos [40].

El kit de herramientas SET está diseñado específicamente para realizar ataques avanzados contra el elemento, esta herramienta rápidamente se convirtió en estándar para ataques de usuarios en emprendimiento [40]. SET fue creado por David Kennedy (ReL1K) con gran ayuda de la comunidad para combinar ataques sin precedentes en un solo conjunto de herramientas de explotación [40].

Está conformada por muchas funciones de Metasploit, además, por lo que no es posible diseñar un SET sin instalar primero dicha herramienta [40].

2.3 MARCO TEÓRICO

2.3.1. PRÁCTICAS DE INGENIERÍA SOCIAL

El presente artículo titulado “Ingeniería Social, un ejemplo práctico”, habla de las empresas y el impacto que tienen en la actualidad, adoptando espacios de almacenamiento digital donde recopilan el activo más valioso que posee, la información, la misma se constituye de datos financieros, clientes, informes, entre otros, la cual puede ser prescindida con malas intenciones por los ciberdelincuentes o personas que buscan utilizar esta información de forma maliciosa para perjudicar la entidad [41].

Las empresas siempre buscan tomar medidas de seguridad, que ayuden a administrar los datos que poseen, teniendo en cuenta tres pilares esenciales: confidencialidad, integridad y disponibilidad [42]. Con el pasar del tiempo, la tecnología avanza y con ello se asocian los posibles riesgos que presentan los sistemas de información, y la manera de protegerlos, con herramientas como firewall, sistemas de detección de intrusos, entre otras [42].

En el trabajo de investigación se propone la metodología para la generación y ejecución de campañas de ingeniería social, donde se tendrá como resultado una evaluación de vulnerabilidades a nivel personal en la entidad determinada, concluyendo con los grados de riesgo de la misma, generando una metodología aplicada, teniendo la capacidad de poder planificar una serie de ataques computacionales a través de métodos de ingeniería social en la empresa perfilada [41]. También, se identificaron pasos importantes dentro del proceso de la guía, tales como: perfilamiento previo de la institución y planificación de campañas de ingeniería social [41].

Se logra reconocer que el fin del atacante que aplica ingeniería social, es el de explotar al eslabón débil de la institución, generando un buen ambiente de confianza con la persona, empleando herramientas tecnológicas o encuentros cara a cara, para obtener la información que necesita [43]. Es importante tener en cuenta que, no solamente el usuario está expuesto a ser víctima de un ataque cibernético, si no también, el mismo personal de seguridad informática [43].

Finalmente, como parte de las recomendaciones, las víctimas pueden descubrir que están siendo un blanco de ataques informáticos, por lo tanto, es recomendable que el ingeniero social esté en constante monitoreo de las reacciones de los usuarios y pueda actuar de manera rápida en caso de una emergencia [41].

2.3.2. EXPERIMENTO PARA CREAR CONCIENCIA EN LAS PERSONAS ACERCA DE LOS ATAQUES DE INGENIERÍA SOCIAL

Eduardo Benavides, Walter Fuertes y Sandra Sánchez, señalan en su artículo "Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social", que la misma, es una técnica que permite recopilar información de usuarios de manera fraudulenta, con el objetivo de emplearla en contra de ellos mismos, o de las instituciones donde laboran, presentando un experimento que se enfoca en crear conciencia acerca de las consecuencias de este tipo de ataque, a través de la ejecución de ataques controlados a personas de confianza [44]. Para lograr esto, se ha llevado a cabo un conjunto de actividades y engaños, que los hackers utilizan comúnmente para obtener información sensible, generando curiosidad de los contactos en redes sociales para que visiten una página falsa con información ficticia [44].

Los ataques de ingeniería social utilizan sitios falsos como señuelos para afectar a los usuarios, invitando a los mismos, a acceder a una página fraudulenta, infectando con malware, especialmente troyanos, para posteriormente, robar información de los equipos de las víctimas, obteniendo datos de tarjetas de crédito o suplantar la identidad de las personas [45]. Así mismo, luego de realizar los ataques se hace una encuesta a los individuos acerca del conocimiento que poseen de Phishing e ingeniería social, mostrando en los resultados que únicamente el 2% de los usuarios que visitaron la página, no tienen conocimiento de cómo se puede vulnerar la información [44].

Se puede decir que los estudios que presentan una propuesta para concientizar a las personas, incentivan a los usuarios a informarse acerca de los riesgos que traen consigo estas prácticas de los ciberdelincuentes, del mismo modo, saber la manera de prevenirlos y las medidas de seguridad para reducirlos [46].

Finalmente, en diversos trabajos de ingeniería social, se evidencia que los usuarios actúan por desconocimiento o curiosidad, siendo víctimas de ataques cibernéticos, mediante diversas técnicas para obtener información a través de pentesting, lo que presenta un alto índice de riesgo por falta de manejo de estos temas en relación de la seguridad [47].

Por último, se puede destacar que hoy en día, es importante implementar un plan de capacitación y sensibilización dirigido a las personas y entidades, teniendo en cuenta que es más común de lo que se percibe, ser víctima de los ciberdelincuentes [47].

2.3.3. CIBERSEGURIDAD EN PLATAFORMAS EDUCATIVAS INSTITUCIONALES DE EDUCACIÓN SUPERIOR

El objetivo de la presente investigación, es desarrollar un procedimiento para la gestión de seguridad en plataformas educativas de los Institutos Tecnológicos Superiores, el cual ayude con la identificación de vulnerabilidades y riesgos de ciberseguridad, con el fin de brindar protección a las diversas plataformas o sitios de educación [48].

La infraestructura digital en la actualidad permite la conectividad en línea a través de aplicaciones móviles, en donde los estudiantes se integran hacia nuevas experiencias de estudio remoto, mediante plataformas educativas disponibles para la conexión y gestión académica en cualquier parte del mundo, brindando una oportunidad para que los docentes implementen nuevas estrategias de enseñanza – aprendizaje en las limitaciones del contexto virtual [48]. La mayoría de las instituciones educativas, emplean dichas plataformas para la preparación académica, de manera que, incrementa la posibilidad de ataques informáticos y violaciones en la seguridad [48].

Chhertri y Motti, indican en su estudio que, entre los medios electrónicos más vulnerables, están: tablets, teléfonos inteligentes, computadoras portátiles, de escritorio y routers, debido a los factores: manipulación de datos, fuga de información, falla en la interfaz de voz, interrupción, detección del comportamiento de usuario y autenticación de las cuentas, debido a que no disponen de medidas de seguridad apropiadas y utilizan mecanismos sencillos como, contraseñas débiles, credenciales predeterminadas como datos personales, lo cual es un error grave por parte de las personas, al momento de resguardar su información [49].

En el Ecuador aún no se desarrolla una estrategia nacional para la ciberseguridad, que establezca lineamientos, objetivos y plan de acción necesario para proteger los servicios, información e infraestructuras, frente a crímenes cibernéticos [50]. Esta consideración abarca a las Instituciones de Educación Superior, de modo que es declarada en el país como política pública [50]. Por ende, existen aspectos que deben ser tomados en cuenta para proteger la información en la web [50].

El proceso de metodología planteado logra establecer un marco de gestión para la ciberseguridad, aplicado a la infraestructura física y virtual de las plataformas educativas, proponiendo una guía para el control y seguimiento de cada una de las áreas que implican riesgos de seguridad [48].

2.4. COMPONENTES DE LA PROPUESTA

2.4.1. REQUERIMIENTOS

El documento abarcará un análisis completo de cada infección recolectada en el transcurso de la fase 2. De la misma forma, luego de analizar los procedimientos en las fases anteriores.

Código	Especificación de requerimientos
RQ01	Realizar la recolección de información, mediante una encuesta utilizando la escala de Likert a los docentes y estudiantes.
RQ02	Obtener el permiso de los individuos para realizar los ataques de ingeniería social.
RQ03	Identificar el grado de conocimiento de los estudiantes y docentes, con respecto al uso seguro de sistemas informáticos.
RQ04	Emplear la metodología marco de evaluación de seguridad de la información, propuesta en el proyecto.
RQ05	Seleccionar las técnicas adecuadas de ingeniería social, para aplicarlas en el presente trabajo de investigación.
RQ06	Aplicar ingeniería social, mediante técnicas computacionales, por comandos.
RQ07	Utilizar ingeniería social, mediante técnicas no computacionales, por medio de habilidades sociales.
RQ08	Analizar las encuestas a través de gráficos estadísticos, para tener información acerca del conocimiento de dichos ataques y procedimientos realizados en la entidad.
RQ09	Crear un informe de los ataques generados para constatar de qué manera se obtuvo la información, abarcando un análisis completo de los mismos.
RQ10	Elaborar una guía de buenas prácticas sobre el uso seguro de sistemas informáticos, a las personas que participaron en este estudio.

RQ11	Instalar Kali linux en una máquina virtual, para poder ejecutar la fase de ataques.
RQ12	Utilizar un equipo con almacenamiento mínimo de 4 GB de RAM.
RQ13	Realizar pruebas de seguridad en escenarios controlados.
RQ14	Ejecutar las pruebas en horas estratégicas para realizar un ataque exitoso.
RQ15	Crear los ataques en base a páginas conocidas por los individuos, para obtener buenos resultados.

Tabla 2. Requerimientos

3. CAPÍTULO III

3.1. RESULTADOS DE ENCUESTA CON CUADROS ESTADÍSTICOS

I. USO DE SISTEMAS INFORMÁTICOS

1. **¿Qué nivel de conocimientos considera que tiene sobre el uso de internet y sistemas informáticos?**

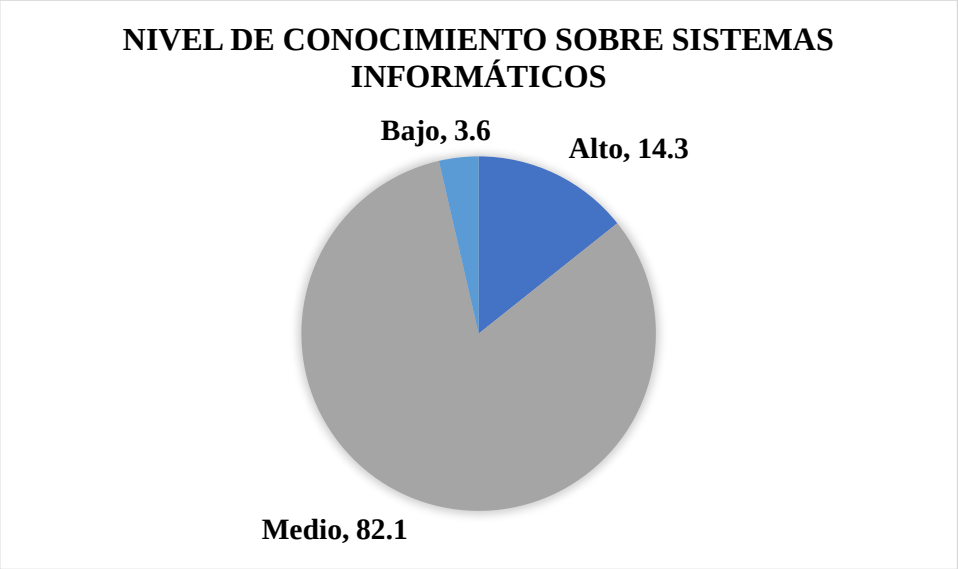


Figura 2. Nivel de conocimiento sobre sistemas informáticos

Del 100% de los encuestados, se pudo determinar que, el 82.1% tiene un nivel medio de conocimientos acerca del uso de internet y sistemas informáticos, mientras que, el 14.3% tiene un nivel alto sobre el tema y solo el 3.6% considera tener un bajo nivel de conocimientos.

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

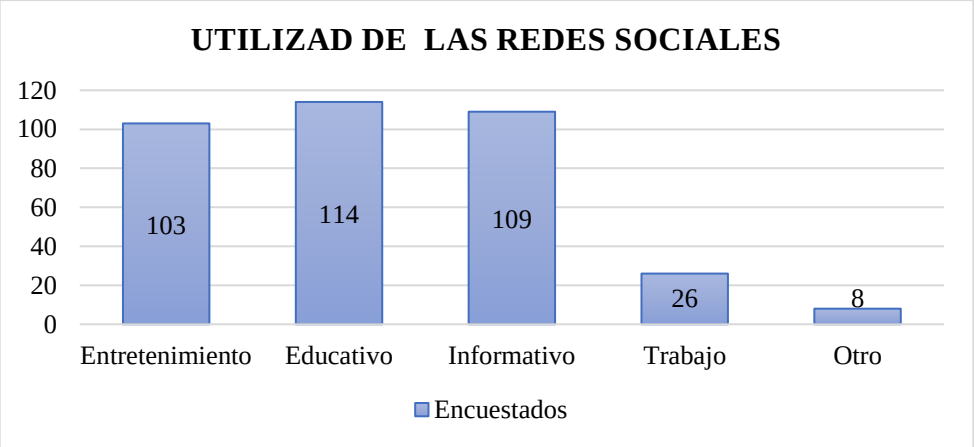


Figura 3. Fin de utilizar las redes sociales

El 73.6% de la población utiliza las redes sociales como medio de entretenimiento, mientras que, el 81.4% manifiesta que las usan para educarse, así mismo, el 77.9% declara que la emplean para informarse, del mismo modo, el 18.6% de los encuestados las utilizan para trabajo y el 5.7% usan las redes sociales con otro fin.

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

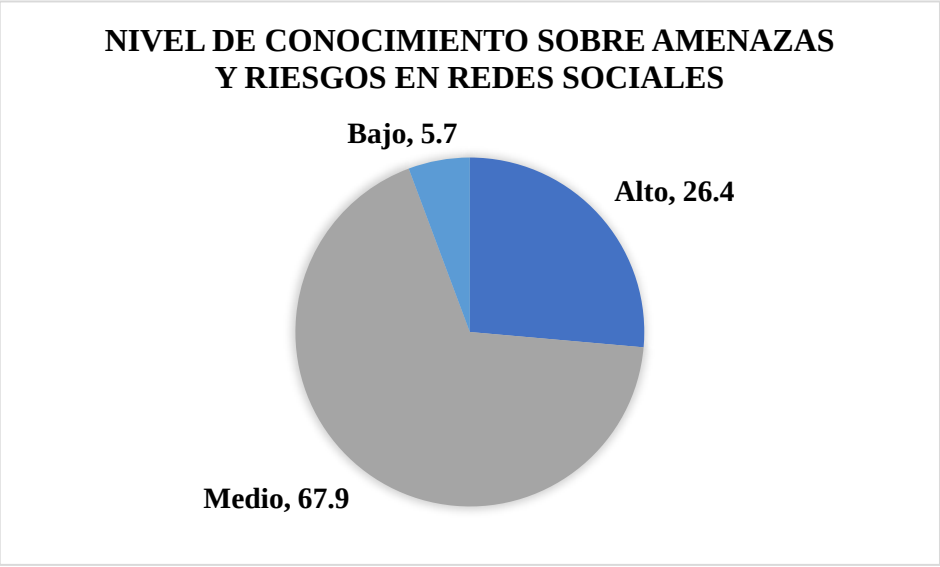


Figura 4. Nivel de conocimiento sobre amenazas y riesgos en redes sociales

Se determinó que, el 67.9% de los encuestados señalan que, tienen un nivel medio de conocimiento respecto a las amenazas y los riesgos informáticos que están presentes en las redes sociales, así mismo, el 26.4% manifiesta tener un alto conocimiento respecto al tema y el 5.7% dicen tener un nivel bajo de conocimiento.

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

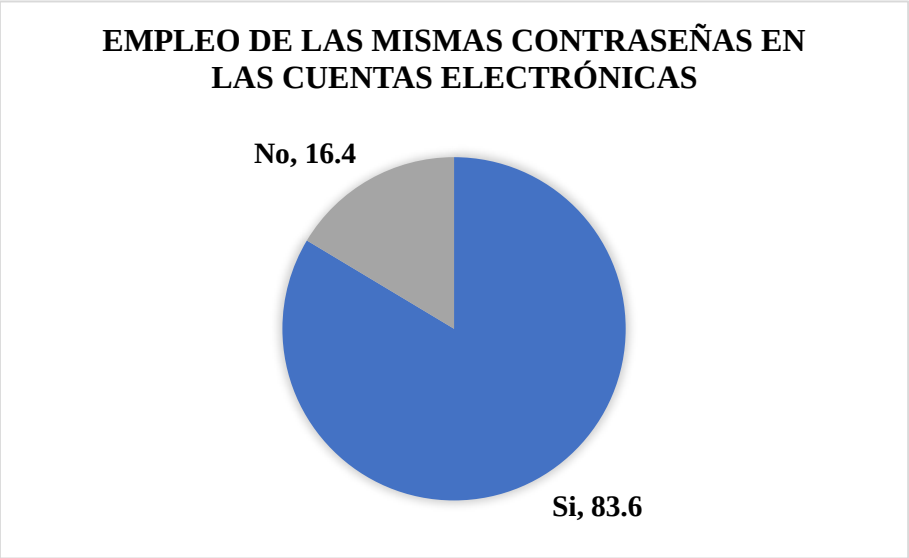


Figura 5. Empleo de las mismas contraseñas en las cuentas electrónicas

El 83.6% de la población declara en la encuesta que, utilizan contraseñas diferentes para sus cuentas electrónicas como redes sociales, email y aula virtual, sin embargo, el 16.4% de los encuestados, manifiestan que emplean las mismas claves.

II. CONOCIMIENTOS DE CIBERATAQUES

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

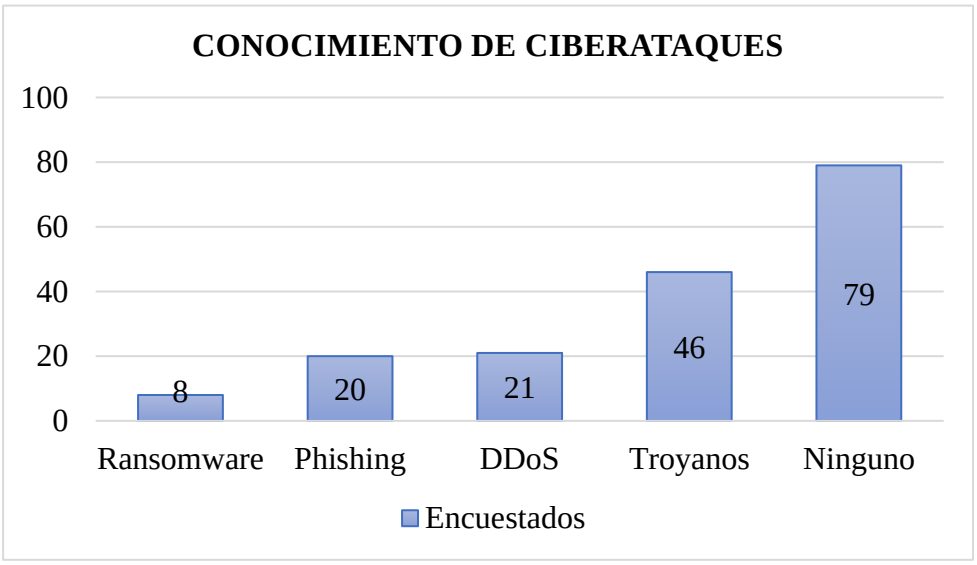


Figura 6. Conocimiento de ciberataques

El 56.4% de los encuestados manifiestan que, no conocen ningún ciberataque, no obstante, las demás personas declaran que conocen diversos ciberataques, pudiendo explicarlos a otras personas. A continuación, se detallan las respuestas: Ransomware (5.7%), phishing (14.3%), ataques de denegación de servicios (15%) y troyanos (32.9%).

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

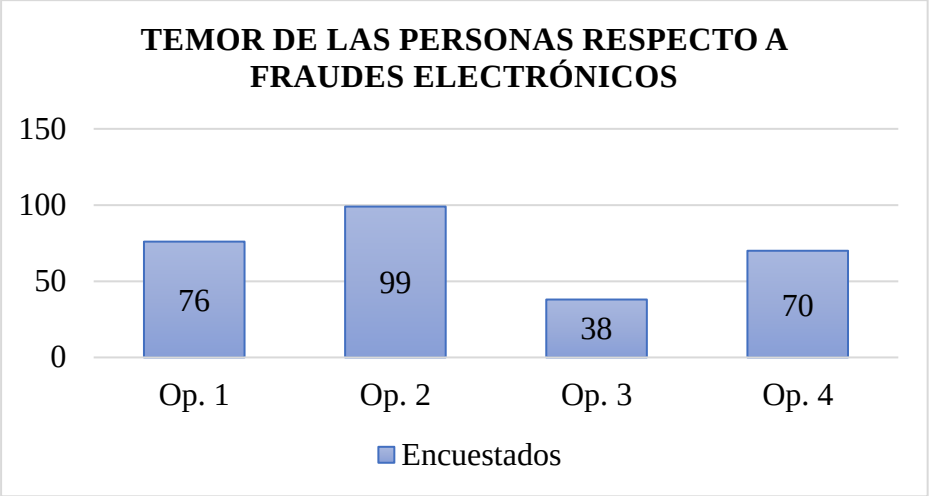


Figura 7. Temor de las personas respecto a fraudes electrónicos

Del 100% de la población encuestada se pudo determinar que, el 54.3% manifiesta que el tipo de fraude electrónico que le genera mayor temor es que les roben dinero de las cuentas bancarias, mientras que, el 70.7% declara que, la suplantación de identidad es su mayor miedo, así mismo, el 27.1% dicen que temen que secuestren su WhatsApp y el 50% desconfían de las estafas de vendedores en sitios web ilegítimos.

7. **¿Con qué frecuencia recibe mensajes de texto que da aviso que alguien ha ingresado a una de sus cuentas electrónicas como Facebook, Instagram, email?**

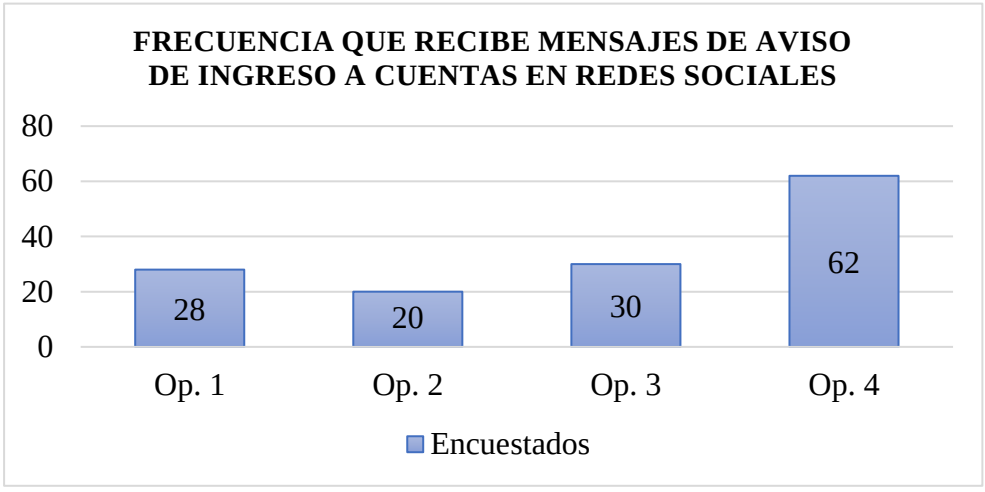


Figura 8. Frecuencia que recibe mensajes de aviso de ingreso a cuentas en redes sociales

El 20% de los encuestados reciben mensajes de texto que dan aviso que alguien ha ingresado a una de sus cuentas electrónicas como Facebook, Instagram o email, 1 vez al mes, de la misma forma, el 14.3% reciben este tipo de mensajes 1 vez cada 3 meses, el 21.4%, 1 vez al año y el 44.3% nunca ha recibido estas alertas.

