Universitat Oberta de Catalunya

uoc.edu

Metodologías de Ingeniería Social

Ellien Yulieth Rodríguez Rincón
Máster Universitario en Seguridad de las TIC
Área del trabajo final - Ad hoc

Ángela María García Valdés
Junio/2018

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Metodologías de Ingeniería Social*
Nombre del autor:	*Ellien Yulieth Rodríguez Rincón*
Nombre del consultor/a:	*Ángela María García Valdés*
Nombre del PRA:	*Victor Garcia Font*
Fecha de entrega (mm/aaaa):	06/2018
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Informacion y de las Comunicaciones*
Área del Trabajo Final:	*Ad hoc*
Idioma del trabajo:	*Español*
Palabras clave	*Ingeniería Social, ataque, víctima.*

Resumen del Trabajo (máximo 250 palabras):

Para el presente trabajo de grado se evidenciará el estudio de las técnicas de Ingeniería Social, sus causas, consecuencias y métodos para proteger todo tipo de información, así mismo la legislación que persigue las acciones de la Ingeniería Social, siendo estos actos catalogados como delitos informáticos, también a través de esta investigación se concientizará y sensibilizará a los niños, niñas, adolescentes, padres de familia, empresas y sociedad en general, sobre el uso correcto de la tecnología, específicamente internet y redes sociales.

Se ejecutará un caso práctico de phishing enfocado en el juego minecraft para que sea ejecutado por niños, niñas y adolescentes, teniendo como referencia el auge de este juego.

La metodología utilizada será de tipo descriptiva donde a través de la investigación de los conceptos que abarca la Ingeniería social, por otro lado la fuente de información utilizada es la encuesta, con su correspondiente análisis y conclusiones.

A través de los resultados obtenidos de las encuestas realizadas se puede deducir que existe desconocimiento de la Ingeniería Social, por lo cual las personas fácilmente son víctimas de ataques informáticos, donde son inconscientes de las consecuencias que se pueden presentar. Por ello es fundamental tomar controles que permitan neutralizar y contrarrestar posibles

amenazas, es necesario estar a la defensiva.

Como conclusión principal se puede establecer que se llevó a cabo la campaña de concientización y sensibilización a adolescentes y adultos por medio de charlas programadas, utilizando medios de material didáctico y audiovisual para generar mayor impacto en la audiencia.

Abstract (in English, 250 words or less):

For the present work of degree it will be evident the study of the techniques of Social Engineering, its causes, consequences and methods to protect all type of information, likewise the legislation that pursues the actions of the Social Engineering, being these acts cataloged like computer crimes , also through this research will raise awareness and sensitize children, adolescents, parents, businesses and society in general, on the correct use of technology, specifically internet and social networks.

Sequence a practical case of phishing focused on the game minecraft so that the sea is played by children and adolescents, taking into account the use of this game.

The methodology used is descriptive through the investigation of concepts covered by social engineering, on the other hand, the source of information used in the survey, with its corresponding analysis and conclusions.

Through the results obtained from the surveys conducted, it can be deduced that there is ignorance of Social Engineering, why people are victims of computer attacks, where the consequences are inconsistent. Therefore it is essential to take the controls that allow neutralizing and counteract possible threats, it is necessary to be on the defensive.

As a main conclusion, it can be established that the awareness and awareness campaign was carried out for adolescents and adults through the programmed talks, using media of didactic and audiovisual material to generate a greater impact on the audience.

Índice

Capítulo 4 Metodología

4.1 Tipo de investigación

4.1.1 Población y muestra

4.1.2 Fuentes y técnicas de recolección de información

Capítulo 5 Marco legal

5.1 Nivel nacional

5.2 Nivel Internacional

Capítulo 6 Campaña de concientización

6.1 Diagnostico

6.2 Población

6.2 Medios y estrategias

6.4 Ejecución de la campaña

Capítulo 7 Recursos Disponibles

7.1 Recursos

7.2 Planificación y cronograma

7.3 Presupuesto

Capítulo 8 Resultados y evidencias

8.1 Caso práctico (simulación)

8.1.1 Recomendaciones del caso práctico

8.2 Resultados de la encuesta

8.2.1 Recomendaciones de las encuestas

Capítulo 9 Conclusiones

Glosario

Referencias Bibliográficas

Lista de figuras

Capítulo 1 Introducción

1.1 Introducción

El presente trabajo comprende el estudio de las metodologías de Ingeniería Social y métodos usados para obtener información, descubrir qué tipo de información puede llegar a obtenerse y cómo esta es utilizada para obtener beneficios.