8. **¿Alguna vez han vulnerado la seguridad de sus cuentas electrónicas?**

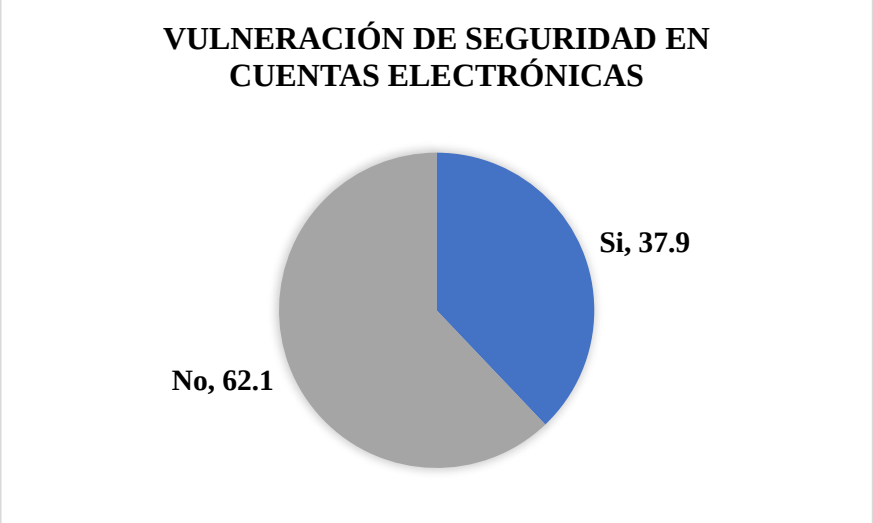


Figura 9. Vulneración de seguridad en cuentas electrónicas

Se pudo determinar que, el 37.9% de los encuestados, alguna vez vulneraron la seguridad de sus cuentas electrónicas, mientras que, el 62.7% no ha presentado este inconveniente.

III. USO SEGURO DE REDES SOCIALES

9. **¿Qué nivel de conocimiento tiene sobre las seguridades que se aplican en sus cuentas electrónicas?**

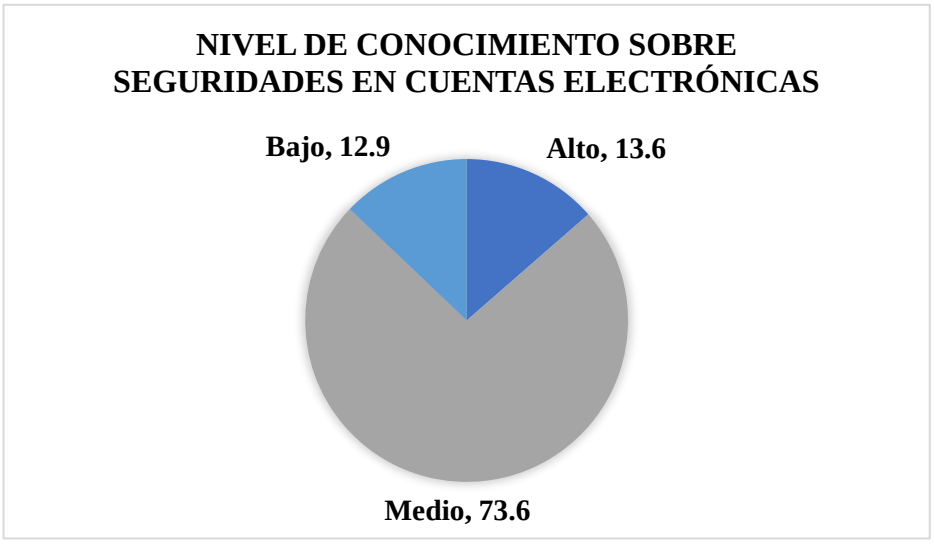


Figura 10. Nivel de conocimiento sobre seguridades en cuentas electrónicas

El 73.6% de la población encuestada manifiesta que, tiene un nivel medio de conocimiento sobre seguridades que se aplican en sus cuentas electrónicas, mientras que, el 13.6% tiene un nivel alto y solo el 12.9% consideran tener un bajo nivel de conocimiento respecto al tema.

10. **¿Cuál de estos métodos le genera mayor seguridad con sus dispositivos y cuentas electrónicas?**

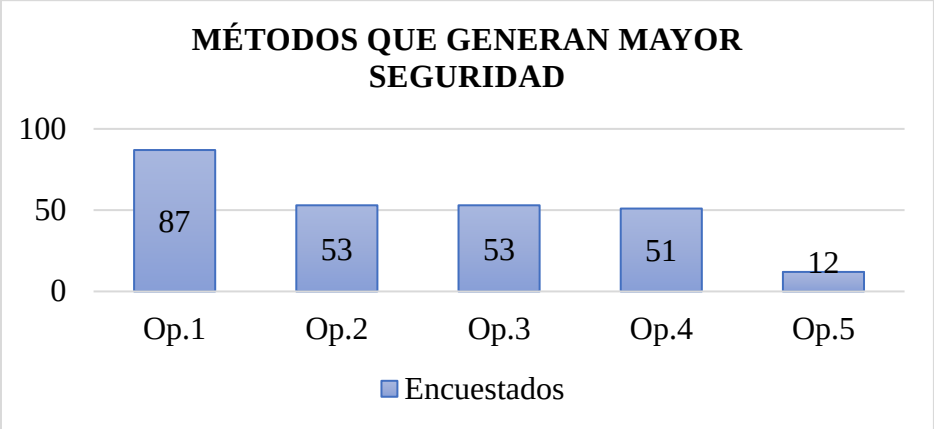


Figura 11. Métodos que generan mayor seguridad

El 62.1% de los encuestados les genera mayor seguridad en sus dispositivos y cuentas, el tener instalado un antivirus, mientras que, el 37.9% manifiesta que es más seguro, desconfiar de todo lo que llega al teléfono, así mismo, el 37.9% dice que, es mejor tener una protección integral de la presencia digital, del mismo modo, el 36.4% declara que, con no abrir emails raros es suficiente y el 8.6% manifiestan que no hacen nada, ya que, sus dispositivos son seguros.

11. **¿Considera importante conocer a las personas que tiene agregadas en sus redes sociales?**

Figura 12. Importancia de conocer a las personas en redes sociales

El 58.6% considera que es muy importante conocer a las personas que tienen agregadas en redes sociales, mientras que, el 32.1% dicen que es importante, así mismo, el 8.6% declaran que es poco importante y el 0.7% manifiestan que, para ellos, no es importante.

12. ¿Considera que su seguridad informática está más amenazada ahora?

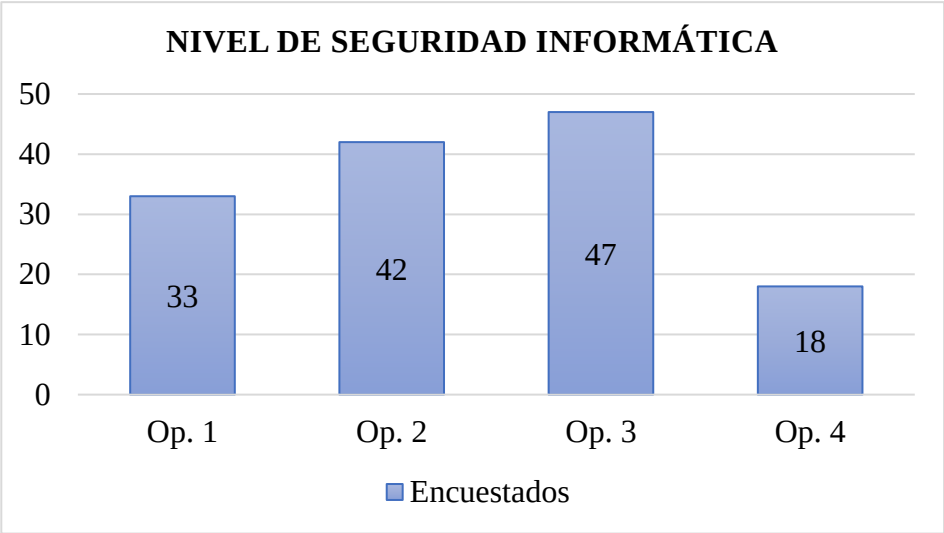


Figura 13. Nivel de seguridad informática

Del 100% de la población encuestada, el 23.6% considera que ahora hay los mismos riesgos de antes, el 30% manifiesta que los riesgos han aumentado un poco pero no les afectan, mientras que, el 33.6% declara que se sienten más vulnerables ante riesgos informáticos y el 12.9% dicen que se sienten muy seguros antes y ahora.

13. En su opinión, ¿Qué tan segura es la red de la Universidad?

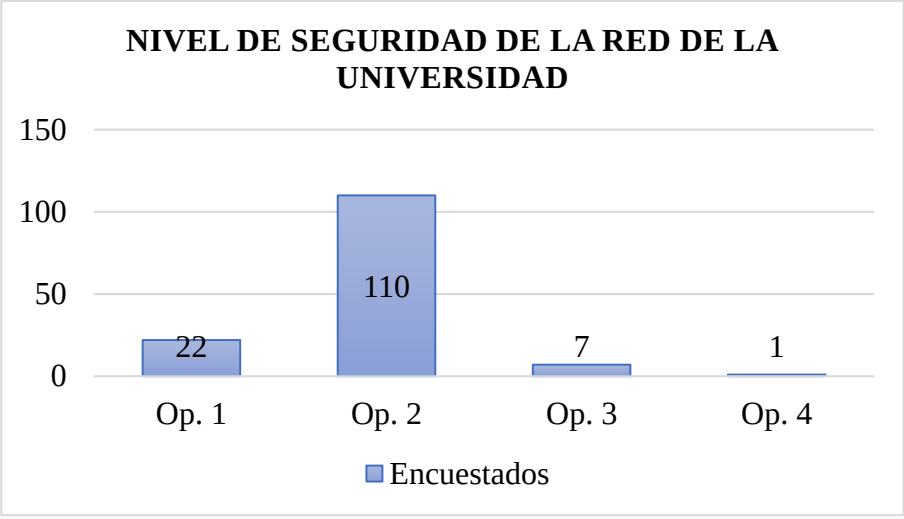


Figura 14. Nivel de seguridad de la red de la universidad

El 15.7% de la población considera que, la red de la universidad es muy segura, mientras que, el 78.6% dice que es segura, así mismo, el 5% declara que es insegura y el 0.7% manifiesta que es muy insegura.

14. ¿Qué nivel de seguridad cree usted que tiene la red WIFI de su institución?

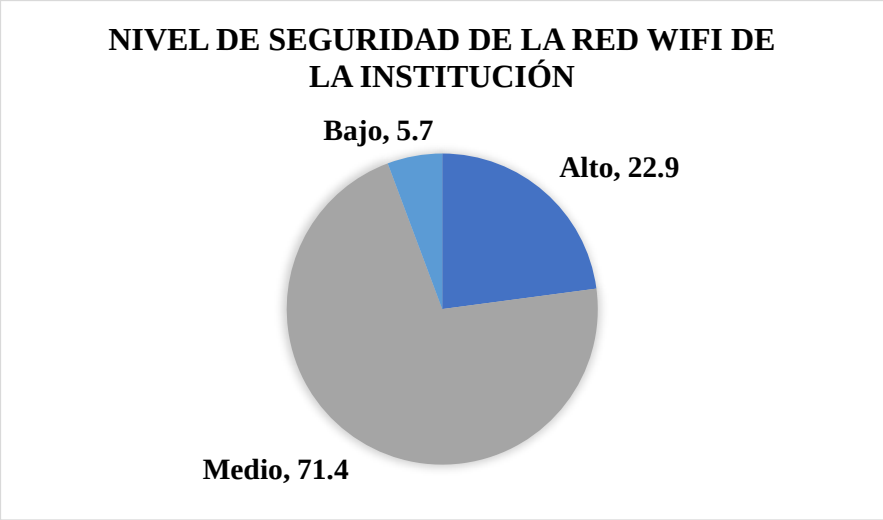


Figura 15. Nivel de seguridad de la red WIFI de la institución

El 22.9% de los encuestados manifiestan que, el nivel de seguridad que tiene la red WIFI de la institución es alto, mientras que, el 71.4% indican que tiene un nivel medio y solo el 5.7% declaran que la red WIFI posee un nivel bajo de seguridad.

15. ¿Conoce de algún ciberataque dirigido a su entidad educativa?

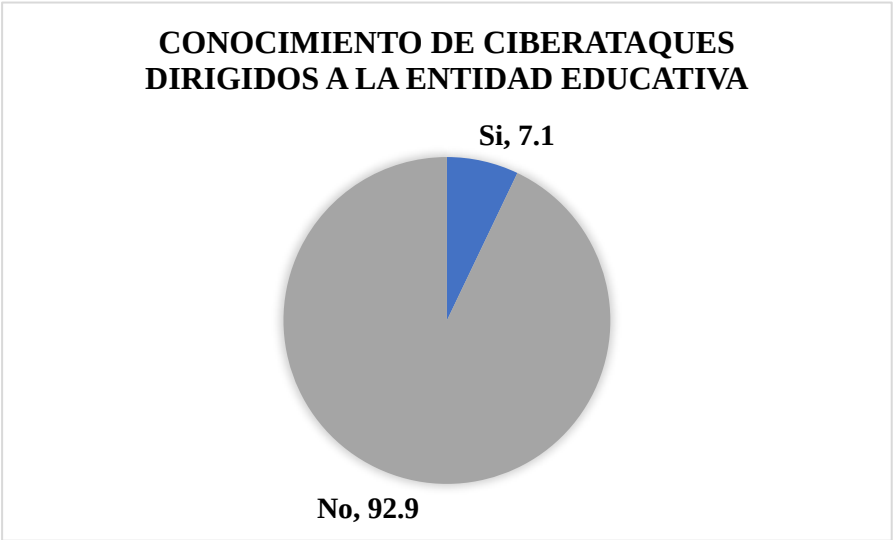


Figura 16. Conocimiento de ciberataques dirigidos a la entidad educativa

Del 100% de los encuestados, el 92.9% conocen de algún ciberataque dirigido a la entidad educativa y el 7.1% no conoce sobre ninguno.

16. ¿Desea participar en este trabajo investigativo como informante del nivel de seguridad que posee en sus dispositivos y cuentas electrónicas?

Figura 17. Participación en el presente trabajo de investigación

El 73.6% de las personas encuestadas, desean participar en este trabajo investigativo como informantes del nivel de seguridad que poseen en sus dispositivos y cuentas electrónicas, mientras que, el 26.4% no está de acuerdo en participar.

3.2. VECTORES DE ATAQUES DE INGENIERÍA SOCIAL

3.3. SELECCIÓN DE TÉCNICAS DE INGENIERÍA SOCIAL COMPUTACIONALES Y NO COMPUTACIONALES

3.3.1. CUADRO COMPARATIVO DE VECTORES DE ATAQUES EN INGENIERÍA SOCIAL CON TÉCNICAS COMPUTACIONALES

VECTOR DE ATAQUE	DESCRIPCIÓN	DIRIGIDO	EFICIENCIA
Spear-Phishing Attack Vectors	Se utiliza para llevar a cabo, ataques de correo electrónico dirigidos contra una víctima.	Usuarios o victimas que frecuentemente usan páginas con correo y contraseña	**MEDIA**
Website Attack Vectors	Es una forma única de utilizar múltiples ataques basados en Web con el fin de comprometer a la posible víctima.	Usuarios o victimas que frecuentemente usan páginas web determinadas con correo y contraseña	**MEDIA**
Infectious Media Generator	La mayoría de las personas tienen al menos una memoria USB para transferir archivos del trabajo a sus hogares. También una característica común de los humanos es la curiosidad. Estas dos cosas combinadas pueden crear una gran amenaza.	Este tipo de ataque permite que el probador de penetración cree un USB, DVD o CD con contenido malicioso. Cuando el usuario desprevenido abre el archivo, la carga útil se ejecutará y devolverá un shell.	**ALTA**

VECTOR DE ATAQUE	DESCRIPCIÓN	DIRIGIDO	EFICIENCIA
Create a Payload and Listener	Crea el contenido de una carga útil saliente en un puerto de elección para el SMB de destino, que luego se conecta. Detrás de escena, las cargas útiles se procesan con un búfer de pila y luego se ejecutan en respuesta a la máquina de ataque que desborda sus puertos.	El oyente se utiliza para monitorear las actividades del ejecutable en la computadora de la víctima. Sin embargo, un atacante tiene que plantar físicamente este ejecutable en la máquina de la víctima y ejecutarlo. Debido a la dinámica de hacer un ataque usando este método, es desfavorable ya que existen otros módulos que pueden entregar el ejecutable al usuario de formas más efectivas.	**BAJA**
Mass Mailer Attack	Un correo masivo generalmente se usa para enviar un enlace de página de phishing a la ID de correo electrónico del objetivo.	El agresor debe conocer la técnica de recolección de correo electrónico para dominar este ataque. Un correo masivo también se usa para ejecutar un ataque de denegación de servicio	**MEDIA**

VECTOR DE ATAQUE	DESCRIPCIÓN	DIRIGIDO	EFICIENCIA
Arduino-Based Attack Vector	Este vector de ataque utiliza el dispositivo basado en Arduino para programar el dispositivo. Puede aprovechar los Teensy, que tienen almacenamiento integrado y pueden permitir la ejecución remota de código en el sistema físico.	Este vector de ataque generará automáticamente el código necesario para implementar la carga útil en el sistema por usted.	**BAJA**
Wireless Access Point Attack Vector	El módulo Wireless Attack creará un punto de acceso falso aprovechando su tarjeta inalámbrica y redirigirá todas las consultas de DNS hacia usted.	creará un punto de acceso inalámbrico, un servidor dhcp y un DNS falso para redirigir el tráfico a la máquina atacante.	**ALTA**
QRCode Generator Attack Vector	El QRCode Attack Vector creará un QRCode para usted con la URL que desee. Cuando haya generado el QRCode, seleccione un vector de ataque adicional dentro de SET e implemente el QRCode en su víctima	Genere un QRCode del SET Java Applet y envíe el QRCode a través de un correo.	**MEDIA**

VECTOR DE ATAQUE	DESCRIPCIÓN	DIRIGIDO	EFICIENCIA
Powershell Attack Vectors	El módulo PowerShell Attack Vector le permite crear ataques específicos de PowerShell. Estos ataques le permitirán utilizar PowerShell, que está disponible de forma predeterminada en todos los sistemas operativos Windows Vista y superior.	PowerShell proporciona un panorama fructífero para implementar cargas útiles y realizar funciones que no se activan con tecnologías preventivas. Inyector de código Shell alfanumérico Powershell Carcasa inversa Powershell Carcasa de unión Powershell Base de datos SAM de volcado de Powershell	**MEDIA**
Third Party Modules	Puede usar Módulos de terceros para agregar funcionalidad al Producto LINQ, siempre que dicho uso esté limitado al uso interno por parte de Usted de una manera que no infrinja ninguna de las disposiciones	Proporciona al atacante un enlace para poder realizar el ataque en una empresa de forma interna.	**MEDIA**

Tabla 3. Cuadro comparativo de vectores de ataques con técnicas computacionales

3.3.2. SELECCIÓN DE TÉCNICAS COMPUTACIONALES

VECTOR DE ATAQUE	DESCRIPCIÓN	DIRIGIDO	EFICIENCIA
Website Attack Vectors	Es una forma única de utilizar múltiples ataques basados en Web con el fin de comprometer a la posible víctima.	Usuarios o victimas que frecuentemente usan páginas web determinadas con correo y contraseña	**MEDIA**
Infectious Media Generator	La mayoría de las personas tienen al menos una memoria USB para transferir archivos del trabajo a sus hogares. También una característica común de los humanos es la curiosidad. Estas dos cosas combinadas pueden crear una gran amenaza.	Este tipo de ataque permite que el probador de penetración cree un USB, DVD o CD con contenido malicioso. Cuando el usuario desprevenido abre el archivo, la carga útil se ejecutará y devolverá un shell.	**ALTA**
QRCode Generator Attack Vector	El QRCode Attack Vector creará un QRCode para usted con la URL que desee. Cuando haya generado el QRCode, seleccione un vector de ataque adicional dentro de SET e implemente el QRCode en su víctima	genere un QRCode del SET Java Applet y envíe el QRCode a través de un correo.	**MEDIA**

Tabla 4. Selección de técnicas computacionales

3.3.3. CUADRO COMPARATIVO DE VECTORES DE ATAQUES EN INGENIERÍA SOCIAL NO COMPUTACIONALES

VECTOR DE ATAQUE	DESCRIPCIÓN	DIRIGIDO	EFICIENCIA
Smishing	Ataque de Phishing realizado a través de un SMS, El contenido del mensaje invita a pulsar en un link que lleva a una web maliciosa.	Estos SMS generalmente se hacen pasar por servicios habitualmente usados en la población, comúnmente bancos o servicios de reparto.	**ALTA**
Vishing	Ataque de Phishing realizado por teléfono o a través de un sistema de comunicación por voz. El cibercriminal se pone en contacto con la víctima a través de una llamada, haciéndose pasar por un servicio técnico, le pide a la víctima determinados requisitos para resolver la incidencia.	Víctima a través de una llamada	**MEDIA**

VECTOR DE ATAQUE	DESCRIPCIÓN	DIRIGIDO	EFICIENCIA
Spear phishing	El atacante emplea técnicas de OSINT para obtener toda la información disponible sobre la víctima, y de esta forma modelar y dirigir el ataque hacia esta.	Ataque de Phishing concretamente dirigido a una víctima o conjunto de víctimas.	**MEDIA**
	Los ciber atacantes consideran a los ejecutivos "High level" como "whales" de ahí el nombre del ataque.	Phishing, donde cuyo objetivo es un "peso pesado" de la organización.	**MEDIA**
Dumpster Diving	Acción de "bucear" en la basura de una organización para obtener información de documentos que iban a ser reciclados.	Dirigida a la organización	**BAJA**

VECTOR DE ATAQUE	DESCRIPCIÓN	DIRIGIDO	EFICIENCIA
Shoulder surfing	Su nombre es muy descriptivo, ya que hace referencia a mirar por encima del hombro (para conseguir información).	Dirigida a victima en específico.	**MEDIA**
Tailgating	Consiste en seguir a una persona, para acceder con ella a una zona de acceso restringido. Esta técnica se basa en la generosidad de las personas, ya que por cortesía se suele aguantar de la puerta a quien viene detrás.	Dirigida a victima en específico.	**MEDIA**
Eliciting information	Algunas de estas técnicas de comunicación son: escucha activa, Preguntas reflexivas o utilizar afirmaciones falsas (Para que el objetivo corrija con la info que interesa). De esta forma, en una conversación aparentemente casual, el atacante irá «tirando de la lengua» al objetivo y conseguirá información.	Dirigida a victima en específico.	**BAJA**

VECTOR DE ATAQUE	DESCRIPCIÓN	DIRIGIDO	EFICIENCIA
Identity Fraud	Una usurpación de identidad es apropiarse de la identidad de otra persona generalmente con la intención de poder acceder a recursos y tener beneficios en nombre de la otra persona.	Dirigida a victima en específico.	**MEDIA**
Invoice Scams	La estafa de las facturas falsas se produce cuando el atacante envía una factura fraudulenta a su objetivo, de manera que este, sino la revisa atentamente puede llegar a pagar la cantidad que se pide en la factura.	Dirigida a victima en específico.	**MEDIA**
Reconnaissance	Los cibercriminales recopilarán toda la información disponible sobre el objetivo, para de este modo poder personalizar y dirigir el ataque.	Dirigida a victima en específico.	**MEDIA**

VECTOR DE ATAQUE	DESCRIPCIÓN	DIRIGIDO	EFICIENCIA
Hoax	Son peligrosos porque intentan manipular a la víctima para que haga alguna acción en su equipo que lo deje desprotegido o incluso inservible. Estos ataques se basan una vez más en el miedo.	Dirigida a victima en específico. Suelen estar constituidos por 3 partes reconocibles: **Gancho:** Sirve para captar la atención de la víctima y que lea el mensaje. **Advertencia:** Enumera los peligros que hay si la víctima no reacciona o hace algo de inmediato. Juega con el miedo **Petición:** Pide una acción para resolver el problema, y a mayores darle difusión al mensaje (Así el bulo sigue circulando)	**ALTA**

Tabla 5. Cuadro comparativo de vectores de ataques con técnicas no computacionales

3.3.4. SELECCIÓN DE TÉCNICAS NO COMPUTACIONALES

VECTOR DE ATAQUE	DESCRIPCIÓN	DIRIGIDO	EFICIENCIA
Shoulder surfing	Su nombre es muy descriptivo, ya que hace referencia a mirar por encima del hombro (para conseguir información).	Dirigida a victima en específico.	**MEDIA**
Vishing	Ataque de Phishing realizado por teléfono o a través de un sistema de comunicación por voz. El cibercriminal se pone en contacto con la víctima a través de una llamada, haciéndose pasar por un servicio técnico, le pide a la víctima requisitos para resolver la incidencia.	Víctima a través de una llamada	**MEDIA**

Tabla 6. Selección de técnicas no computacionales

3.4. IMPLEMENTACIÓN DE TÉCNICAS DE INGENIERÍA SOCIAL COMPUTACIONALES

3.4.1. DISEÑO Y EJECUCIÓN DE ATAQUES DE INGENIERÍA SOCIAL

Ataque 1. Vector de ataque empleado: Phishing

Iniciamos la aplicación Social Engineering toolkit desde un sistema operativo virtualizado, la cual mostrará este entorno de inicio.

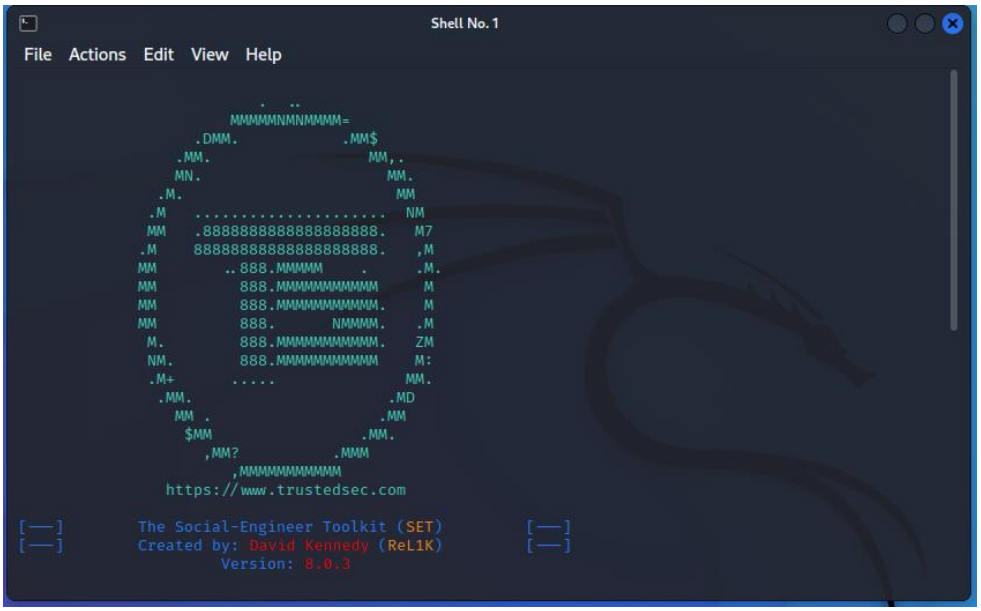


Figura 18. Entorno de inicio de SET

Luego se escogen las opciones para el ataque, que se realizará a la víctima.

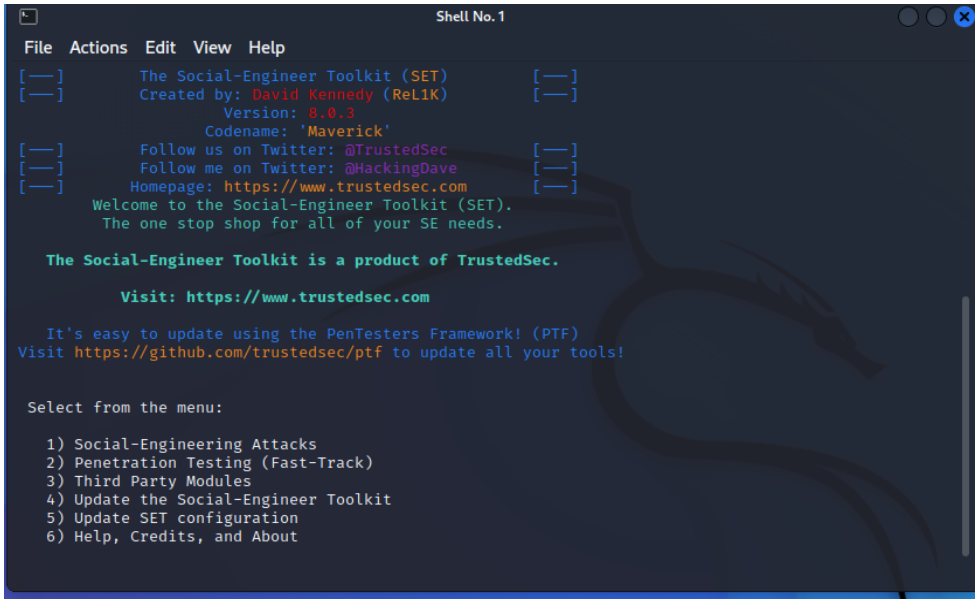


Figura 19. Opciones para el ataque

Se elige la opción 1, la cual es un ataque de ingeniería social.

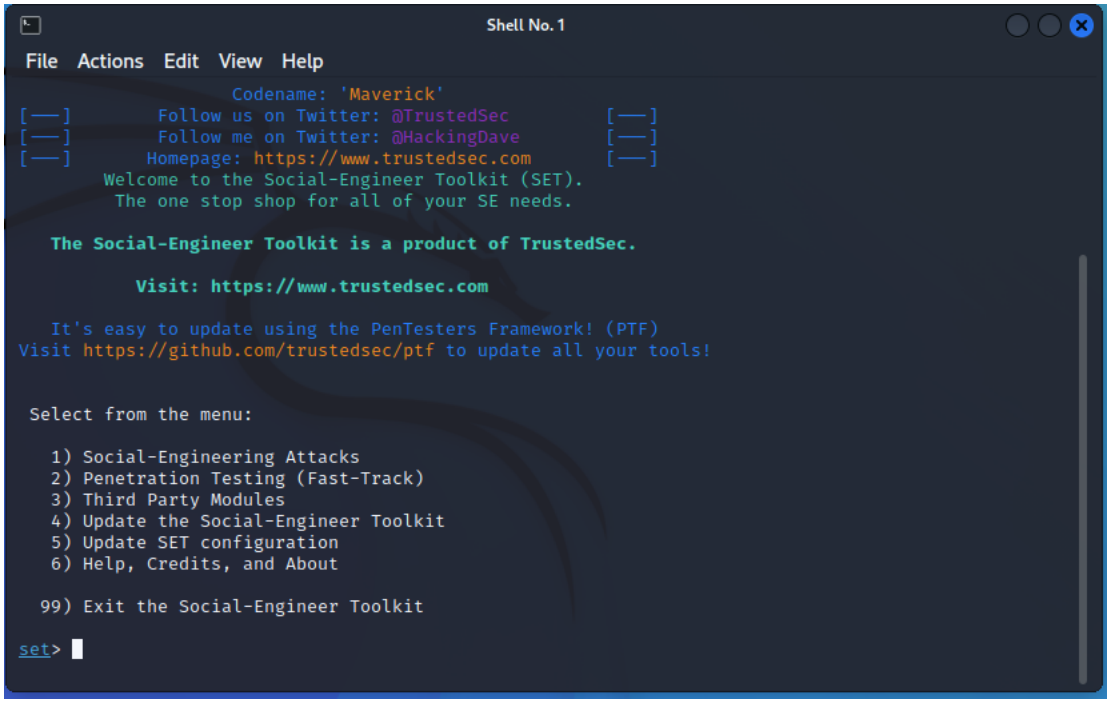


Figura 20. Escoger la opción de ataque de ingeniería social

Dará como resultado un segundo menú, en el cual se selecciona la opción 2: Penetration Testing.

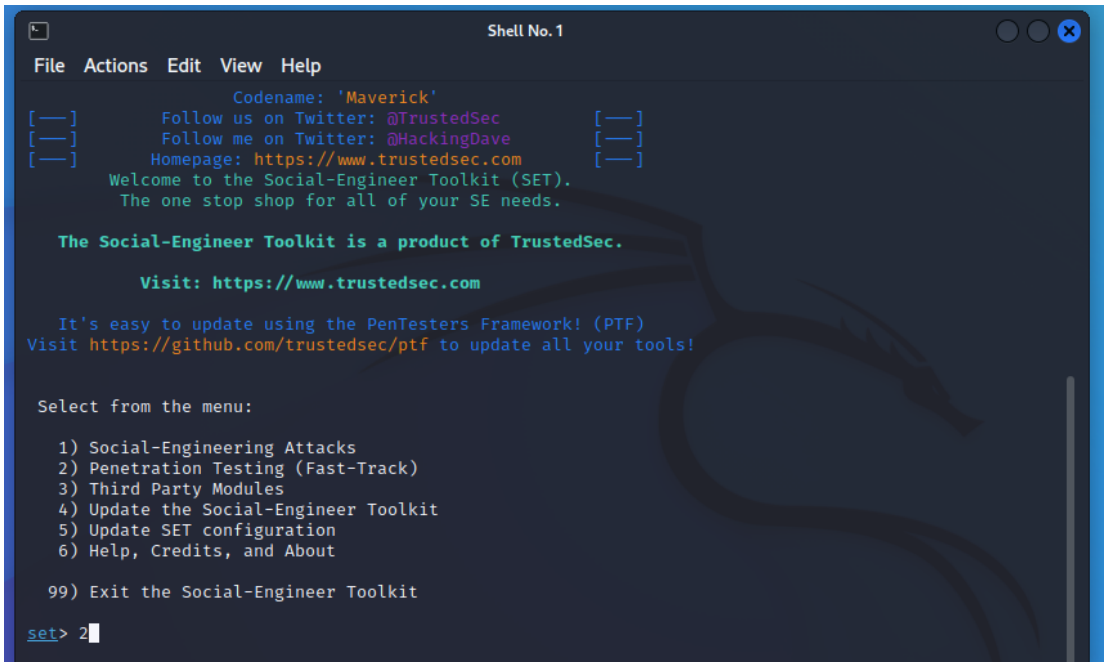


Figura 21. Opción 2, Penetration testing

Continuamente, se desplazará un tercer menú con múltiples opciones, en el cual se elegirá la opción 2: Website attack vector.

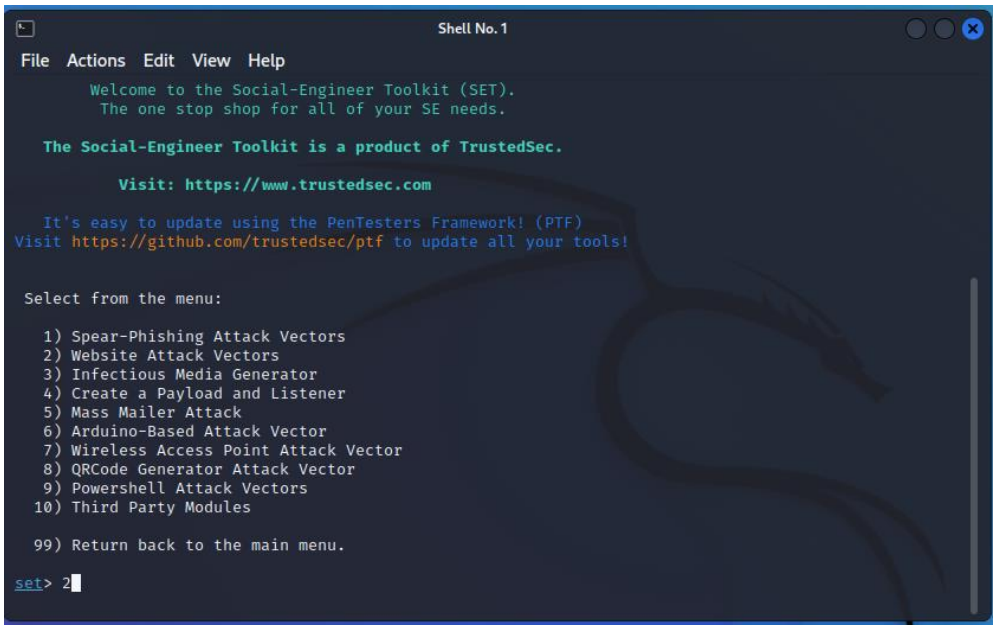


Figura 22. Opción 2, Website attack vector

En el siguiente menú, se seleccionará la opción 3: Credential harvester, attack metol, permitiendo clonar una página web que será subida a un servidor.

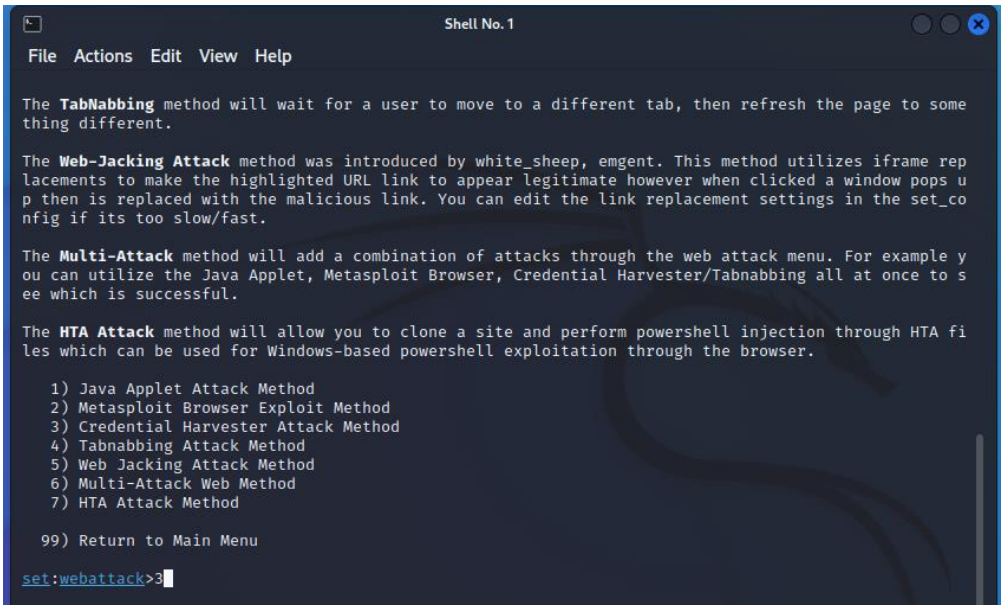


Figura 23. Opción 3, Credential harvester, attack metol

En el menú que se muestra a continuación, se determinará una opción entre tres, de las cuales, la primera es una web que viene por defecto, la segunda es una site cloner, que es poner el link para el sitio a clonar y la tercera es custom import, que es una página creada por autoría propia, en este caso se seleccionará la opción 2.

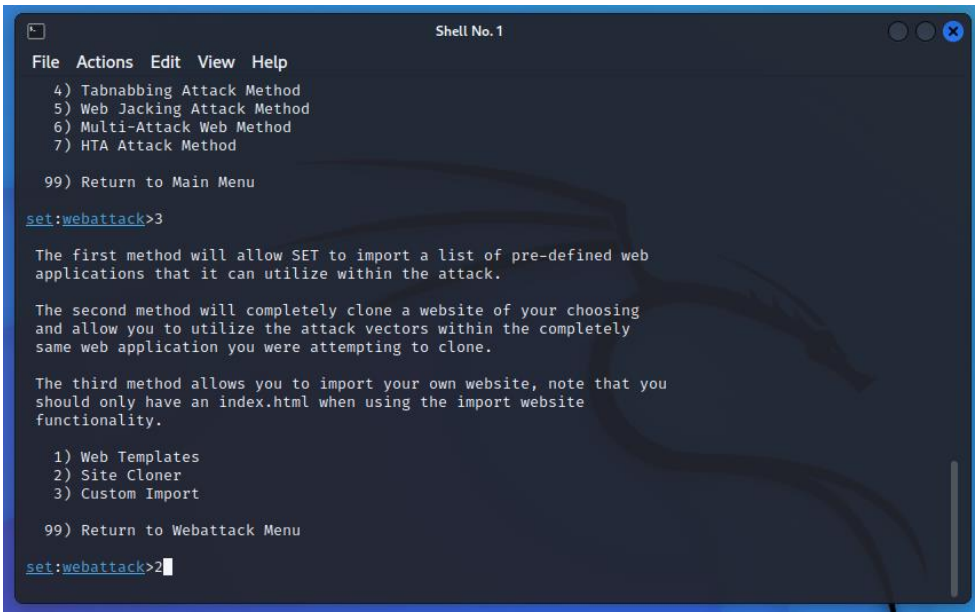


Figura 24. Opción 2, site cloner

A continuacion, pide que se ingrese la ip que recogerá los datos ingresados por las víctimas, comúnmente es la ip de la máquina creadora.

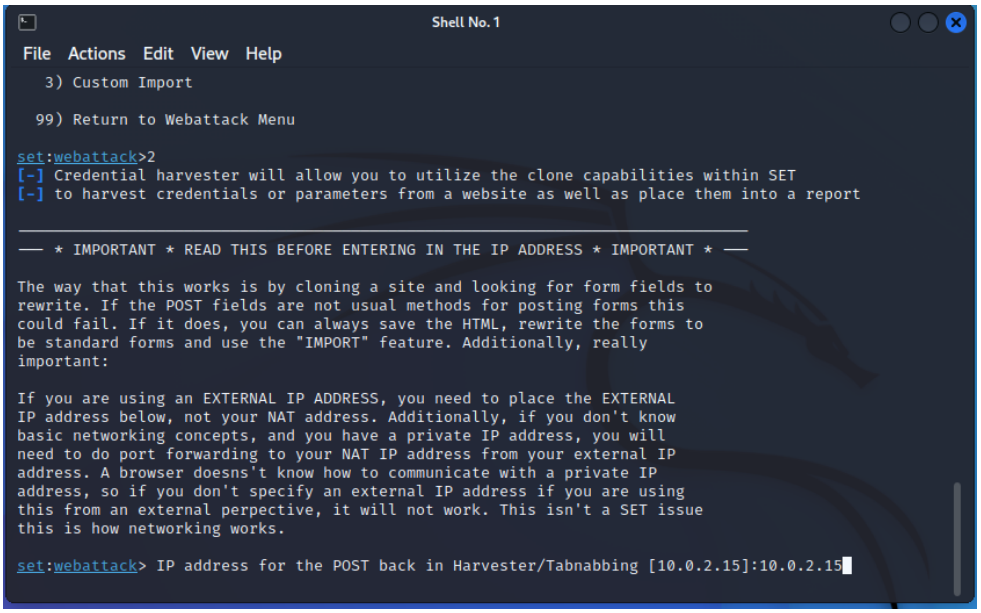


Figura 25. Ingreso de IP

Por último, se escribe la dirección de la página a clonar.

Figura 26. Escribir dirección de la página a clonar

Una vez ingresada la dirección, el sitio web solo se generará por defecto.

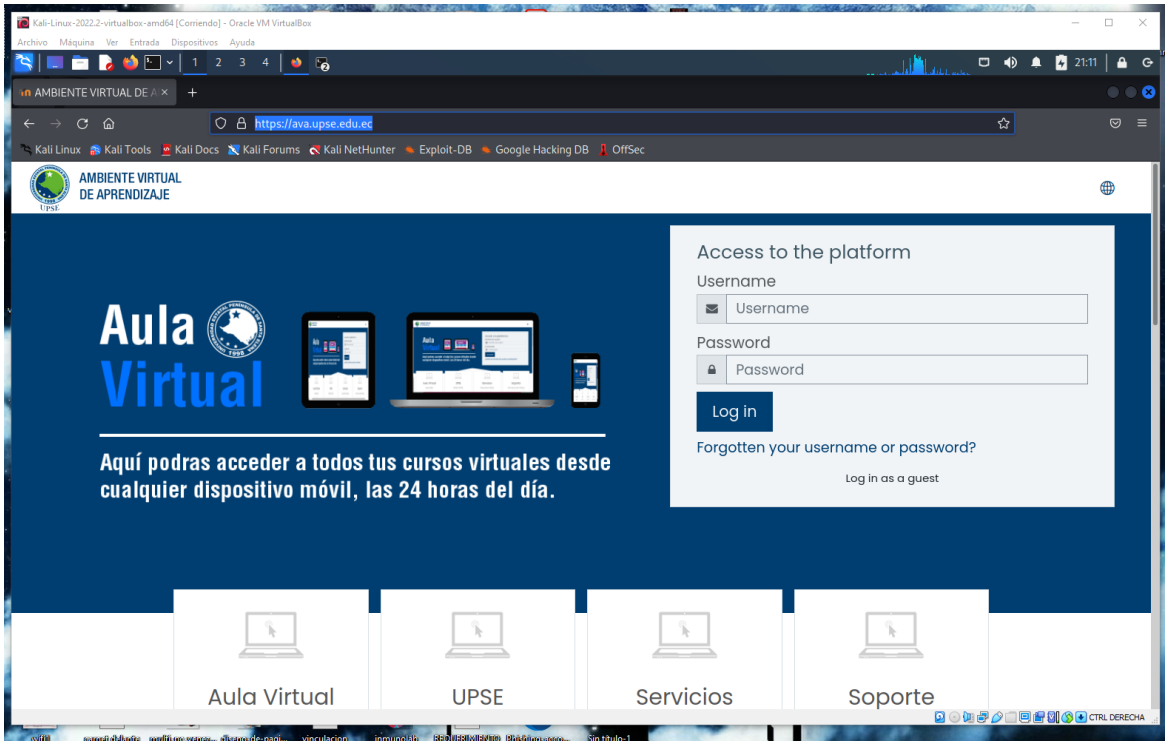


Figura 27. Sitio web se genera por defecto

Finalmente, se mostrará la información que afirma la creación de la página, encontrándose lista para agregarla a un servidor web y comenzar a enviar el link a las víctimas.

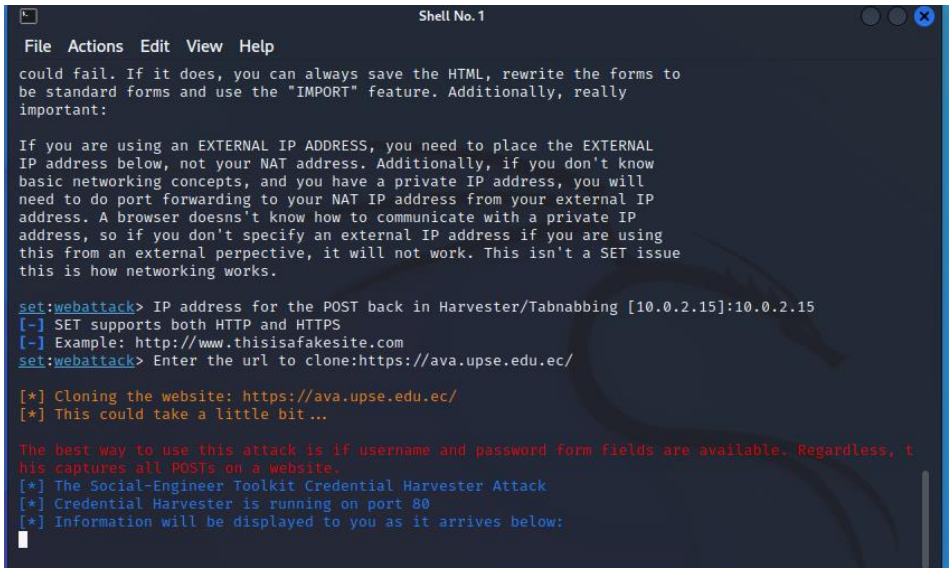


Figura 28. Creación de la página

Para la implementación de este vector de ataque en dicha institución, se realizó una encuesta en la que se propuso participar en este estudio y otorgando los permisos correspondientes por partes de las víctimas, aquellas recibieron el primer ataque llegándoles a sus respectivos correos un Qr generado para el mismo.