Es importante que las personas y empresas estén alertas con esta temática, teniendo en cuenta que, al implementar medidas y controles estrictos, se puede evitar ser víctima de atacantes que busquen vulnerar los sistemas informáticos a través de diferentes técnicas y por diferentes motivos accediendo y obteniendo información relevante que pueda ocasionar daños irreversibles.

Por ello es necesario que la sociedad se concientice y genera cultura, sobre el uso correcto que se le debe dar a las tecnologías específicamente al internet y redes sociales, de esta forma se logra que las personas coadyuven para apoyar, orientar, neutralizar y contrarrestar los delitos que se ejecutan por medio de acciones correspondiente a Ingeniería Social y evitando que los atacantes cumplan con su misión.

1.2 Descripción del problema

Cada día son más comunes los ataques informáticos enfocados en la Ingeniería social caracterizándose en explotar la confianza del usuario para extraer información confidencial, por medio de diferentes técnicas como pretexting, tailgaiting, dumpster diving, shoulder surfing, baiting, phishing, vishing y redes sociales, con el objetivo de la instalación de algún tipo de malware para tomar el control del equipo, lograr la infiltración de personas a entidades, robo o suplantación de identidad, a través del engaño y manipulación psicológica e inocencia de las víctimas.

Específicamente en el caso del *phishing* su finalidad es el fraude, robo bancario, envío de virus, spam, robo de datos personales, suplantación de identidad, extorsión entre otros factores que pueden ser irremediables, a través de la duplicación y/o suplantación de sitios falsos, el engaño se realiza usualmente por medio de correos electrónicos que contienen enlaces de sitios falsos e idénticos a los originales, los usuarios engañados ingresan información importante y confidencial como número de identificación, contraseñas, datos bancarios, sin percatarse de lo sucedido, así mismo puede suceder al dar clic en alguna imagen o banner (archivo o programa infectado) que ha llegado al correo electrónico, alojando algún tipo de malware y de esta

manera violentar una vulnerabilidad del sistema, obteniendo el control y acceso remoto de dispositivos tecnológicos como el computador, celular, ipad, televisor, entre otros, por parte del atacante.

Actualmente la sociedad aún no es consciente de los riesgos que trae consigo la Ingeniería Social y cada una de sus técnicas en el momento que son llevadas a cabo; en el caso de los niños y adolescentes, hoy en día viven en un mundo lleno de tecnología, donde no son conscientes del uso correcto que se debe dar a las redes sociales, correo electrónico e internet, es por ello que se evidencian casos de cyberbulling, ciberacoso, grooming, sextortion, ocasionando daños psicológicos irremediables y situaciones que muchas veces se salen de las manos.
Es necesario tomar las medidas pertinentes y necesarias para evitar que se presenten casos de Ingeniería Social en niños, niñas, adolescentes, adultos y empresas, los cuales no saben cómo actuar y muchas veces callan por miedo o vergüenza, sin encontrar solución alguna, accediendo a las peticiones que solicite el atacante.

1.3 Justificación

Con el paso del tiempo la tecnología y el internet han sido de gran importancia a nivel mundial, sus múltiples avances que han logrado facilitar la vida de las personas respecto a comunicación, interacción, obtención de información, enseñanza, aprendizaje, empleo, entre otros, más sin embargo el incorrecto uso de la tecnología e Internet por parte de personas inescrupulosas trae consigo aspectos negativos que afectan a personas inocentes en este caso por medio de diferentes técnicas de Ingeniería Social atacando a las víctimas sin consideración alguna.

De acuerdo con un estudio realizado durante el año 2017 correspondiente a la empresa ESET Security se puede evidenciar las infecciones de malware en las empresas específicamente de troyanos valiéndose de técnicas de Ingeniería Social, dedicados a robar información de los equipos de las víctimas en diferentes países latinoamericanos, en el caso de Nicaragua ocupa el primer lugar con el 53%, seguido de Panamá con el 50,3% y Colombia con 46,7%.

Remtasu, una familia de troyanos dedicada a robar información sensible de los equipos de las víctimas, tuvo una importante actividad en Colombia a través campañas que se valían de técnicas de Ingeniería Social.