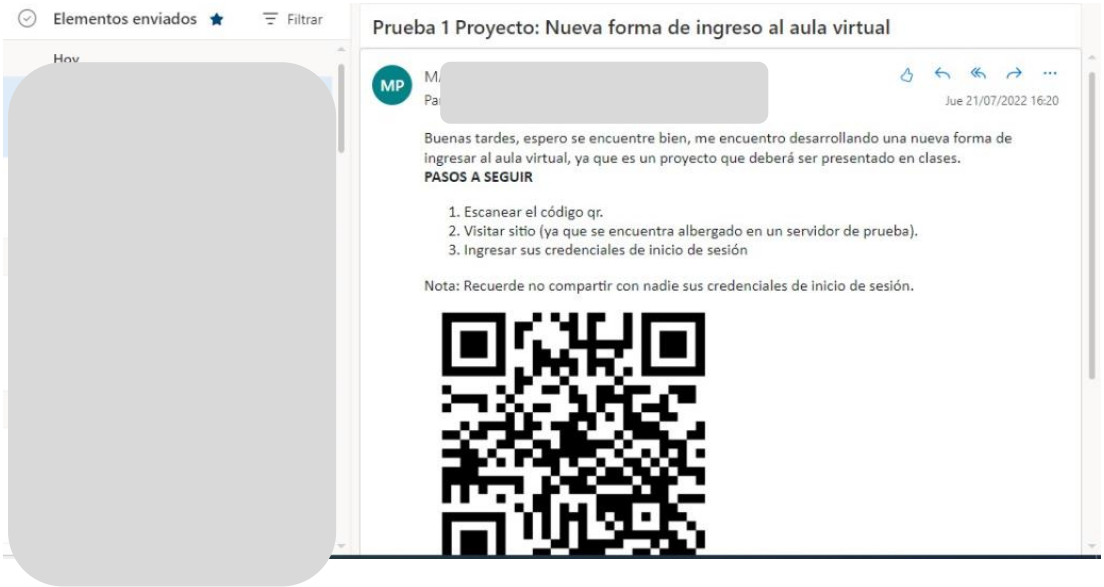


Figura 29. Correos con el QR generado

Ataque 2. Vector de ataque empleado: Medios infecciosos con archivos PDF o Exe.

Siguiendo la matriz inicial igual a la anterior se llega al segundo menú y se selecciona la opción 3.

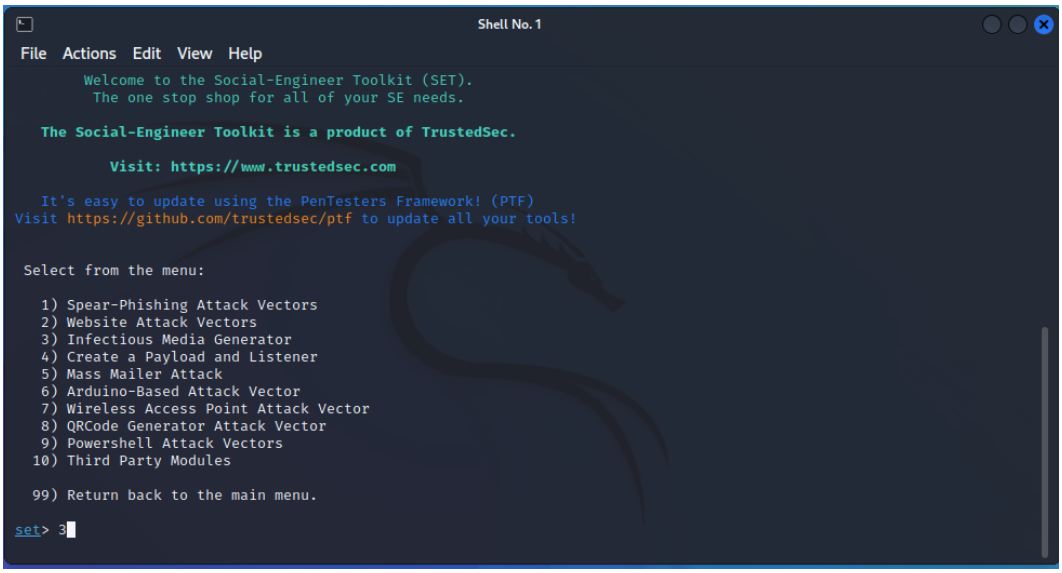


Figura 30. Opción 3, infección por medios generados

Siendo un medio generado nos permite usar 2 opciones por archivo o por Metaexploit se seleccionará la opción 1.

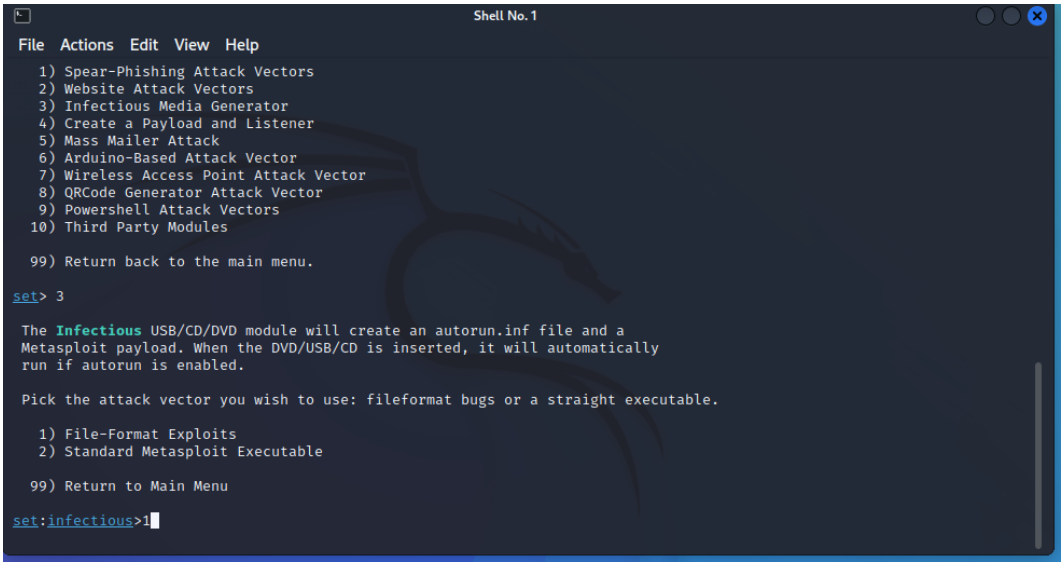


Figura 31. Opción 1, archivo de formato exploits

Luego nos solicitara que ingresemos la IP de destino de reverso del payload.

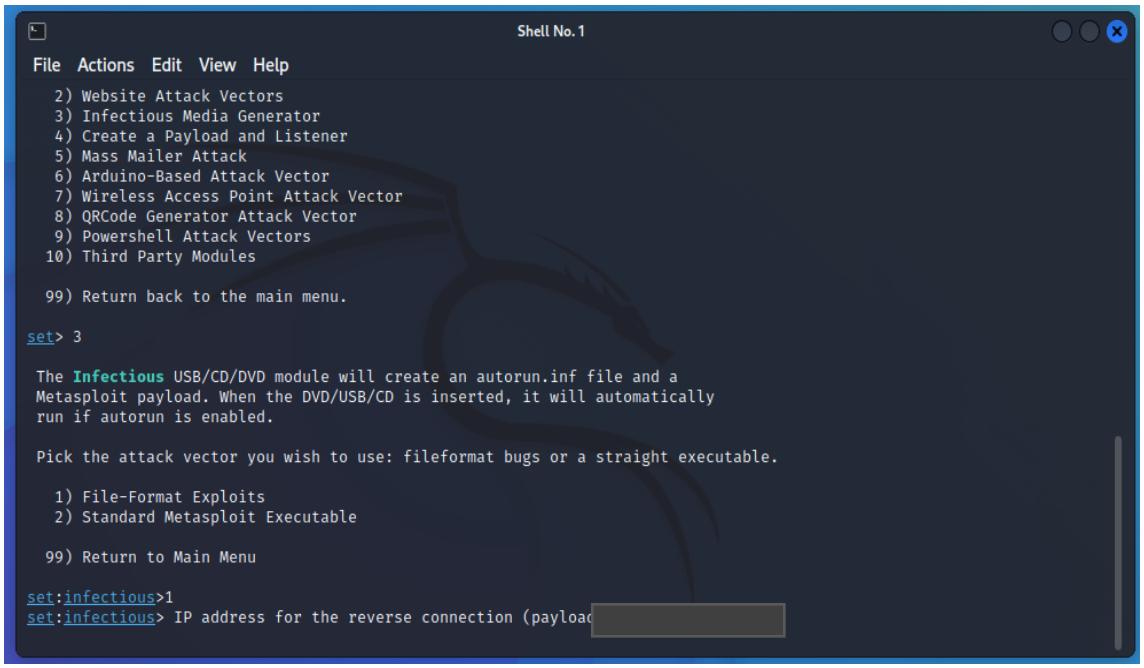


Figura 32. Ingreso de la IP

Se desplegará un listado con los diferentes tipos de ataque la cual se deberá seleccionar la opción 13.

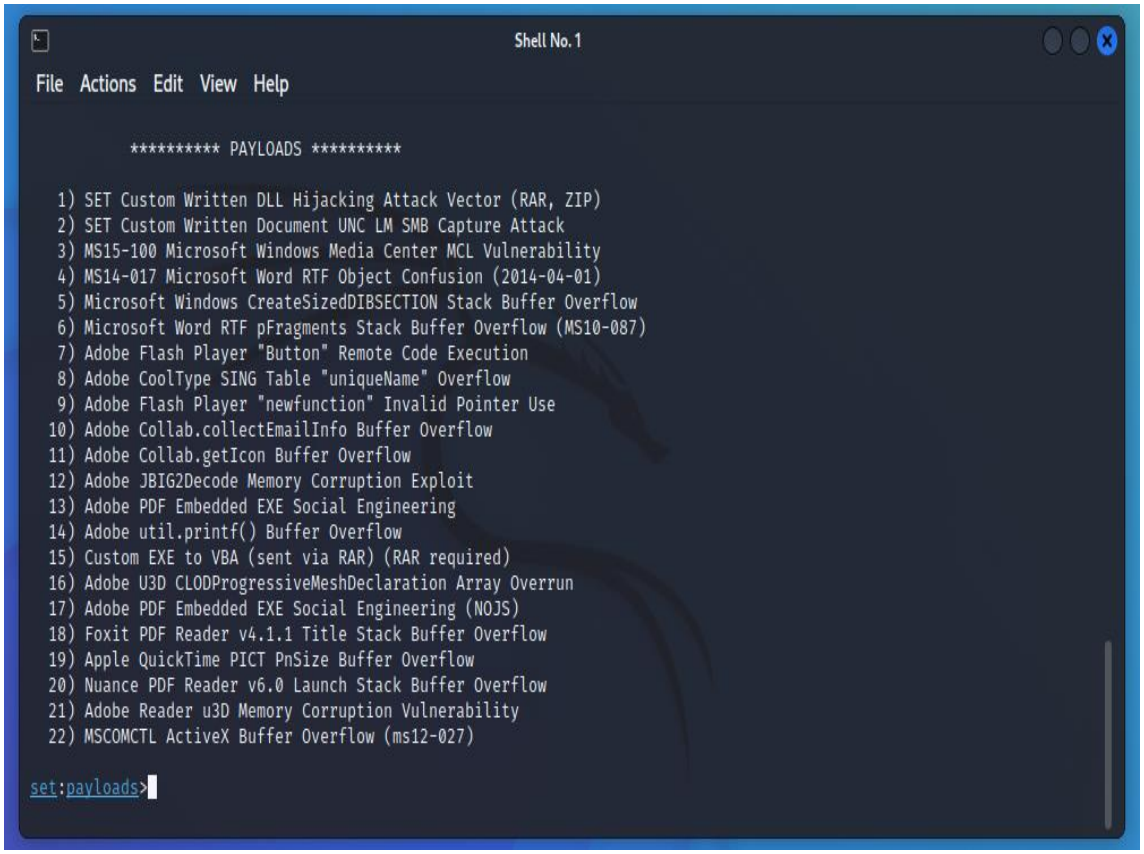


Figura 33. Opción 13, tipo de archivo PDF

Luego de seleccionar el PDF se seleccionará la opción 2.

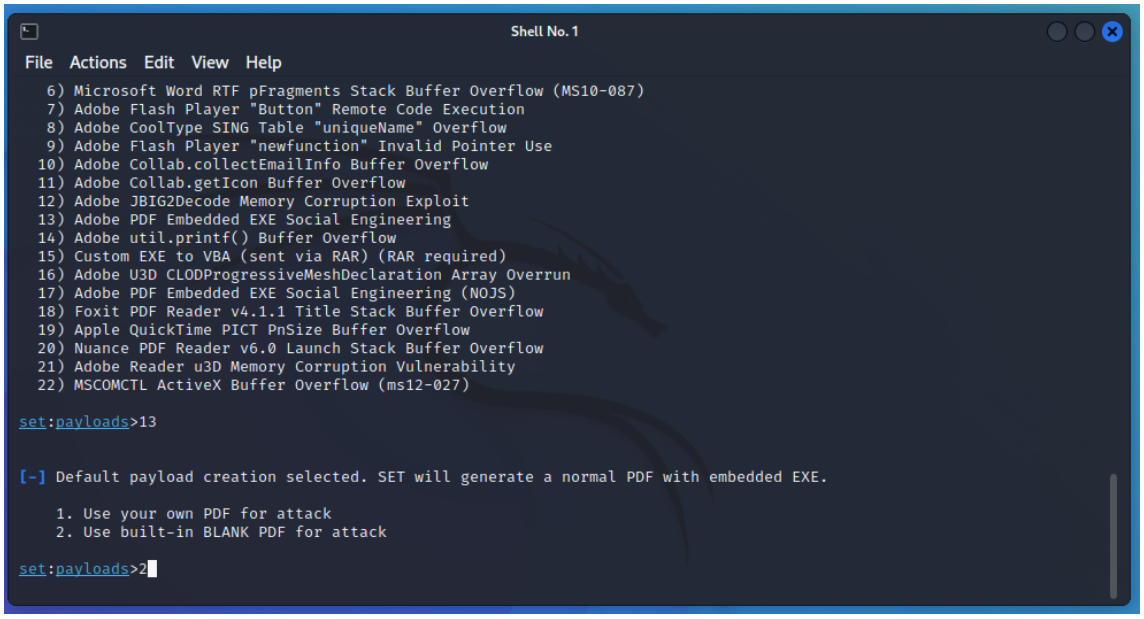


Figura 34. Opción 2, PDF en blanco

Por último, se seleccionará la opción 1 para que nos devuelva los datos de reverso en el ataque.

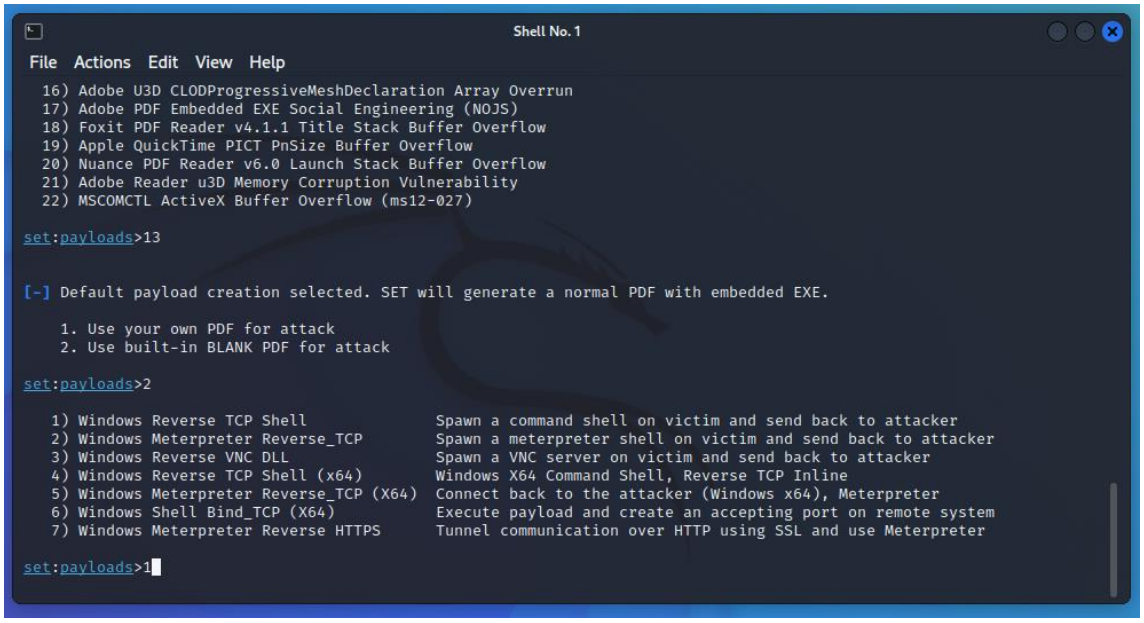


Figura 35. Opción 2, Método payload reverse TCP

Continuamente se escribirá el LHOST al que se dirigirá la IP.

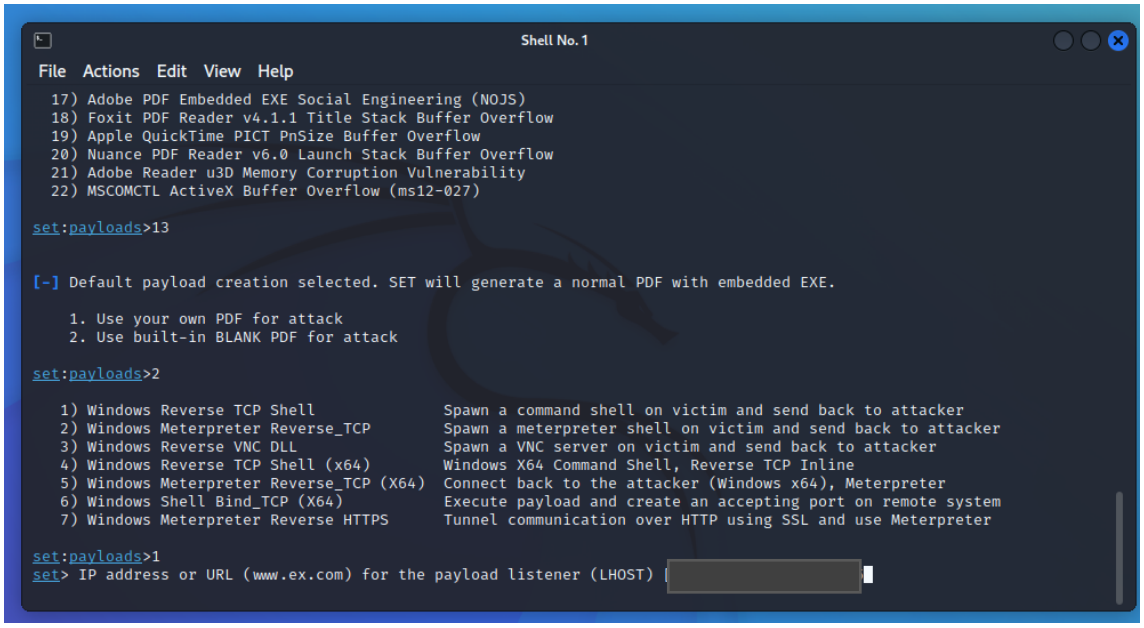


Figura 36. Ingreso de la IP

Luego de insertar la IP se insertará el puerto para determinar la entrada.

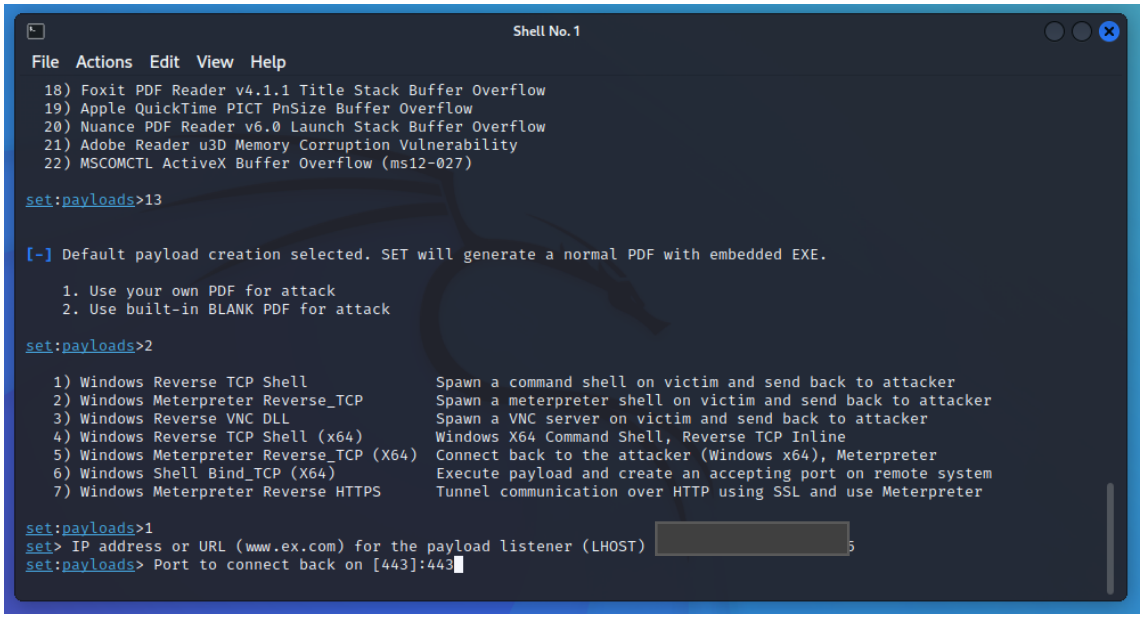


Figura 37. Ingreso del puerto de entrada

Una vez generada la IP y el puerto (cualquier puerto) se generará el archivo PDF para el ataque.

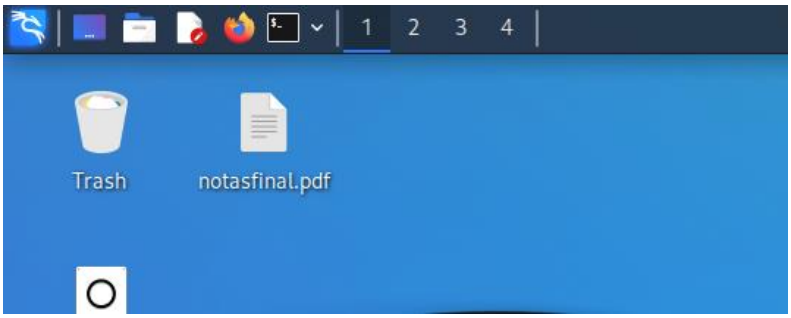


Figura 38. Archivo generado para el ataque

Para poder proceder con el proceso se genera un Metaexploit para la explotación del ataque generando el LHOST y el LPORT que ya se habían determinado.

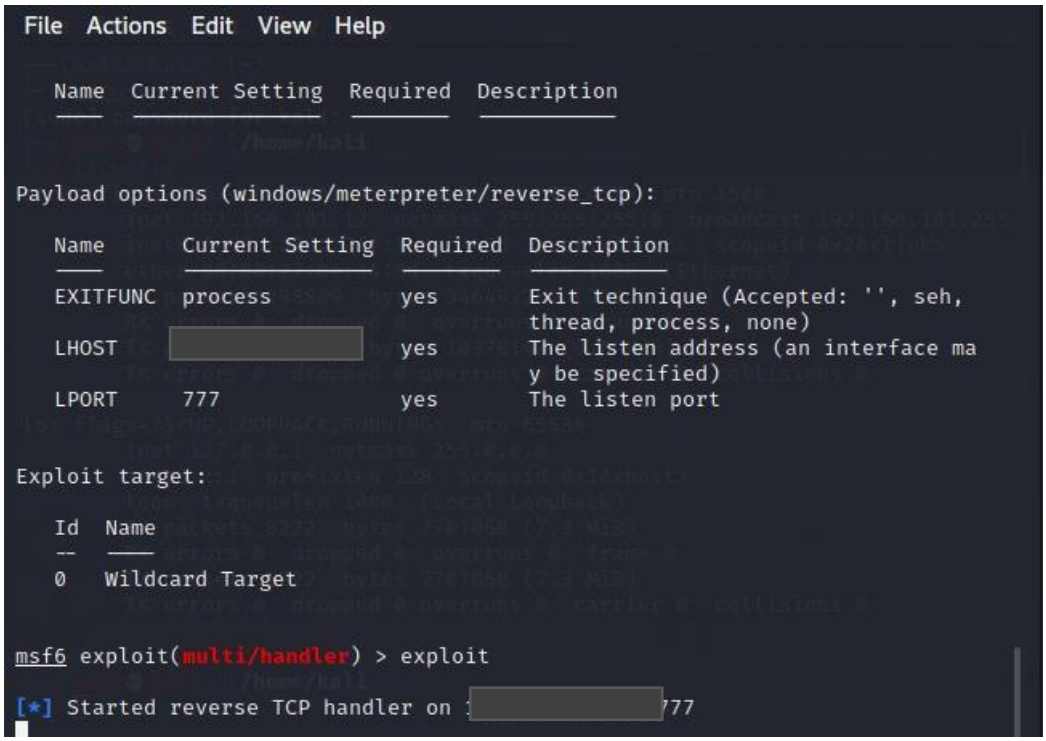


Figura 39. Ingreso set para LHOST y LPORT

El fin de este PDF es insertarlo en un USB para que la víctima pueda encontrarlo e incentivando por su curiosidad abrir el archivo para dar acceso a la explotación.

Ataque 3. Vector de ataque empleado: Phishing e ingeniería social por medio de redes sociales WhatsApp.

Iniciando del ataque anterior en la cual se creó una página phishing para obtener datos nos dispondremos a realizar la técnica que se utilizara para realizar este ataque.

Se selecciona la opción 8 que nos permitirá crear un QR que alojará el ataque que estamos creando.

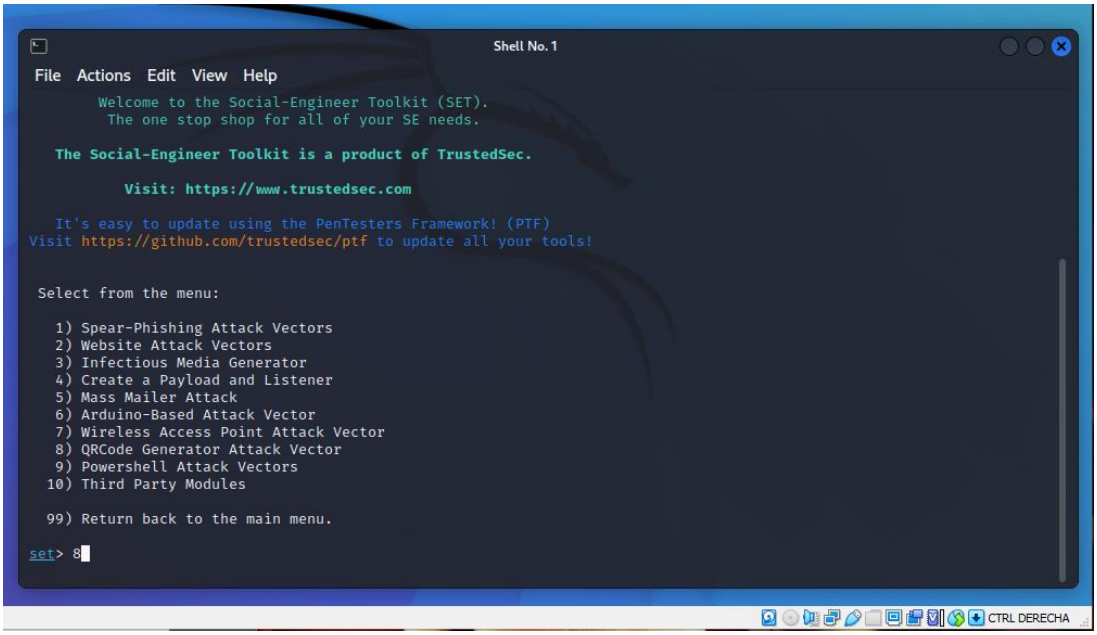


Figura 40. Opción 8 Generador de código QR

No pedirá que introduzcamos la IP con la que generamos la página web del phishing para realizar el respectivo ataque.

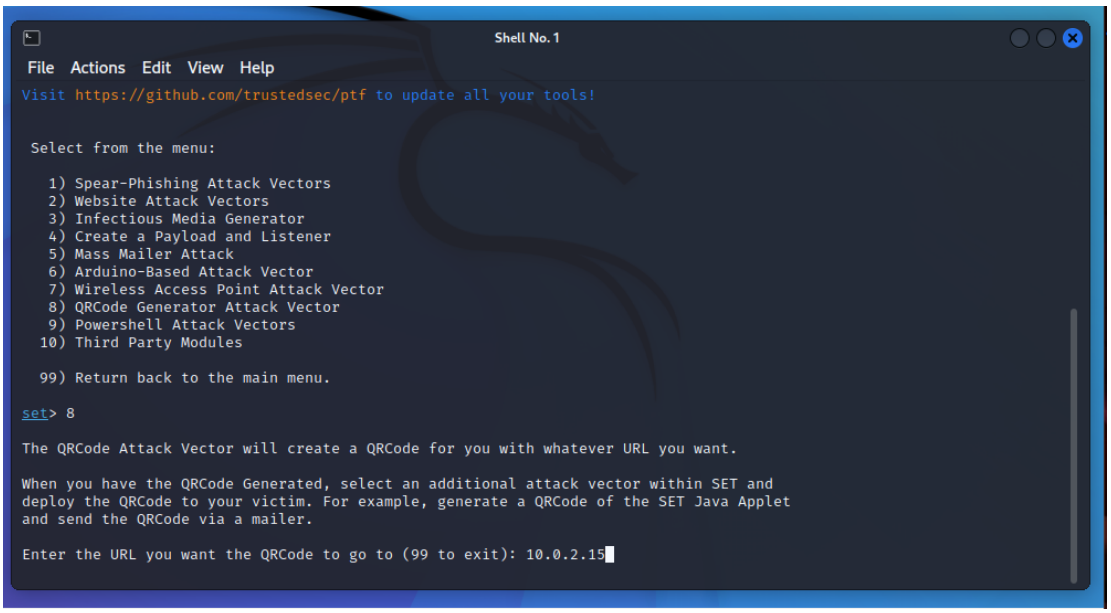


Figura 41. Ingreso de la IP

Luego de haber generado mostrara la dirección en donde se guardó la imagen del QR para poder copiarlo, como esta en una carpeta Root necesita privilegios de administrador.

Figura 42. Dirección del Código QR

No dirigiremos a la dirección donde se encuentra la imagen usada los codigos CD para abrir carpetas y LS para mostrar los archivos.

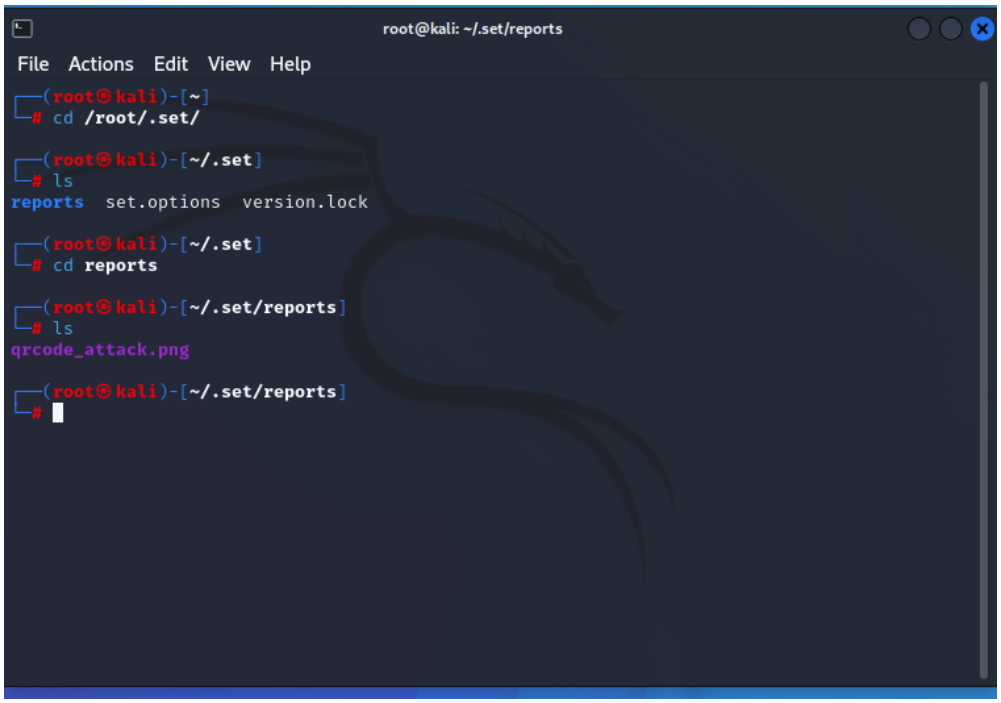


Figura 43. Ingreso al Root

Continumente procedemos a copiar el archivo en una direccion donde podremos verla sin autorizacion del administracion usando el codigo MV qu es para mover un archivo.

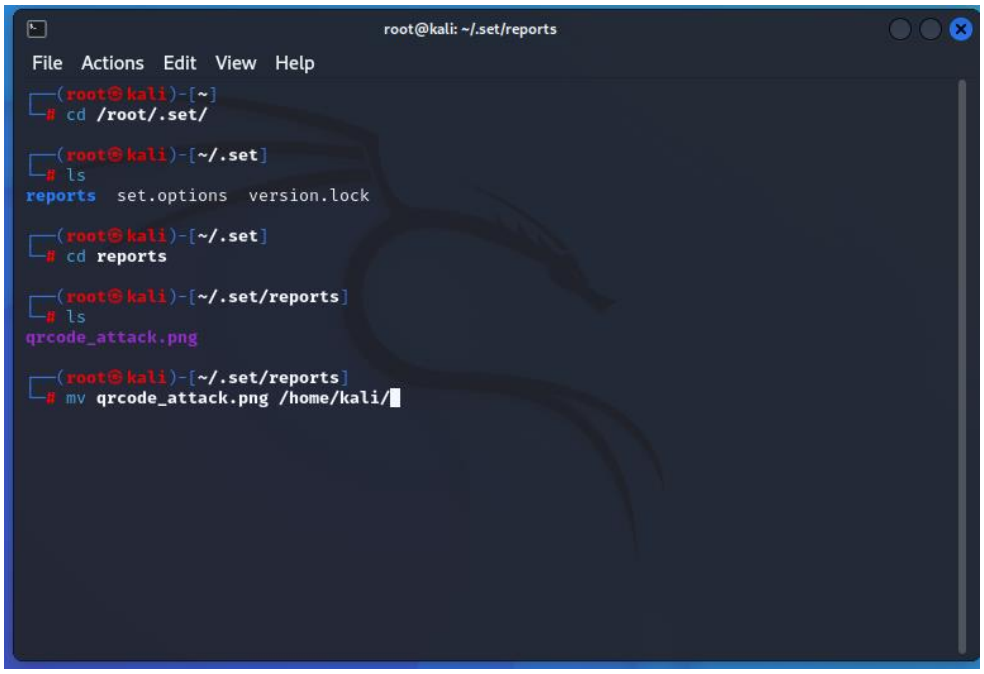


Figura 44. Redireccionar el archivo PNG

El archivo se trasladara a una direccion para poder observar el QR generadoy poder usaralo por medio de las redes sociales.

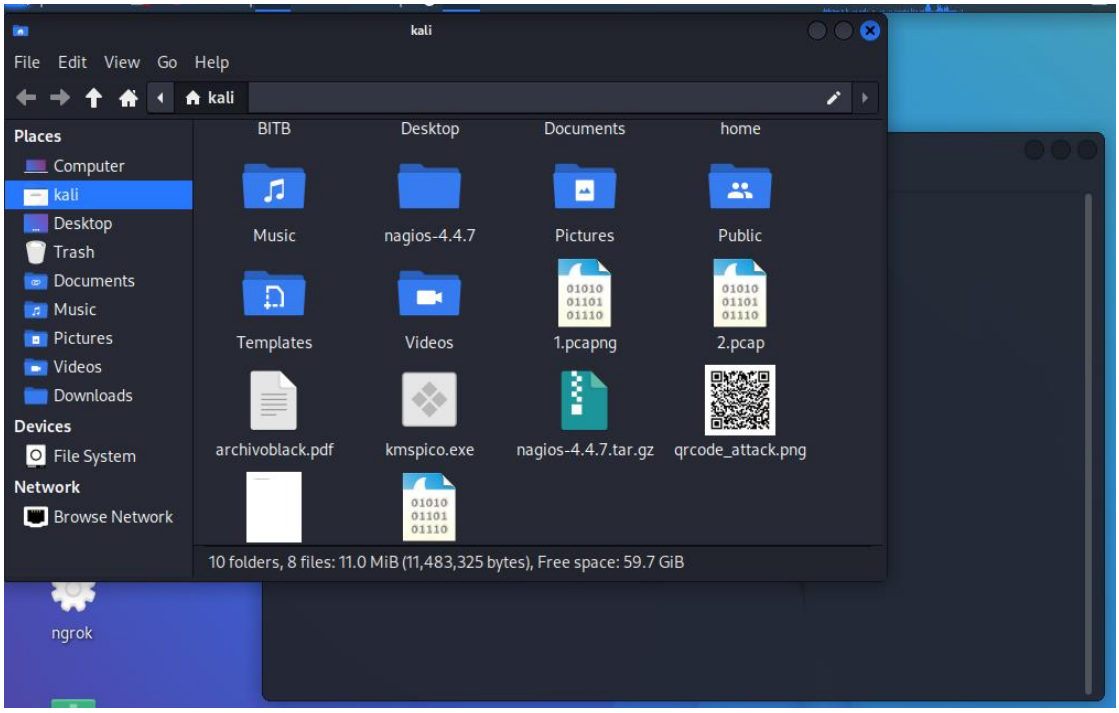


Figura 45. Imagen del Qr

Figura 46. QR

Una vez generado el ataque se procede a usar la red social WhatsApp para poder enviar el ataque usando un mensaje falso llamativo para la victima especificada.

Figura 47. Ataque por WhatsApp

3.5. IMPLEMENTACIÓN DE TÉCNICAS DE INGENIERÍA SOCIAL NO COMPUTACIONALES

Ataque 1. Vector de ataque empleado: Shoulder Surfing

ATAQUE SHOULDER SURFING	
Software escogido.	No necesita software.
Funcionamiento.	Obtener credenciales de inicio de sesión, solo con observar a la víctima mientras utiliza su dispositivo electrónico.
EJECUCIÓN DEL ATAQUE	
➢ En este caso, el atacante se posicionó en una línea de visión directa hacia la pantalla de su dispositivo móvil y logró observar la clave utilizada por el usuario, el atacante busca replicar la secuencia en una nueva sesión, pero el sistema generó una notificación por mensaje de texto al dispositivo móvil, en este caso el atacante no logra ingresar al sistema, reflejando que el algoritmo es robusto frente al Shoulder Surfing. ➢ Como se puede verificar este ataque para esta evaluación, son sencillos de ejecutar y no necesitan conocimientos avanzados en computación, es decir, cualquier persona puede aplicar estas técnicas para sustraer claves de acceso a diferentes sistemas.	

Tabla 7. Vector de ataque Shoulder Surfing

Ataque 2. Vector de ataque empleado: Vishing

ATAQUE VISHING	
Software escogido.	No necesita software.
Funcionamiento.	Se utiliza el teléfono como herramienta con el objetivo de receptar información de la víctima.
EJECUCIÓN DEL ATAQUE	
➢ En este ataque, por medio telefónico trata de convencerlo a que nos entregue sus credenciales de inicio de sesión o que ingrese a un sitio web clonado. ➢ El verdadero problema de este tipo de ataques es la confianza que la víctima tiene en el teléfono y en el uso que tradicionalmente han hecho de él, las empresas legítimas	

Tabla 8. Vector de ataque Vishing

3.6. ANÁLISIS DE RESULTADOS

3.6.1. EVALUACIÓN DE RESULTADOS DE EJECUCIÓN DE INGENIERÍA SOCIAL

Resultados del primer ataque computacionales.

Dentro de un tiempo determinado que estuvo abierto el ataque en la primera jornada de trabajo (Ver Anexo 8). Como resultado se obtuvo:

Resultados de ataque de vector por medio de clonación de página.			
Vector de Ataque		Phishing - Explotación con página web	
Horas Ejecutadas	4 horas	Cantidad de Víctimas	15 personas
Resultados		Observaciones	
De las 15 víctimas, 10 realizaron el trabajo. 2 de las víctimas no llenaron datos.		Entre las observaciones obtenidas en este primer ataque, se determinó que existe una cantidad de alumnos que cayeron en el mismo, 3 de las víctimas no respondieron dando a entender que no están atentos a su correo institucional y 2 previeron el ataque.	

Tabla 9. Datos de ataque Phishing

Resultados de ataque de generador de medios infecciosos (PDF).			
Vector de Ataque		Explotación por archivo PDF	
Horas Ejecutadas	5 horas	Cantidad de Víctimas	15 personas
Resultados		Observaciones	
De las 10 víctimas, 9 realizaron el trabajo. 5 de las víctimas no prestaron atención al archivo y 1 uno presto atención al USB.		Entre los resultados adquiridos en este ataque con un archivo PDF en un dispositivo USB, casi más de la mitad de las victimas cayeron, 5 de las víctimas no desconfiaron del archivo y simplemente no le prestaron atención y lo borraron, 1 persona no usó el USB.	

Tabla 10. Datos de ataque generado por medios PDF.

Resultados de ataque generado por redes sociales WhatsApp.			
Vector de Ataque		Técnica computacional y no computacional. Phishing - Explotación por mensaje texto en WhatsApp (QR)	
Horas Ejecutadas	3 horas	Cantidad de Víctimas	15 personas
Resultados		Observaciones	
De las 15 víctimas, 12 realizaron el trabajo. 2 de las víctimas no se redireccionaron con el QR y 1 elimino respondió que detecto el virus.		Entre las observaciones obtenidas en este mensaje con código QR, se determinó que los alumnos se sintieron tentado por la propuesta de una beca, 3 de las víctimas no respondieron dando a entender previeron el ataque.	

Tabla 11. Datos de ataque generado por redes sociales WhatsApp.

Resultados del primer ataque no computacionales.

Dentro de un tiempo determinado que se trabajó en campo para el análisis de potenciales víctimas por todo un campus (Ver Anexo 9). Como resultado se obtuvo:

Resultados para la técnica de Shoulder surfing.			
Vector de Ataque		Shoulder surfing – Ver sobre el hombro	
Horas Ejecutadas	8 horas	Cantidad de Víctimas Seguidas	25 personas
Resultados		Observaciones	
De las 25 víctimas se concluyó: 6 abrieron Facebook. 5 WhatsApp 2 Tiktok. 4 aulas virtuales. 3 de las víctimas se pudo determinar sus claves y contraseñas del aula virtual.		Entre las observaciones obtenidas durante este trabajo de campo se determinó que, en el caso de las redes sociales, los dispositivos móviles por defecto guardan contraseñas impidiendo el reconocimiento de las mismas al usar esta técnica no computacional a diferencia del aula que por defecto solicita clave del mismo.	

Tabla 12. Datos de ataque usando técnica Shoulder Surfing.

Resultados para la técnica de Vishing.			
Vector de Ataque		Vishing – Llamada telefónica	
Horas Ejecutadas	4 horas	Cantidad de Víctimas Seguidas	5 personas
Resultados		Observaciones	
3 de las víctimas potenciales contestaron, pero no se obtuvo resultados favorables. 2 se las llamó para pruebas con el Qr.		En las llamadas realizadas las personas desconfiaron demasiado impidiendo que nos den información necesaria. En las pruebas obtenidas con el Qr, las víctimas fueron comprometidas con sus datos.	

Tabla 13. Datos de ataque usando técnica Vishing.

3.7. INFORME DE RESULTADOS

Resultados de ataque de vector por medio de clonación de página

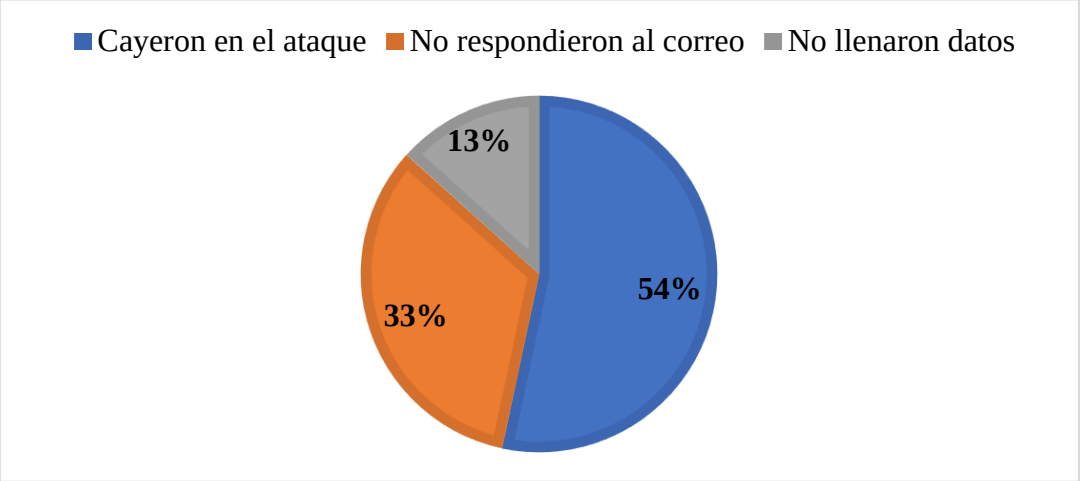


Figura 48. Gráfico estadístico del ataque de vector por medio de clonación de página

Con el ataque de vector por medio de clonación de página, se pudo determinar que, existe una cantidad de estudiantes que cayeron en el mismo, el 54% de las víctimas brindaron información sensible, además, el 33% no revisa su bandeja de entrada, razón por la cual, no respondieron al correo y el 13% de las personas, ingresaron a la página, pero no llenaron datos.

Resultados de ataque de generador de medios infecciosos (PDF).

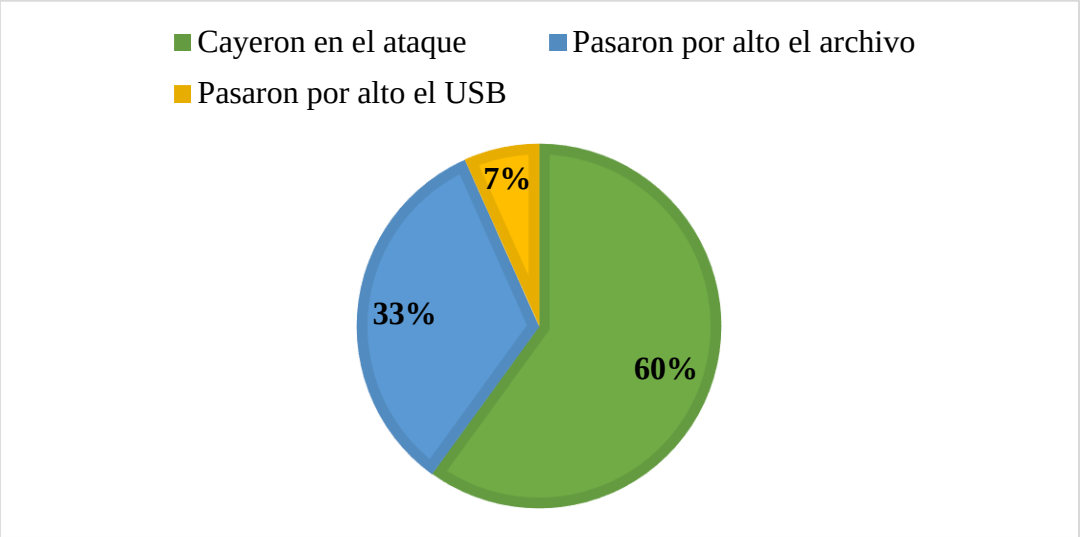


Figura 49. Gráfico estadístico del ataque de generador de medios infecciosos (PDF)

En el ataque de generador de medios infecciones mediante PDF, se pudo obtener que, el 60% de los colaboradores en este proyecto cayeron en el ataque, el 33% pasaron por alto el archivo y el 7% pasaron por alto el USB.

Resultados de ataque generado por redes sociales WhatsApp.

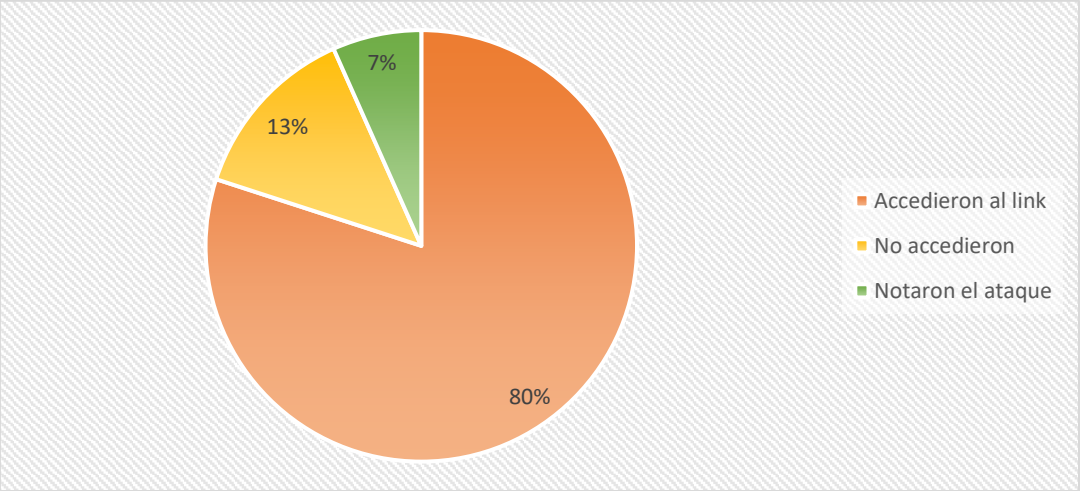


Figura 50. Gráfico estadístico del ataque generado por redes sociales WhatsApp

El ataque generado por redes sociales tuvo gran éxito, ya que. El 80% de las personas accedieron al link que se les envió a través de un código QR, así mismo, el 13% de los usuarios, desconfiaron del enlace, razón por la cual, no accedieron y el 7% fueron precavidos y notaron el ataque.

Resultados para la técnica de Shoulder surfing.

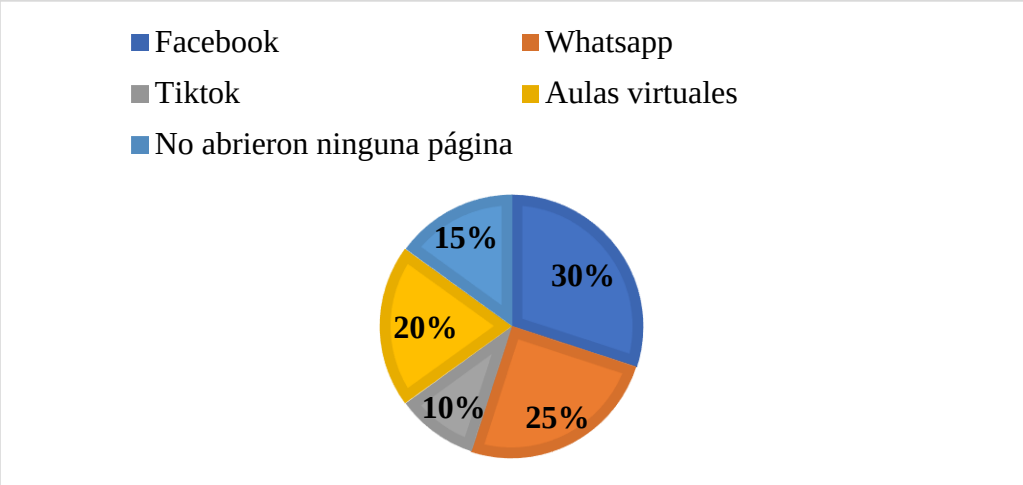


Figura 51. Gráfico estadístico de ataque Shoulder Surfing.

En la técnica empleada de Shoulder Surfing, se pudo obtener que, el 30% de las personas abrieron Facebook, 25% WhatsApp, 20% aulas virtuales, 10% Tiktok y el 15% no abrieron ninguna página. Con este ataque se determinó que, las redes sociales por defecto guardan las contraseñas, lo que impidió que las víctimas ingresaran las mismas por teclado, sin embargo, en el aula virtual si registran la clave en cada inicio de sesión, por lo que se pudo obtener 3 contraseñas.

Resultados para la técnica de Vishing.

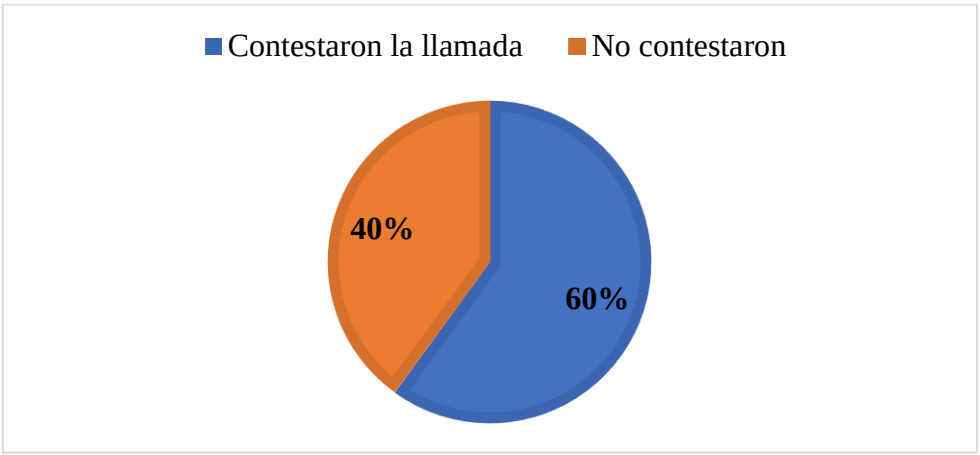


Figura 52. Gráfico estadístico de ataque Vishing.

En la técnica de Vishing, el 60% de las personas contestaron la llamada, pero no brindaron información sensible y el 40% de las víctimas no respondieron.

4. PROPUESTA DE BUENAS PRÁCTICAS PARA SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN

4.1. INTRODUCCIÓN

La ingeniería social posee técnicas computacionales y no computacionales, que buscan confundir a las víctimas mediante mentiras y engaños, de esta forma, conseguir información personal que les permita acceder a sus cuentas electrónicas o a sus dispositivos. En el presente trabajo, se realizaron varios ataques a una institución de educación superior, que evidenciaron las vulnerabilidades en los usuarios.

Esta guía tiene como finalidad, concientizar a las personas y presentar diversas recomendaciones que se pueden ejecutar, para mitigar los riesgos de un futuro ataque y reforzando la seguridad informática. Para esto, se utilizarán las normas ISO27001, que se basan en la clasificación dependiendo de las características de la seguridad de la información, las cuales se nombran a continuación:

- **Disponibilidad:** Acceso a los datos cuando se requieran, teniendo en consideración la privacidad.

- **Confidencialidad:** Información sensible solo para las personas autorizadas. Dichos datos no deben llegar a terceros que no estén autorizados.

- **Integridad:** Información correcta sin ser modificada por personas no autorizadas. Se protege frente a vulnerabilidades externas.

- **Autenticación:** Datos procedentes de un usuario que es quien dice ser. Además, se verifica y se garantiza que el origen de la información es correcto.

4.2. PRÁCTICAS DE SEGURIDAD

Disponibilidad	
Práctica de seguridad	**Descripción**
Utilizar cortafuegos.	Teniendo una buena gestión de cortafuegos, se evitan caídas de sistema que permitan accesos ilegítimos. Para esto, se deben seguir los siguientes pasos:

	- Proteger adecuadamente las conexiones en los equipos electrónicos. - La configuración del cortafuegos debe revisarse periódicamente. - Establecer procesos adecuados de gestión y supervisión del cortafuegos.
Realizar copias de seguridad de la información.	Es importante mantener a salvo la información que se posee en los dispositivos electrónicos. Por esta razón, se recomienda regularmente realizar copias de seguridad apropiadas de la información. Se pueden realizar mediante un disco externo, guardar datos en la nube o en sitios remotos de la red.
Actualizaciones de parches de seguridad.	Para mantener disponible la información de forma correcta, se requiere tener actualizados todos los parches de seguridad en el sistema operativo, esto permite que los equipos electrónicos estén constantemente en monitoreo de los datos del dispositivo. La actualización de los parches de seguridad se debe realizar con licencias oficiales.

Tabla 14. Disponibilidad

Confidencialidad	
Práctica de seguridad	**Descripción**
Información sensible.	No compartir información sensible en las redes sociales, que permita a las personas saber datos personales sobre usted.

Contraseñas diferentes.	Al momento de crear distintos usuarios en diversas cuentas electrónicas, es importante tener diferentes claves para el registro de cada cuenta, asegurando la información que se posee.
Cambio de claves.	Se recomienda crear contraseñas fuertes y tener un tiempo de caducidad para las mismas, es recomendable que las claves sean cambiadas con frecuencia.
Monitorear las cuentas electrónicas.	Se debe monitorear constantemente todos los perfiles sociales y cuentas bancarias, para confirmar que toda la información esté en orden.
Clave de ingreso al dispositivo.	Es importante poseer una clave de ingreso al dispositivo, que evite el acceso no autorizado a la información que posee en los equipos electrónicos. Esta práctica de seguridad se puede realizar a través de la configuración del dispositivo.

Tabla 15. Confidencialidad

Integridad	
Práctica de seguridad	**Descripción**
Actualización del software.	Para asegurar la integridad de la información, sin que sea modificada, es importante tener actualizado el software de nuestro dispositivo electrónico, ya sea: computadora, teléfono móvil o tablet, así mismo, mantener actualizado el antivirus del equipo constantemente, evitando archivos maliciosos.
	Esta práctica es muy importante, ya que permite que no se recuerden las credenciales de acceso de las plataformas.

Eliminar historial y caché.	Para eliminar el caché de la computadora, se deben seguir los siguientes pasos: 1. Abrir el navegador. 2. En la esquina superior derecha, hacer clic en Más. 3. Haz clic en Más herramientas. 4. En la parte superior, elegir un intervalo de tiempo. 5. Marcar las casillas junto a "Cookies y otros datos de sitios" e "Imágenes y archivos almacenados en caché". 6. Haz clic en borrar datos.
Evitar conectarse a redes externas.	En caso de requerir conexión a internet, debe evitar en lo posible conectarse a redes wifi-desconocidas o públicas para navegar por internet. Para verificar si una red es segura, debe seguir los siguientes pasos: 1. Si la red es abierta, es recomendable no utilizarla. 2. Utilizar redes con cifrado WPA2. 3. Verificar si pide varios datos personales para poder conectarse. 4. Si ese es el caso, abandonar la red inmediatamente.
Utilizar una VPN.	VPN (Red Privada Virtual), ayuda a tener una conexión a internet segura y protegida. Para usar una VPN, solo tiene que seguir los siguientes pasos: 1. Registrarse para obtener un servicio de VPN en una página confiable.

	2. Descargar la VPN y ejecutar la aplicación. 3. Seleccionar un servidor al que desee conectarse. 4. Ahora puede navegar en internet de forma segura.
Instalar aplicaciones seguras.	La instalación de software puede afectar la seguridad y el rendimiento del equipo. Por esta razón, es recomendable utilizar aplicaciones legítimas.
Restringir el uso de dispositivos extraíbles.	Es importante no permitir el uso de dispositivos extraíbles, tales como: CD, pendrive, memorias, entre otros. Para emplear estos dispositivos es importante aplicar procedimientos que garanticen que no contienen malware. Se pueden seguir los siguientes pasos: 1. Verificar que el software antivirus esté funcionando. 2. Utilizar un programa para detectar que el dispositivo no contenga virus. 3. Iniciar la búsqueda de virus, dejar que el programa detecte y quite cualquier infección.
Utilizar sistemas de detección y prevención de intrusiones.	Siempre que sea posible, es importante utilizar herramientas que permitan la detección y prevención de intrusiones para proporcionar una visión detallada de la actividad de la red. Estas herramientas se deben adaptar al entorno de control de procesos.

Cifrado de datos	Se recomienda utilizar el cifrado de datos para garantizar que la información de un sistema de una computadora no pueda ser robada ni leerla alguien que quiera utilizarla con fines maliciosos. Implica convertir texto sin formato legible por humanos en un texto incomprensible.
Firma electrónica	Para evitar la vulneración de datos en internet, es recomendable emplear la firma electrónica, ya que tiene los cuatro principios: - Identidad: Verifica y confirma la identidad del titular de la firma. - Confidencialidad: El emisor sabe que la información del documento fue cifrada y que solo el receptor es capaz de descifrarlo. - No repudio: El firmante no puede rechazar que ha firmado un documento. - Integridad: Permite la encriptación y protección de los datos.

Tabla 16. Integridad

Autenticación y no repudio	
Práctica de seguridad	**Descripción**
Credenciales de acceso	Nunca entregar credenciales de acceso de las cuentas electrónicas.
	En caso de recibir un correo con ofertas, regalos o contenido tentador, seguir los siguientes pasos: 1. Evite abrir el correo. 2. No haga click en el enlace en cuestión.

Correos con ofertas, regalos o contenidos tentadores.	3. Para verificar si es real, basta con hacer una búsqueda rápida en Google. 4. Si se considera que es contenido falso, se debe eliminar el correo.
Correos de fuentes sospechosas.	En caso de recibir un correo o archivos adjuntos de fuentes sospechosas, debe seguir los siguientes pasos: 1. Verificar el nombre del remitente. 2. Si conoce a la persona, preguntarle directamente si son archivos válidos que él, envió. 3. Caso contrario, no responder al correo hasta verificar su autenticidad. 4. Si se verifica que es contenido fraudulento, se recomienda eliminar el correo en cuestión.
Mensajes con enlaces sospechosos.	Se puede dar el caso de recibir mensajes en las cuentas electrónicas, con un enlace que redirige a una página para colocar credenciales de acceso. Para verificar si es un sitio falso, se deben seguir los siguientes pasos: 1. Verificar la URL (dominio), visualizando la barra de direcciones del navegador. 2. Corroborar que haya un símbolo de candado en la parte izquierda de la web. 3. Revisar la gramática del sitio. 4. Identificar al propietario del sitio web.

	5. Estudiar el contenido del sitio. Por otro lado, se puede buscar herramientas en la web, que permiten verificar si el sitio presenta alguna vulnerabilidad.
Brindar información sensible.	Si una persona desea comunicarse con usted para saber información sensible, puede realizar lo siguiente: 1. Contactarme de forma directa con el remitente del mensaje. 2. Verificar su identidad. 3. Brindar la información de manera no tan detallada, para evitar futuros problemas.

Tabla 17. Autenticación y no repudio

REFORZAR LA SEGURIDAD EN EL TELÉFONO MÓVIL

Práctica de seguridad	Descripción
Código de seguridad.	Registrar un PIN para activar el acceso al dispositivo móvil, permite proteger los datos si se reinicia el equipo, cuando se cambia el chip del dispositivo o si una persona quiere ingresar a la información del teléfono.
Copia de seguridad.	Realizar una copia de seguridad de los datos del dispositivo, permite respaldar toda la información del teléfono móvil en caso de cualquier falla, pérdida de datos o borrados accidentalmente. Hay varias formas de realizarlo, entre ellas:

	- Copia a la tarjeta de expansión o mediante el software del fabricante. - Realizar una copia de seguridad periódica con los datos y ajustes de las aplicaciones. - Conectar el equipo a la computadora y realizar el respaldo. - Guardar información en servicios en la nube.
Activar las conexiones solo cuando sea necesario.	Es importante activar las conexiones bluetooth, infrarrojo y WIFI solo cuando se vayan a utilizar, debido que estos puertos son evidentes a simple vista y pueden ser un blanco fácil para el atacante, propiciando la fuga de datos.
Asegurar que la información transmitida o recibida esté libre de virus.	Teniendo en cuenta el sistema operativo de cada teléfono, existe una variedad de virus que afectan la funcionalidad del dispositivo, para esto, es necesario tener instalado un antivirus para comprobar los archivos que se transmiten.
Descargar aplicaciones de sitios oficiales.	Existen diversas aplicaciones con funciones ocultas para crear problemas o fallos en el teléfono. Es recomendable solo instalar aplicaciones que se puedan corroborar su procedencia y que sean seguras de utilizar. Se puede guiar de las tiendas de aplicaciones del fabricante, ya que, son ideales para instalar aplicaciones.
Cerrar todas las sesiones iniciadas.	Al terminar de usar una cuenta electrónica, es recomendable cerrar

	completamente la sesión, debido que, no se sabe cuándo se pueda perder el teléfono o caer en las manos equivocadas.
Actuar el sistema operativo del teléfono.	Es importante mantener actualizado el software del dispositivo, para evitar fallos de seguridad y optimizar las características que resultan un blanco potencial para los atacantes.
Guardar el número IMEI	Es un código pregrabado en los dispositivos móviles, que identifican el equipo a nivel mundial. Esto permite tener la información a salvo de terceras personas, permitiendo bloquear el teléfono en caso de robo o pérdida.

Tabla 18. Reforzar la seguridad en el teléfono móvil

4.3. HERRAMIENTAS PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN

Disponibilidad

- **Firewall:** Herramienta de seguridad cibernética que se emplea para filtrar el tráfico de una red [51]. Los cortafuegos pueden ser utilizados para separar nodos de red de fuentes de tráfico externas, internas o de aplicaciones específicas [51].
- **Google drive:** Es una plataforma que permite compartir archivos que se pueden utilizan como espacio de almacenamiento personal y seguro en la nube [52]. Proporciona un acceso cifrado y seguro de la información [52].
- **Mega:** Es un servicio basado en la nube que permite guardar archivos y ser utilizado desde cualquier lugar con internet, en cualquier dispositivo y plataformas principales [53].
- **Licencias oficiales de sistema operativo:** Es importante descargar los parches de seguridad desde la página legítima del sistema operativo que se emplee.

Confidencialidad

- **Navegador en modo incógnito:** Si una persona navega en modo incógnito, los datos de actividad no se guardan en el dispositivo ni cuenta a la que no haya accedido [54].
- **Servidor proxy:** Dispositivo que actúa como intermediario entre el internet y las conexiones del navegador, filtrando los paquetes que circulan entre ambos puntos [55].

Integridad

- **VPN:** Las herramientas VPN brindan la oportunidad de establecer una conexión segura y protegida al utilizar redes públicas [56]. Las VPN cifran el tráfico en internet y disfrazan la identidad en línea, dificultando a terceros, el seguimiento de las actividades en línea y el robo de información [56].
- **Play Store:** Es una app oficial de Google, donde los usuarios pueden descargar juegos y contenido digital para el dispositivo [57].
- **Antivirus:** Software que permite buscar, detectar, evitar y eliminar virus de un equipo [55].
- **Herramientas IDS:** Las herramientas de detección de intruso se refieren a una aplicación que sirve para monitorear la red informática, las aplicaciones o los sistemas de una empresa, buscando infracciones de políticas y actividades maliciosas [58]. Entre las herramientas más utilizadas, están: NIDS, HIDS, IDS basados en firmas, IDS basados en anomalías, IDS pasivo e identificación reactiva [58].
- **Aplicaciones para ver redes WIFI seguras:** Estas aplicaciones permiten realizar un escaneo de la red a donde se quiere conectar, y verificar que todo esté en orden [59]. A continuación, se enlistan herramientas de este tipo: NetSpot, WIFI Analyzer, Wiffinity, WeFI, entre otras [59].
- **Herramientas para detectar memorias USB, pendrives o discos externos falsos:** Para comprobar que los dispositivos que ingresen al equipo están libres de virus o malware, existen diversos programas que permiten escanear este tipo de problemas, los cuales son: check flash, chip genius, H2testw, entre otros [60].

Autenticación y no repudio

- **VirusTotal**

Es uno de los sitios más conocidos y completos, cuenta con una base de datos actualizada, permitiendo saber si un dominio o página web contiene virus y es una amenaza. Así se visualiza el sitio web:

Figura 53. Página VirusTotal

Se puede escoger entre las opciones: Archivo, URL y buscar. Permite analizar un sitio web en concreto o archivos que se encuentren alojados en el computador. En este caso, se procede a escoger la segunda opción “URL”, y pegar el enlace de la página que se quiere verificar.

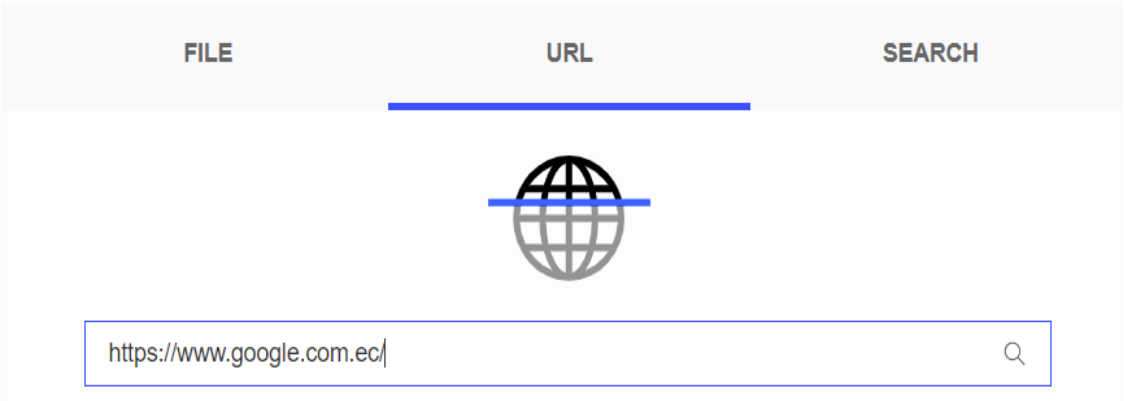


Figura 54. Enlace de verificación

La página procede a realizar el análisis del sitio. A continuación, se visualiza que la página en cuestión, no tiene amenazas ni virus de por medio.

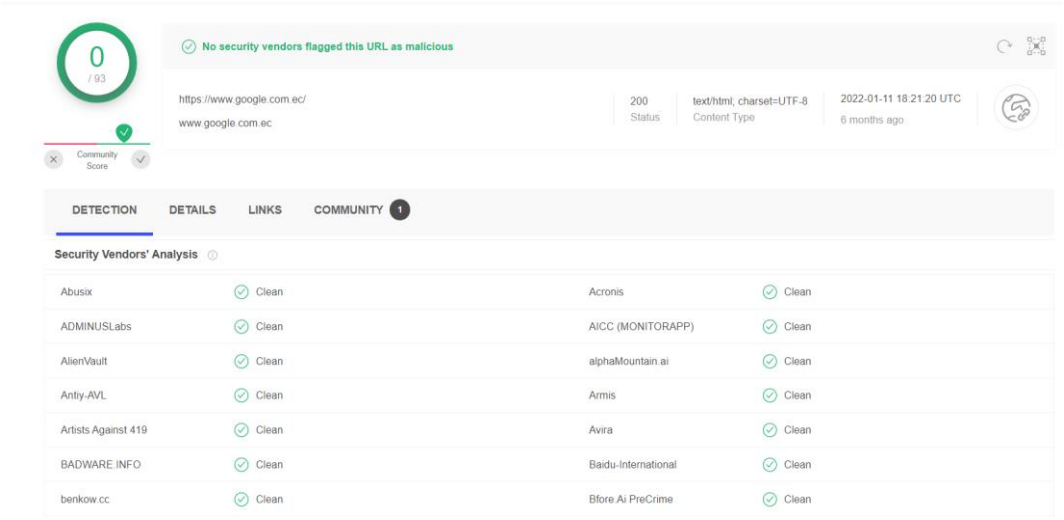


Figura 55. Resultados de la página VirusTotal

- **Google Navegación Segura**

Google posee una enorme variedad de servicios en internet, y uno de ellos es la opción de Google Navegación Segura o Safe Browsing. Este sitio bloquea el acceso a una página web que pueda contener algún tipo de virus o malware.

Además, permite analizar una URL sin necesidad de ingresar a ella. El sitio web es el siguiente:

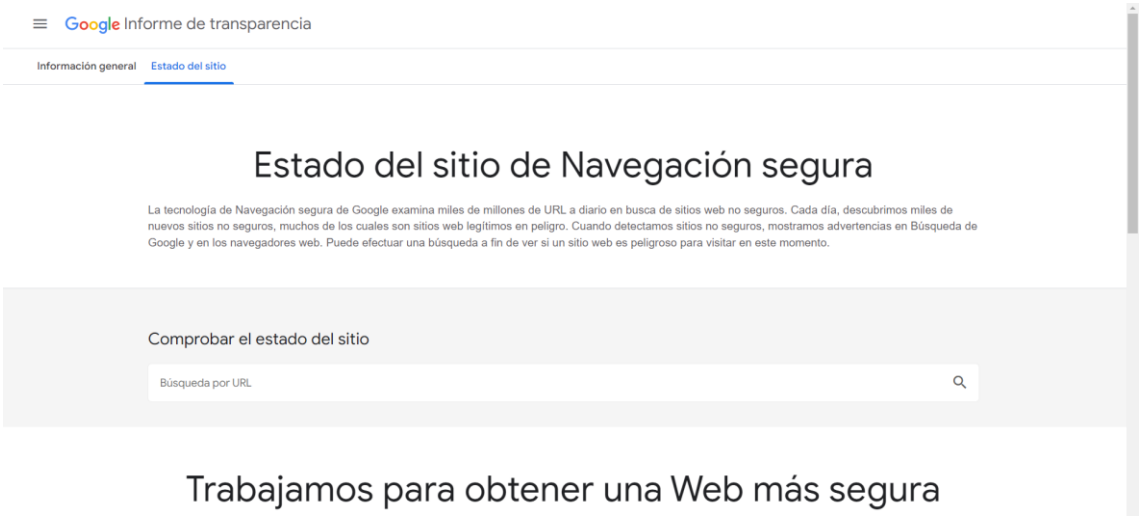


Figura 56. Página Google Navegación Segura

Escribimos la URL que se quiere analizar y el sitio web presentará el estado actual del mismo.

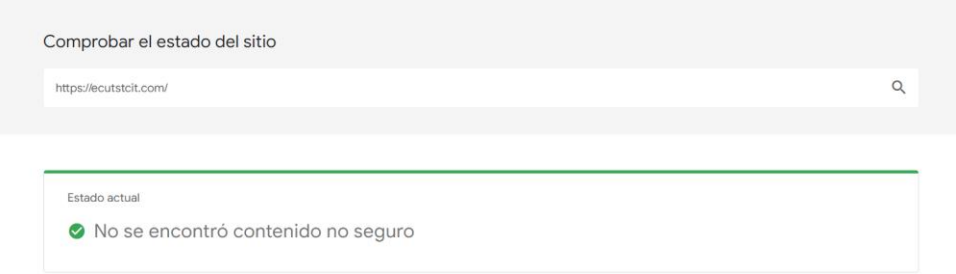


Figura 57. URL en Google Navegación Segura

- **Securi SiteCheck**

Es una herramienta gratuita que permite verificar si una página tiene malware. Lo que hace es comprobar que sea un sitio seguro, comprobando si se encuentra o no, en una lista negra. Es capaz de escanear diversas páginas dentro de un dominio. El sitio web es el siguiente:

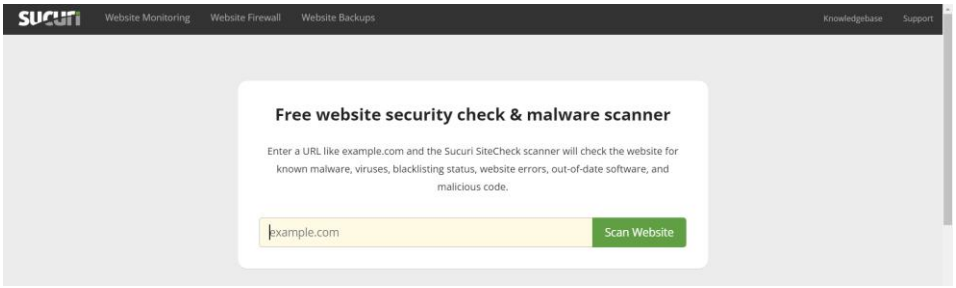


Figura 58. Página Securi SiteCheck

Se debe ingresar la URL para que el sitio web la escanee, y posteriormente se conocen los resultados del mismo.

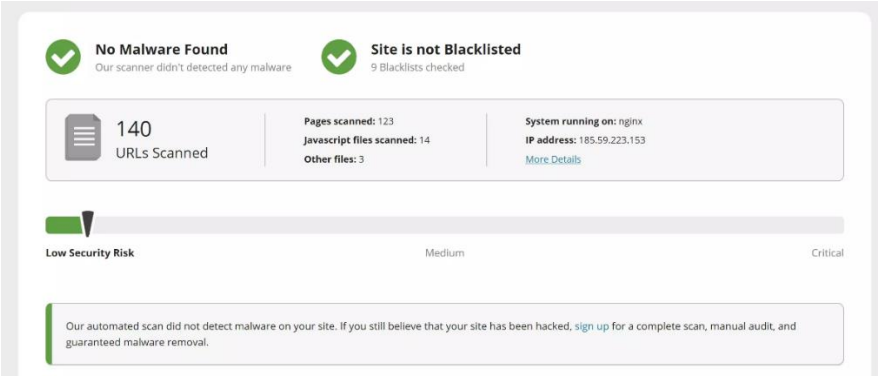


Figura 59. Resultados de la página Securi SiteCheck

CONCLUSIONES

- ✓ Se investigó acerca de los diferentes tipos de métodos empleados en ingeniería social, escogiendo los vectores de ataque: Website attack Vectors, Infectious media Generator, QRCode Generator attack vector, Shoulder surfing y Vishing.

- ✓ Se recopiló información a través de una encuesta al personal docente y estudiantes de la institución de educación superior, en base a los conocimientos que poseen con respecto al uso seguro de los sistemas informáticos, permitiendo establecer de manera correcta los requerimientos del proyecto

- ✓ Se emplearon los vectores de ataques computacionales y no computacionales nombrados anteriormente, identificando las vulnerabilidades a las que están expuestas los usuarios por la falta de conocimiento en seguridad informática

- ✓ El diseño de los ciberataques, se realizaron en el sistema operativo Kali Linux, en conjunto con la herramienta Social Engineering Toolkit, tomando en consideración los requerimientos del proyecto.

- ✓ Se elaboró un informe final con los resultados obtenidos de los ataques realizados en la institución de educación superior, evidenciando el tipo de vector de ataque, horas ejecutadas, cantidad de víctimas, resultados y observaciones, teniendo en cuenta las consecuencias que produjo cada uno.

- ✓ Se realizó una guía de buenas prácticas de seguridad de la información, clasificada según las características de la seguridad de esta (Disponibilidad, confidencialidad, integridad, autenticación), teniendo como objetivo, concientizar a las personas y presentar diversas recomendaciones que se puedan ejecutar, para mitigar riesgos de un futuro ataques.
- ✓ Un gran porcentaje de las personas que participaron en este trabajo investigativo, no sospecharon, que los enlaces y códigos Qr enviados eran con mal intencionados, para que entreguen sus credenciales de inicio de sesión.

RECOMENDACIONES

- ✓ En caso de querer realizar otros ataques de ingeniería social, es importante contar con el permiso de los individuos, ya que, el robo de la información es un delito cibernético.

- ✓ Se recomienda realizar periódicamente pruebas de ataques de ingeniería social, para conocer la situación actual del personal docente y estudiantes, verificando las mejoras que han tenido respecto al conocimiento de seguridad informática.

- ✓ Para realizar los ciberataques de ingeniería social, es recomendable utilizar el software Kali Linux en una máquina virtual, debido que, es un instrumento fácil de usar y contiene las herramientas necesarias para el diseño de los ataques.

- ✓ Se recomienda leer la guía de buenas prácticas, ya que, cuenta con recomendaciones que ayudan a mitigar riesgos de ciberataques y refuerzan la seguridad informática, así mismo, posee prácticas de seguridad para teléfonos móviles y páginas que permiten verificar si el sitio web es confiable o contiene algún malware.

BIBLIOGRAFÍA

[1] E. J. Sandoval Castellanos, «Ingeniería social: Corrompiendo la mente humana,» *Seguridad - Cultura de prevención para TI,* nº 10, p. 10, 2018.

[2] J. P. Prado Díaz, «Ingeniería social, un ejemplo práctico,» *Revista Odigos,* vol. 2, nº 3, p. 24, 10 10 2021.

[3] C. J. Londoño, «La ingeniería social: Un desafío investigativo,» *Revista universal Eafit,* p. 11, 2020.

[4] J. E. A. CHANG*, «ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR,» *Revista Científica Aristas,* p. 19, 2020.

[5] L. G. H. Jaramillo, «Estudio del grado de incidencia de la ingeniería social en la primera fase de los ataques informáticos que se realizan actualmente en las empresas privadas del Ecuador,» Quito, 2020.

[6] J. E. A. Chang, «Análisis de ataques cibernéticos hacia el Ecuador,» *Revista Científica Aristas,* p. 10, 05 2020.

[7] C. Dergarabedian, «iprofesional.com,» 28 08 2019. [En línea]. Available: https://www.iprofesional.com/tecnologia/298857-en-la-argentina-hay-casi-50-ataques-informaticos-por-minuto. [Último acceso: 17 05 2022].

[8] K. Lab, «latam.kaspersky.com,» 12 05 2021. [En línea]. Available: https://latam.kaspersky.com/about/press-releases/2021_el-legado-de-wannacry-cuarto-aniversario-de-la-epidemia-de-ransomware-global-busca-crear-conciencia-sobre-esta-persistente-amenaza. [Último acceso: 17 05 2022].

[9] L. A. R. Matías, «Análisis de vulnerabilidades del portal web utilizando metodologías de hacking ético para un GAD Municipal de la Provincia de Santa Elena,» La Libertad, 2021.

[10] E. S. CAMINO RUIZ y E. D. PUENTE PACHECO, «ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD EN LA RED DE LA UNIDAD EDUCATIVA SALESIANA CARDENAL SPELLMAN, UTILIZANDO HERRAMIENTAS DE INGENIERÍA SOCIAL, Y RECOMENDAR MEDIDAS PREVENTIVAS.,» UNIVERSIDAD POLITÉCNICA SALESIANA, Quito, 2020.

[11] Eset, «Eset Security Report,» 2019.

[12] TecnoSeguro, «TecnoSeguro,» 11 12 2020. [En línea]. Available: https://www.tecnoseguro.com/analisis/seguridad-informatica/practicas-

empresariales-proteccion-contra-ataques-ciberneticos-genetec. [Último acceso: 17 05 2022].

[13] O. J. Román, «Plan sectorial de defensa 2017 - 2021,» Quito, 2017.

[14] O. Zafra, «Tipos de investigación,» *Redalyx*, vol. 4, nº 4, p. 3, 2020.

[15] O. Hurtado, «Sistema de educación superior del Ecuador,» Quito, 2020.

[16] virtualeduca, «Los retos de seguridad informática que enfrentan las instituciones educativas colombianas,» virtualeduca, 27 08 2021. [En línea]. Available: https://virtualeduca.org/mediacenter/los-retos-de-seguridad-informatica-que-enfrentan-las-instituciones-educativas-colombianas/. [Último acceso: 22 07 2022].

[17] udla, «Instituciones educativas en riesgo informático,» udla, 15 12 2021. [En línea]. Available: https://www.udla.edu.ec/liderazgo/blog/2021/12/15/instituciones-educativas-en-riesgo-informatico/. [Último acceso: 21 07 2022].

[18] Scielo, «Los retos actuales de las instituciones de educación superior en el área de la gestión,» Scielo, 15 08 2016. [En línea]. Available: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202015000200008. [Último acceso: 21 07 2022].

[19] helpsystems, «Protección de la Infraestructura de IT,» helpsystems, [En línea]. Available: https://www.helpsystems.com/es/soluciones/seguridad-informatica/infraestructura. [Último acceso: 23 07 2022].

[20] sobretiza, «La Seguridad Informática en las universidades,» sobretiza, 24 09 2016. [En línea]. Available: https://www.sobretiza.com.ar/2014/09/24/la-seguridad-informatica-en-las-universidades/. [Último acceso: 21 07 2022].

[21] upse, «Revista cientifica y tecnologica Upse,» upse, 01 2022. [En línea]. Available: https://incyt.upse.edu.ec/ciencia/revistas/index.php/rctu/article/view/627/528. [Último acceso: 21 07 2022].

[22] /telecomunicaciones, «Importancia de la ciberseguridad en el Campus Universitario.,» /telecomunicaciones, 13 11 2019. [En línea]. Available: https://telecomunicaciones.edu.ec/repositorio/articulos-blog/redes/importancia-de-la-ciberseguridad-en-el-campus-universitario. [Último acceso: 21 07 2022].

[23] P. d. l. República, «Ley orgánica de educación superior, LOES,» Quito, 2018.

[24] M. D. C. Molinero y U. Cháves Morales, «Herramientas tecnológicas en el proceso de enseñanza - aprendizaje en estudiantes de educación superior,» *Scielo*, vol. 10, nº 19, p. 11, 15 05 2020.

[25] google, «google.com,» [En línea]. Available: https://www.google.com/intl/es/gmail/about/.

[26] Microsoft, «microsoft.com,» [En línea]. Available: https://www.microsoft.com/es-es/microsoft-365/word.

[27] Adobe, «adobe.com,» [En línea]. Available: https://www.adobe.com/la/acrobat/complete-pdf-solution.html?mv=search&ef_id=Cj0KCQjw8amWBhCYARIsADqZJoVghPSYdsXYpaHVfTd8MreQwynRJXrJAiTK2t4cnLiIbXPAMBLRUowaAjo_EALw_wcB:G:s&s_kwcid=AL!3085!3!584124841135!e!!g!!adobe%20acrobat!178188 2837!68877166443&gclid=.

[28] Google, «google.com,» [En línea]. Available: https://www.google.com/intl/es/chrome/.

[29] Google, «google.com,» [En línea]. Available: https://www.google.com/.

[30] Microsoft, «microsoft.com,» [En línea]. Available: https://www.microsoft.com/es-es/microsoft-365/powerpoint.

[31] Microsoft, «microsoft.com,» [En línea]. Available: https://www.microsoft.com/es-ww/microsoft-365/excel.

[32] Avast, «avast.com,» [En línea]. Available: https://www.avast.com/es-ww/lp-ppc-hp-v5?ppc_code=012&ppc=a&gclid=Cj0KCQjw8amWBhCYARIsADqZJoWN1POxgzVXm3-LxwmzY68XbMTAOq-RINzAtrThOlHmwZQ_U-32mgIaAvgMEALw_wcB&gclsrc=aw.ds#pc.

[33] mundocuentas, «mundocuentas.com,» [En línea]. Available: https://www.mundocuentas.com/facebook/.

[34] neoattack, «neoattack.com,» [En línea]. Available: https://neoattack.com/neowiki/whatsapp/.

[35] Zoom, «zoom.us,» [En línea]. Available: https://zoom.us/.

[36] Moodle, «moodle.org,» [En línea]. Available: https://moodle.org/?lang=es.

[37] Google, «workspace.google.com,» [En línea]. Available: https://workspace.google.com/intl/es-419/products/drive/?utm_source=google&utm_medium=cpc&utm_campaign=latam-T1-all-es-dr-bkws-all-all-trial-e-dr-1011272-LUAC0012558&utm_content=text-ad-none-any-DEV_c-CRE_479487543818-ADGP_Hybrid%20%7C%20BKWS%20-%20EXA%20.

[38] C. d. l. R. d. Ecuador, «Ley orgánica de protección de datos personales,» Quito, 2021.

[39] K. Linux, «kali.org,» [En línea]. Available: https://www.kali.org/. [Último acceso: 17 05 2022].

[40] hackplayers, «Introducción a Social-Engineering Toolkit (SET),» hackplayers, 27 10 2016. [En línea]. Available: https://www.hackplayers.com/2012/10/social-engineering-toolkit-set.html. [Último acceso: 23 07 2022].

[41] J. P. Prado Díaz, «Ingeniería social, un ejemplo práctico,» *Revista ODIGOS*, vol. 2, nº 3, p. 24, 10 09 2021.

[42] D. Romero, «El arte de la ingeniería social,» Bogotá, 2021.

[43] R. Salvador Guadrón, «Ingeniería social: El ataque silencioso,» *Revista tecnológica*, p. 8, 2015.

[44] E. Benavides Astudillo, W. Fuertes Díaz y S. Sánchez Gordon, «Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social,» *Revista Ciencia Unemi*, vol. 13, nº 32, p. 40, 2020.

[45] E. Y. Rodríguez Rincón, «Metodologías de ingeniería social,» 2018.

[46] M. Gómez Urbano, «Análisis del riesgo de ataques de ingeniería social en la secretaría de educación del departamento de Nariño,» 2020.

[47] O. A. Torres Díaz y J. P. López Rodríguez, «Diseño e implementación de un plan de concientización frente a la ingeniería social para la empresa promociones y cobranzas Beta S.A.,» Bogotá, 2017.

[48] P. I. Morales Paredes y P. Medina Chicaiza, «Ciberseguridad en plataformas educativas institucionales de Educación Superior,» *Dialnet*, p. 27, 09 2021.

[49] C. Chhetri y V. Motti, «Identifying Vulnerabilities in Security and Privacy of Smart Home Devices,» 2021.

[50] N. V. Avellán Zambrano y M. F. Zambrano Bravo, «Ciberseguridad y su aplicación en las instituciones de educación superior públicas de Manabí,» Calceta, 2019.

[51] HP, «hp.com,» [En línea]. Available: https://www.hp.com/cl-es/shop/tech-takes/que-es-un-firewall-de-red-y-como-funciona#:~:text=Un%20firewall%20es%20un%20sistema,o%20una%20combinaci%C3%B3n%20de%20ambos..

[52] Google, «google.com,» [En línea]. Available: https://www.google.com/intl/es/drive/.

[53] Mega, «mega.nz,» [En línea]. Available: https://mega.nz/.

[54] Google, «support.google.com,» [En línea]. Available: https://support.google.com/chrome/answer/9845881?hl=es-

419#zippy=%2Cc%C3%B3mo-protege-tu-privacidad-el-modo-inc%C3%B3gnito. [Último acceso: 02 08 2022].

[55] Avast, «avast.com,» [En línea]. Available: https://www.avast.com/es-es/c-what-is-a-proxy-server.

[56] Opera, «opera.com,» [En línea]. Available: https://www.opera.com/es-419/features/free-vpn.

[57] google, «play.google.com,» [En línea]. Available: https://play.google.com/store/games?hl=es&gl=US.

[58] OpenWebinars, «openwebinars.net,» [En línea]. Available: https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/. [Último acceso: 02 08 2022].

[59] NetSpotapp, «netspotapp.com,» [En línea]. Available: https://www.netspotapp.com/es/blog/all-about-wifi/wifi-near-me.html#:~:text=NetSpot%20%E2%80%94%20es%20la%20mejor%20aplicaci%C3%B3n,mejor%20red%20en%20cada%20ubicaci%C3%B3n..

[60] Softzone, «softzone.es,» [En línea]. Available: https://www.softzone.es/2018/03/16/aplicaciones-gratis-detectar-pendrive-disco-duro-externo-memorias-usb-falsas/. [Último acceso: 02 08 2022].

[61] A. Suing, P. Barrazueta Molina y L. Carpio Jiménez, «Orientación al ciudadano en el "gobierno electrónico" de los municipios del Ecuador,» *Dialnet*, p. 15, 29 10 2017.

[62] P. Security, «parrotsec.org,» [En línea]. Available: https://www.parrotsec.org/. [Último acceso: 17 05 2022].

[63] I. Mata Villalpando y O. Guevara Juárez, «Virus informáticos, todo un caso, pero no perdido,» *Redalyc*, vol. 4, nº 4, p. 7, 2020.

[64] N. Oxman, «Estafas informáticas a través de internet: Acerca de la imputación penal del "phishing" y el "pharming",» *Redalyc*, p. 53, 2019.

[65] UPSE, «facsistel.upse.edu.ec,» [En línea]. Available: http://facsistel.upse.edu.ec/index.php?option=com_content&view=article&id=58&Itemid=463. [Último acceso: 17 05 2022].

[66] kaspersky, «latam.kaspersky,» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Último acceso: 23 05 2022].

[67] K. Lavinder, «Ataques cibernéticos,» 2016.

[68] M. S. Mariana Leguizamón, «El phishing,» 2020.

[69] oracle, «oracle.com,» [En línea]. Available: https://www.oracle.com/es/database/security/que-es-el-malware.html#:~:text=Malware%20es%20un%20t%C3%A9rmino%20gen%C3%A9rico,contenido%20activo%20y%20otro%20software.. [Último acceso: 24 05 2022].

[70] U. E. P. d. S. Elena, «Resolución RCF-FST-SO-09 No. 03-2021,» La Libertad, 2021.

[71] UPSE, «upse.edu.ec,» 2021. [En línea]. Available: https://www.upse.edu.ec/index.php?option=com_content&view=article&id=12&Itemid=167. [Último acceso: 2022].

[72] UPSE, «upse.edu.ec,» 2021. [En línea]. Available: https://www.upse.edu.ec/cec/index.php?option=com_content&view=article&id=16:base-legal&catid=13&Itemid=167.

[73] norton, «lam.nortom.com,» [En línea]. Available: https://lam.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html.

[74] derechodelared, «derechodelared.com,» [En línea]. Available: https://derechodelared.com/tecnicas-de-ingenieria-social/.

[75] U. d. Ecuador, «universidades.com.ec,» 24 09 2021. [En línea]. Available: https://www.universidades.com.ec/tiffin-university/articulo-que-caracteristicas-tiene-la-educacion-superior. [Último acceso: 09 07 2022].

ANEXOS

Anexo 1. Crecimiento de ataques por malware

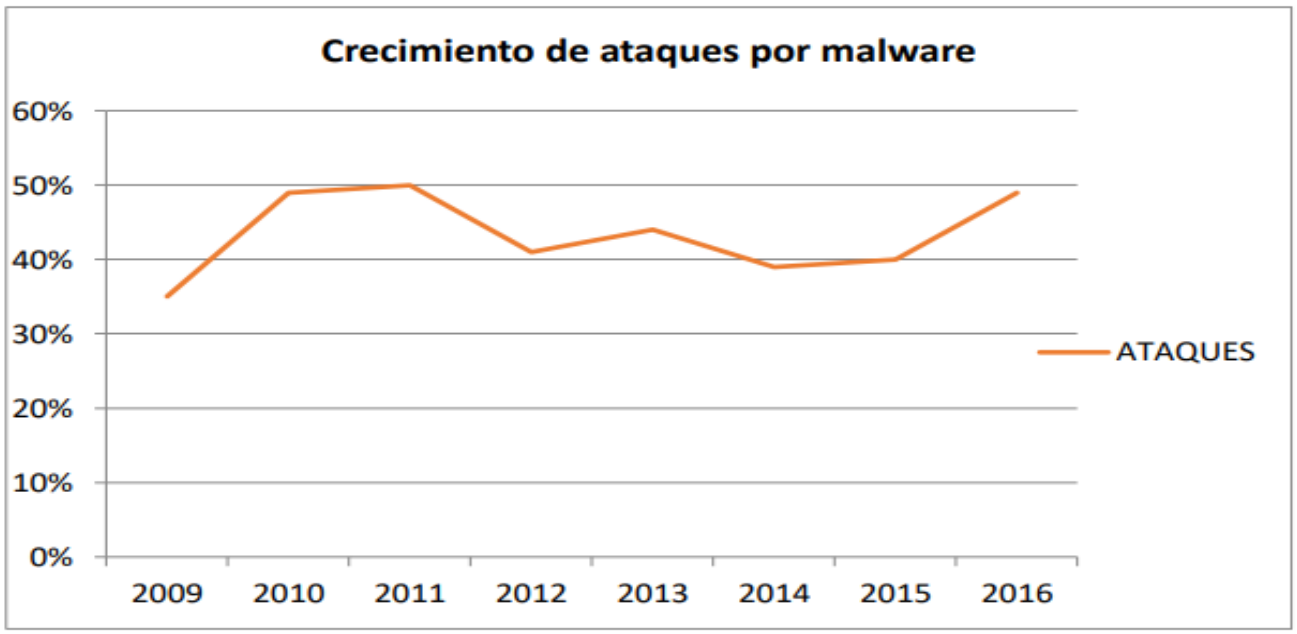


Figura 60. Evolución de ataques por malware desde el 2009 a 2016. Fuente: ESET. (2017)

Anexo 2. Total, de la encuesta

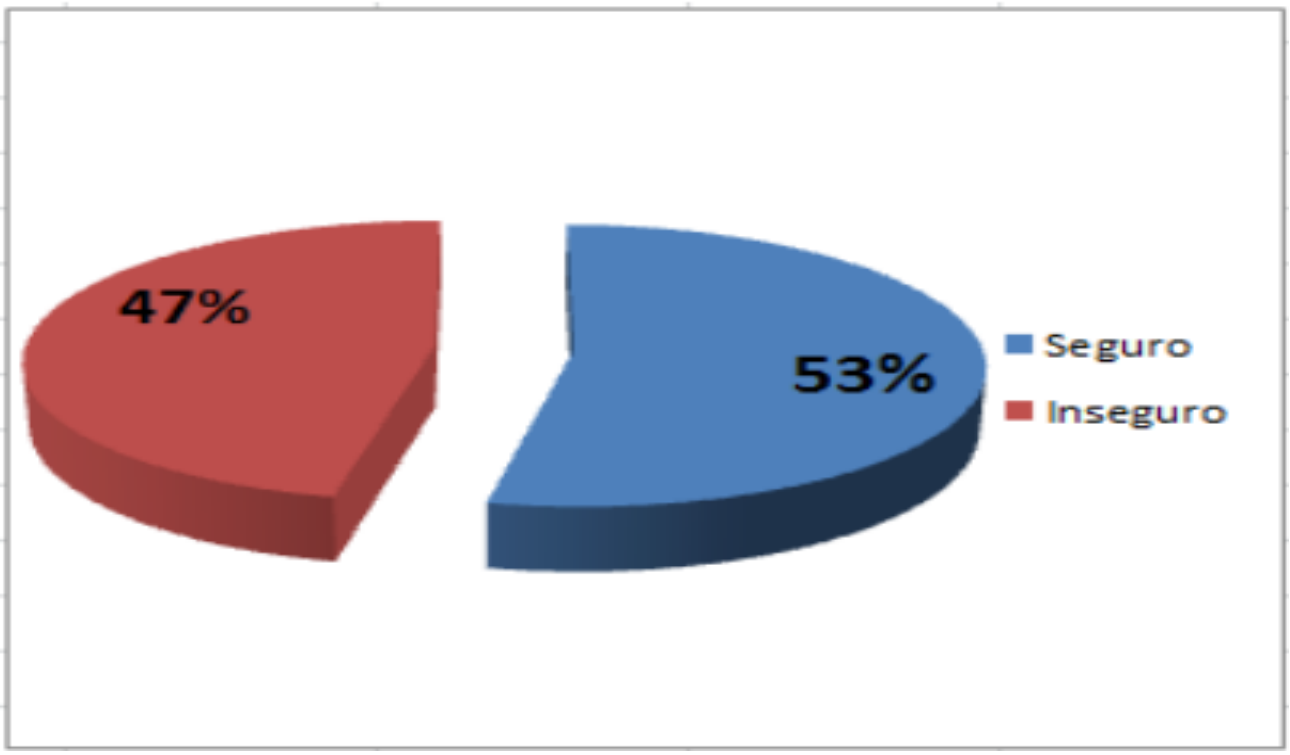


Figura 61. Total, general del resultado de la encuesta de seguridad informática: Espirales revista multidisciplinaria de investigación

Anexo 3. Número de usuarios afectados por ransoware

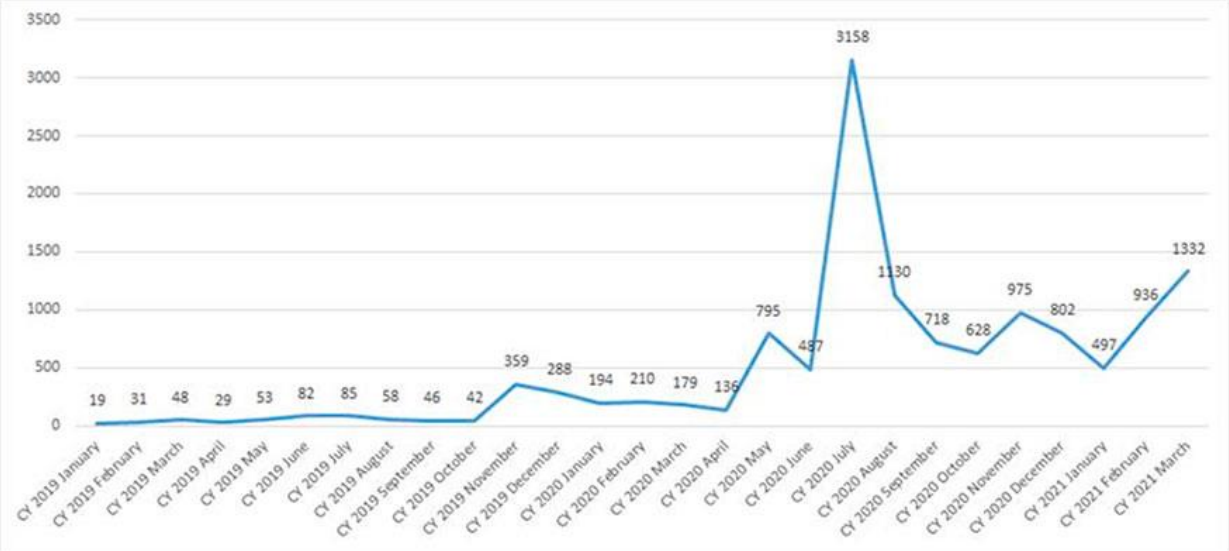


Figura 62. Número de usuarios de Kaspersky afectados por ransoware en el año 2019-2020: Kaspersky

Anexo 4. Ataques durante la pandemia 2020

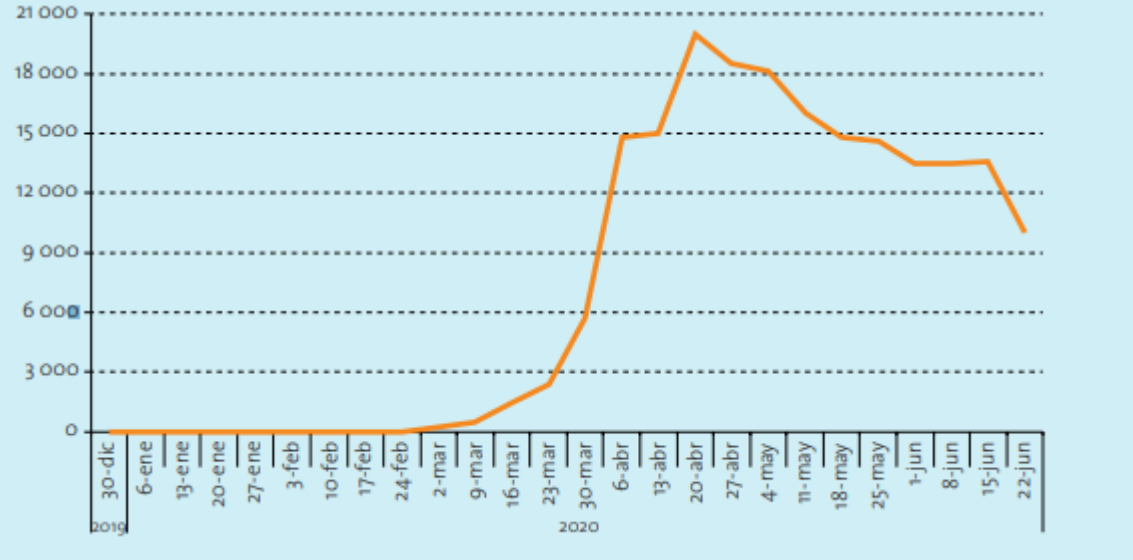


Figura 63. Ataques durante la pandemia 2020 Fuente: CheckPoint (2020), "Cyber attack trends: 2020 mid-year report", Check Point Software Technologies Ltd., Tel Aviv, Israel, Julio [en línea] https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.

Anexo 5. Denuncia de delitos informáticos en Ecuador

Número de denuncias sobre delitos informáticos en ecuador

Tipos de delitos	2014*	2015	2016	2017	2018	2019	2020**	Total
Suplantación de identidad	1355	3920	4152	3676	4180	4607	2162	24052
Falsificación y uso de documento falso	1048	2594	3117	3183	3292	3231	1448	17913
Apropiación fraudulenta por medios electrónicos	507	1280	1045	960	1451	1746	1033	8022
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	54	141	145	218	236	246	175	1215
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	21	80	108	159	202	166	85	821
Ataque a la integridad de sistemas informáticos	49	77	76	86	87	113	51	539
Interceptación ilegal de datos	38	55	82	63	41	87	45	411
Transferencia electrónica de activo patrimonial	17	59	47	54	38	49	31	295
Revelación ilegal de base de datos	29	24	24	22	44	34	18	195
Total	**3118**	**8230**	**8796**	**8421**	**9571**	**10279**	**5048**	**53463**

Figura 64. Denuncia de delitos informáticos en Ecuador

Anexo 6. Encuesta dirigida al personal docente y entudiantes de la Unidad Superior Educativa- Facultad de Educación e idiomas

Universidad Estatal Península de Santa Elena
Facultad de Sistemas y Telecomunicaciones
Carrera de Tecnología de la Información.

Encuesta dirigida al personal docente y estudiantes de la Facultad de Educación e idiomas

Objetivo: Determinar el nivel de conocimiento que tienen los estudiantes y profesores acerca del uso seguro de los sistemas informáticos.

I. USO DE SISTEMAS INFORMATICOS

1.	**¿Qué nivel de conocimientos considera que tiene sobre el uso de internet y sistemas informáticos?** Alto__ Medio__ Bajo__
2.	**¿Con qué fin utiliza las redes sociales?** Entretenimiento__ Educativo__ Informativo__ Trabajo__ Otro__
3.	**¿Qué nivel de conocimiento tiene respecto a las amenazas y los riesgos informáticos que están presentes en las redes sociales?** Alto__ Medio__ Bajo__
4.	**¿Utiliza contraseñas diferentes para sus cuentas electrónicas como redes sociales, email, aula virtual?** Si__ No__

II. CONOCIMIENTOS DE CIBERATAQUES

5.	**¿Cuál de estos ciberataques conoce, y que los podría explicar a otras personas?** Ransomware__ Phishing__ Ataques por denegación de servicios (DDoS)__ Troyanos__ Ninguno __
6.	**¿Qué tipo de fraudes electrónicos le genera mayor temor?** Que me roben dinero de mis cuentas bancarias__ Suplantación de identidad __ Que secuestren mi WhatsApp__ Estafas de vendedores en sitios web ilegítimos__
7.	**¿Con que frecuencia recibe mensajes de texto que da aviso que alguien ha ingresado a una de sus cuentas electrónicas como Facebook, Instagram, email?** 1 vez al mes__ 1 vez cada 3 meses___ 1 vez al año__ Nunca__
8.	**¿Alguna vez han vulnerado la seguridad de sus cuentas electrónicas?** Si__ No__
III. USO SEGURO DE REDES SOCIALES	
9.	**¿Qué nivel de conocimiento tiene sobre las seguridades que se aplican en sus cuentas electrónicas?** Alto__ Medio__ Bajo__
10.	**¿Cuál de estos métodos le genera mayor seguridad con sus dispositivos y cuentas electrónicas?** Tener instalado un antivirus___ Desconfiar de todo lo que llega al teléfono____ Tener una protección integral de mi presencia digital___ Con no abrir emails raros es suficiente___ No hace falta nada, mis dispositivos son seguros____

11.	**¿Considera importante conocer a las personas que tiene agregadas en sus redes sociales?** Muy importante__ Importante__ Poco importante__ No es importante__
12.	**¿Considera que su seguridad informática esta más amenazada ahora?** Ahora hay los mismos riesgos de antes__ Los riesgos han aumentado un poco pero no me afectan__ Me siento más vulnerable ante riesgos informáticos___ Me siento muy seguro antes y ahora__
13.	**En su opinión, ¿Qué tan segura es la red de la Universidad?** Muy segura__ Segura __ Insegura__ Muy insegura___
14.	**¿Qué nivel de seguridad cree usted que tiene la red WIFI de su institución educativa?** Alto__ Medio__ Bajo__
15.	**¿Conoce de algún ciberataque dirigido a su entidad educativa?** Si__ No__
16.	**¿Desea participar en este trabajo investigativo como informante del nivel de seguridad que posee en sus dispositivos y cuentas electrónicas?** Si__ No__
17.	**Si su respuesta anterior fue SI, complete la siguiente información:** Correo Personal: Correo institucional: Numero móvil:
Responsable:	Peñafiel Suárez Marcelo Rodrigo

Anexo 7. Ataque 1: Phishing por clonación de página

Figura 65. Envío de ataque por correo

Figura 66. Datos de víctima del ataque

Figura 67. Datos de víctima del ataque

Figura 68. Datos de víctima del ataque

Figura 69. Datos de víctima del ataque

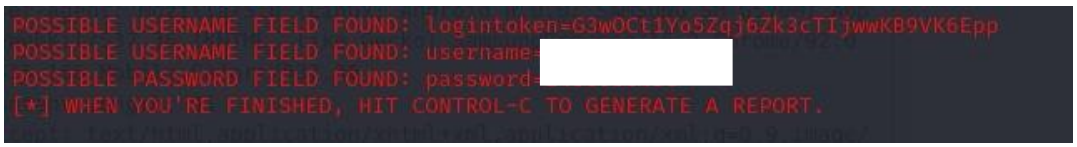


Figura 70. Datos de víctima del ataque

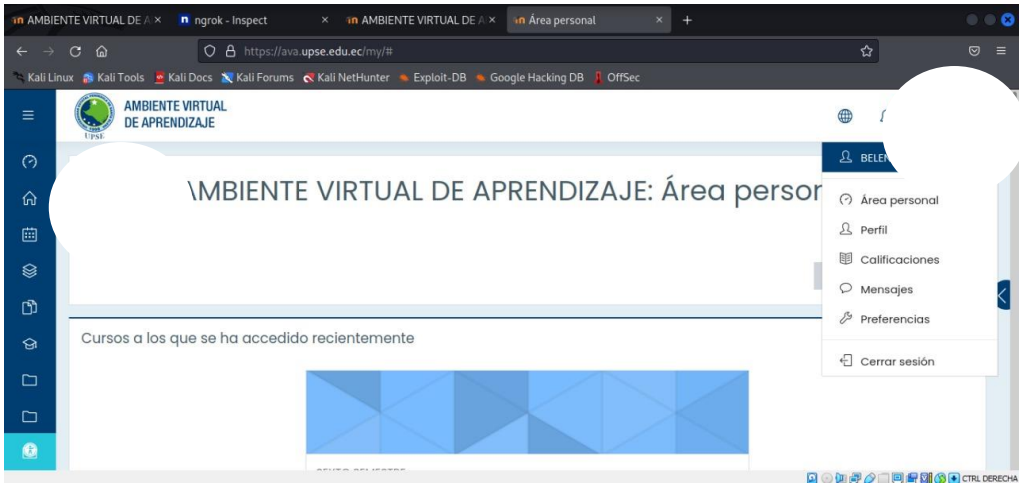


Figura 71. Datos de víctima del ataque

Figura 72. Datos de víctima del ataque

Figura 73. Datos de víctima del ataque

Figura 74. Datos de víctima del ataque

Anexo 8. Ataque Shoulder Surfing

Figura 75. Ataque de Shoulder surfing

Figura 76. Ataque de Shoulder surfing

Figura 77. Ataque de Shoulder surfing

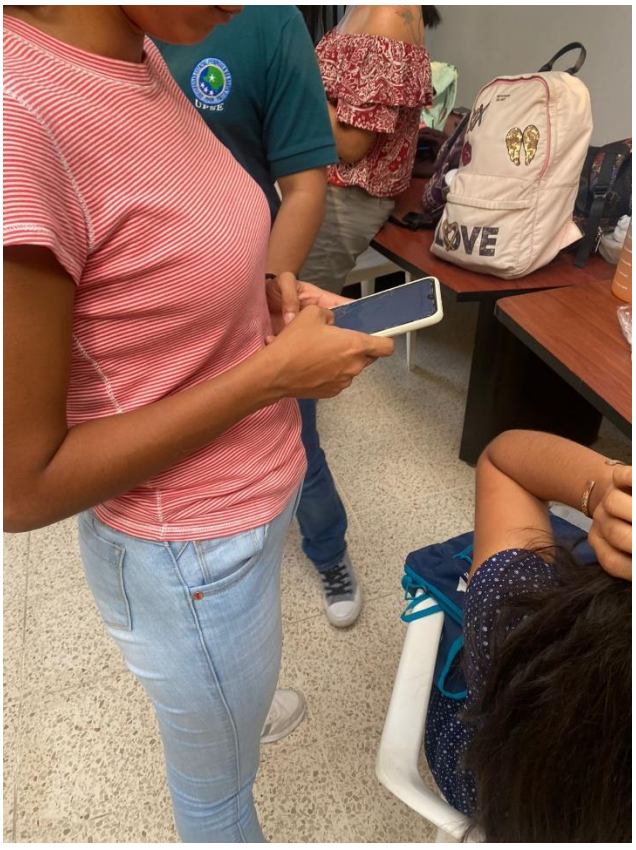


Figura 78. Ataque de Shoulder surfing

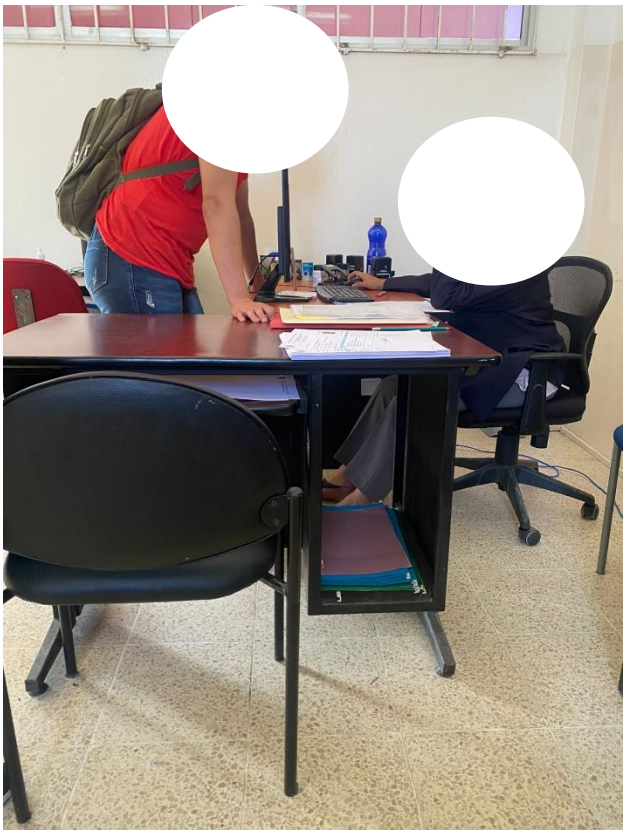


Figura 79. Ataque de Shoulder surfing

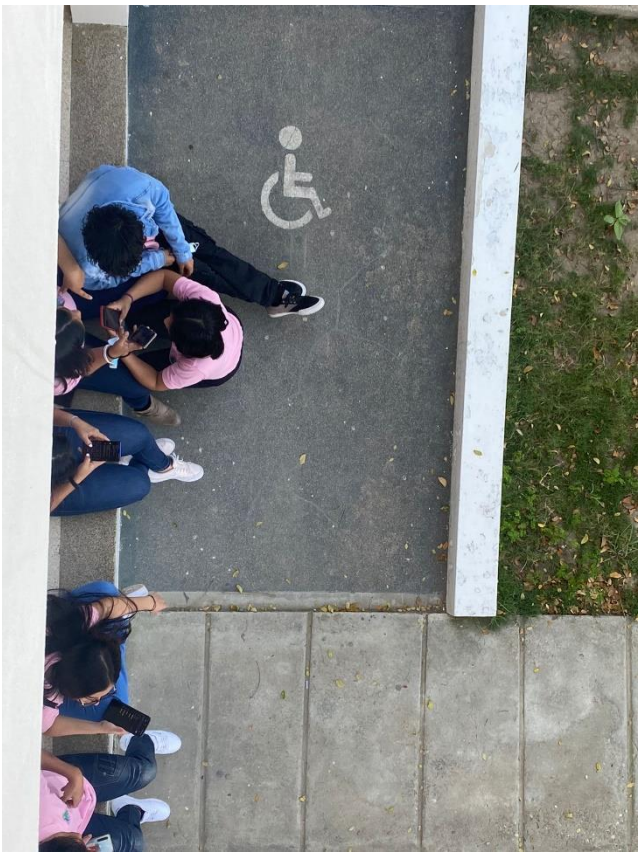


Figura 80. Ataque de Shoulder surfing

Anexo 9. Permiso de la institución

UPSE

Facultad de Ciencias de la Educación e Idiomas

Oficio No. UPSE-FCEI-2022-156
La Libertad, 5 de julio del 2022

Señor
Ing. Jaime Orozco Iguasnia, Mgt.
DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN
Presente. -

Estimado Director:

En atención a Oficio No. UPSE-CTI-246-2022-OF, para aplicación de encuesta, expongo ante usted la respectiva autorización; sin embargo, considero coordinar la actividad con las direcciones de Carreras que componen la Facultad de Ciencias de la Educación e Idiomas, para el efecto adjunto los respectivos correos.

DIRECCIÓN DE CARRERA DE EDUCACIÓN INICIAL
carrera_educacion_inicial@upse.edu.ec
Directora Educación Inicial: Uribe Veintimilla Ana Maria auribe@upse.edu.ec
Asistente: Fabian Benavides fbenavides@upse.edu.ec

DIRECCIÓN DE CARRERA DE PEDAGOGÍA DE LOS IDIOMAS NACIONALES Y EXTRANJEROS
pine@upse.edu.ec
Directora de Carrera de PINE: Gonzalez Reyes Sara Dolores sgonzalezr@upse.edu.ec
Ruth Reyes Sorianorreyess@upse.edu.ec

DIRECCIÓN DE CARRERA DE EDUCACIÓN BÁSICA
carrera_educacion_basica@upse.edu.ec
Director de Carrera de Educación Básica: Puya Lino Anibal Javier apuya@upse.edu.ec
De La Cruz Tigrero, Maria Del Pilar mdelacruzt@upse.edu.ec

Particular que comunico a usted, para los fines pertinentes.

Atentamente,

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE CIENCIAS DE LA EDUCACIÓN E IDIOMAS

Lic. Sara González Reyes, MSc.
DECANA
FACULTAD DE CIENCIAS DE LA EDUCACIÓN E IDIOMAS

UPSE
CARRERA TECNOLOGÍAS DE LA INFORMACIÓN
RECIBIDO
HORA 12:21
05 JUL 2022
FIRMA AUTORIZADA

C.c.: **DIRECCIÓN DE CARRERA DE EDUCACIÓN BÁSICA**
DIRECCIÓN DE CARRERA DE EDUCACIÓN INICIAL
DIRECCIÓN DE CARRERA DE PINE
Archivo
SGR/MJQ.

La Libertad, 06 de octubre de 2022

CERTIFICADO ANTIPLAGIO

En calidad de tutora del trabajo de titulación denominado **"ingeniería social en una institución de educación superior aplicando técnicas computacionales y no computacionales"**, elaborado por el estudiante, **Peñafiel Suárez Marcelo Rodrigo** , egresado de la **Carrera de tecnologías de la información**, de la **Facultad de Sistemas y Telecomunicaciones** de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniera en tecnologías de la información , me permito declarar que una vez analizado en el sistema antiplagio URKUND, luego de haber cumplido los requerimientos exigidos de valoración, el presente proyecto ejecutado, se encuentra con 4% de la valoración permitida, por consiguiente se procede a emitir el presente informe.

Adjunto reporte de similitud.

Atentamente,

Ing. Lidice Haz López, Msi.
DOCENTE TUTORA

Reporte Urkund.

Document Information

Analyzed document	ProyectoUIC MarceloPeñafiel.docx (D142642635)
Submitted	8/4/2022 1:08:00 AM
Submitted by	
Submitter email	marcelo.penafielsuarez@upse.edu.ec
Similarity	4%
Analysis address	lhaz.upse@analysis.urkund.com

Fuentes de similitud

Sources included in the report

W	URL: https://virtualeduca.org/mediacenter/los-retos-de-seguridad-informatica-que-enfrentan-las-instituciones-educativas-colombianas/ Fetched: 8/4/2022 1:08:00 AM
W	URL: https://www.sobretiza.com.ar/2014/09/24/la-seguridad-informatica-en-las-universidades/ Fetched: 8/4/2022 1:08:00 AM
SA	TrabajoSeminario-UO264637.pdf Document TrabajoSeminario-UO264637.pdf (D69797813)