En cuanto a casos de ataques dirigidos a personas, se identificó una escalada que intentaba imitar el sitio de **Visa** para robar datos de los usuarios. Días después surgió una nueva campaña que involucraba a **MasterCard**; a partir

de correos falsos se invitaba a los usuarios a reactivar un supuesto servicio al acceder a un sitio no auténtico. Si el usuario caía en el engaño, toda la información relacionada con su tarjeta de crédito podía ser obtenida por los atacantes.
Sin embargo, las instituciones financieras y bancarias no son las únicas que pueden ser utilizadas como señuelos para afectar a los usuarios, ya que otras organizaciones de renombre también han sido suplantadas. Tal es el caso de **Apple**, **Mercado Libre** e incluso de servicios de redes sociales como **Facebook**, donde los usuarios más afectados fueron de Argentina, México y Colombia.

De esta forma el presente trabajo permitirá conocer y diferenciar las técnicas de Ingeniería Social, así mismo contribuir a mitigar y/o contrarrestar esta problemática a través de la aplicación del caso práctico y recomendaciones a seguir para evitar ser víctimas de los atacantes, es de tener en cuenta que el caso práctico es uno de tantos casos que pueden existir, lo fundamental es crear conciencia en las personas y empresas sobre la importancia de establecer una estrategia de seguridad que les permita protegerse.

1.4 Objetivos

1.4.1 Objetivo general

- Evidenciar el estudio de las técnicas de Ingeniería Social, sus causas, consecuencias y métodos para proteger todo tipo de información.

1.4.2 Objetivos específicos

- Concientizar y sensibilizar a los niños, niñas, adolescentes y padres de familia sobre el uso correcto de la tecnología, específicamente de redes sociales y correo electrónico, así mismo a las empresas, sus funcionarios y demás personas.

- Analizar las metodologías actuales de la Ingeniería Social e identificar los antecedentes que se han presentado en la sociedad.

- Establecer estrategias preventivas que permitan a los usuarios navegar de forma segura e identificar algún tipo de ataque correspondiente a Ingeniería Social y de esta forma saber que hacer al respecto.

- Evidenciar la normatividad y/o leyes que persigue las actividades relacionadas con la Ingeniería Social.

1.5 Viabilidad

1.5.1 Técnica

Teniendo en cuenta el tiempo de entrega del proyecto de grado correspondiente a la temática de metodologías de Ingeniería social se entregará la simulación de un tipo de ataque de las técnicas de Ingeniería social, en este caso phishing, debido a que para realizar algún tipo de ataque informático real, requiere de mayor tiempo de dedicación para su posterior desarrollo, ejecución y monitoreo, más sin embrago es de tener en cuenta que el proyecto reúne las características, condiciones técnicas y operativas que aseguran el cumplimiento de las metas y objetivos.

1.5.2 Económica

Este factor no afecta en el proyecto teniendo en cuenta que se realizará una simulación de las técnicas de la ingeniería social, por lo cual no genera ningún tipo de gasto monetario.

1.5.3 Organizacional

El personal determinado para el diseño e implementación del proyecto en marcha cuenta con la formación necesaria para ejercer cada una de las actividades relacionadas con las técnicas de ingeniería social a ejecutar, así mismo se cuenta con infraestructura adecuada para que el resultado final sea todo un éxito.

Capítulo 2 Estado del Arte

2.1 Estado del arte

El avance de las tecnologías es imparable, a través de los años la humanidad ha tenido grandes cambios en sus vidas satisfaciendo así sus necesidades en el ámbito profesional, personal, laboral y social, e incluso para subsistir; pasar a conectarse a internet por medio de un CD a conectarse a una red wifi es uno de los grandes avances que se ha generado. A pesar de que la tecnología ha traído consigo grandes beneficios, también cuenta con su lado oscuro siendo peligrosa para las personas que hacen uso de ella y más que todo para aquellas personas que no saben dar el uso correcto, cayendo en las redes de personas inescrupulosas cuyas consecuencias pueden llegar hacer irreversibles.

Es por ello que en los últimos años ha aumentado del número de investigaciones respecto a las metodologías de Ingeniera Social, exponiendo los ataques informáticos realizados a través de la diversidad de técnicas, tal y como se evidencian a continuación:

IDENTIFICACIÓN	OBJETIVO GENERAL	CATEGORIAS/ VARIABLES	INTRUMENTOS RECOLECCIÓN DE INFORMACIÓN	RESULTADO
Salazar Natalia, González Marcela, "Phishing: La automatización de la ingeniería social", proyecto de grado, Universidad EAFIT, Medellín, 2007.	Documentar estrategias, de navegación, que permitan a los usuarios de Internet detectar cuando son víctimas de ataques de phishing, con el fin de evitar captura de información.	Ingeniería Social Phishing Información Fraude Entidades bancarias	Información existente en la web a cerca de las entidades financieras nacionales e internacionales.	Generación de estrategias preventivas que le permitieran al cibernauta navegar de una forma segura.
Solanas Vanrell, María del Carmen, "Estudio de las técnicas de la ingeniería social usadas en ataques de ciberseguridad y análisis sociológico", proyecto fin de grado, Universidad Politécnica de Madrid, 2015.	Recopilar toda la información posible acerca de las diferentes técnicas que usan los hackers en ataques basados en Ingeniería Social. Se cree necesario aclarar en qué consiste cada técnica ya que diversas fuentes de información pueden confundir al usuario debido a los diferentes enfoques y definiciones que hay en cada una de ellas	Ingeniería Social Estudio sociológico Campaña de concienciación	Información existente en la web acerca de las técnicas de la ingeniería social usadas en ataques de ciberseguridad y análisis sociológico.	Profundizar en un tema que tiene el peligro ser olvidado o menospreciado por algunos expertos de la seguridad, de igual forma concientizar a los empleados de las empresas, a través de conferencias donde se evidenciaron diferentes tipos de ataques.
Zabala, Alexander, "Responsabilidad Bancaria frente al delito de phishing en Colombia", trabajo de grado, Universidad Católica de Colombia, 2017.	Analizar la controversia de hasta dónde las entidades financieras tienen responsabilidad objetiva frente a sus clientes, cuando se comete un delito por un tercero, es decir, por la ciberdelincuencia, una aproximación desde la perspectiva del derecho y la legislación vigente.	Ciberdelito Responsabilidad Bancaria derechos del consumidor Responsabilidad Objetiva derechos del consumidor	Metodología de forma investigativa ejecutando una clasificación axial de la información obtenida, para después proceder a darle una estructuración lógica.	La responsabilidad del sistema bancario frente al phishing en Colombia, indican que el problema representa un permanente desafío para el Estado, la comunidad internacional y los organismos especializados, así como la comunidad académica, en sentar jurisprudencia y actualización normativa para poder hacer frente a la problemática de la ciberdelincuencia que, con sus ataques, genera graves perjuicios al sector empresarial y a usuarios y consumidor.

2.1.1 Antecedentes

2.1.1.1 A nivel nacional

- **2016 (Quien usaba a su propia hija):** Este ingeniero industrial de 40 años fue capturado por las autoridades en el barrio Ciudad Jardín (Cali) a comienzos de marzo. Su principal característica consistió en crear un perfil falso en Facebook, en el cual utilizaba el nombre y las fotografías de su propia hija de 11 años.

  Gracias a esta página ganaba la confianza de niñas de edades similares a quienes, a través de engaños, les pedía fotografías desnudas o en ropa interior. Una vez recibía las imágenes, amenazaba a sus víctimas con publicarlas a menos que se encontraran personalmente con él en algún lugar público de la ciudad.

  El hombre las obligaba a ir a moteles de Cali, donde ingresaba en un automóvil de vidrios polarizados, con el cual impedía que los empleados de esos establecimientos pudieran percatarse de la edad de sus acompañantes. Al momento de su arresto, tenía dos computadores, dos discos duros y varias memorias USB con material pornográfico.

  La captura se produjo gracias a la denuncia de la madre de una de sus víctimas, quien se percató de la situación y acudió a las autoridades.

- **2017 (Red explotación sexual):** Para el año 2017 desarticulan una red de explotación sexual con menores de edad, las niñas eran contactadas por redes sociales y con engaños eran persuadidas por los integrantes de la red, para ser trasladadas a Carmen de Apicalá y a Cunday (Tolima), donde las explotaban sexualmente. Las víctimas eran ubicadas desde Bogotá y Soacha, por tres mujeres, a las que les pagaban 100 mil pesos por cada niña que enganchaban.

- **2018 (Suplantación de identidad):** Un ciberdelincuente se hizo pasar por el futbolista James Rodríguez a través de redes sociales y logró que periodistas y hasta gente famosa le dieran información personal.

  Ese día la cuenta de Twitter del crack del Bayern Múnich tuvo un movimiento inusual. Supuestamente, James siguió y dio ‘likes’ a más de 40 cuentas, además envió por mensaje directo un número de celular para chatear con ellos por WhatsApp.

  Tal fue el éxtasis de tener a James como amigo que muchos accedieron a compartirle las claves y correos electrónicos al ‘jugador’ sin dudarlo. Supuestamente el ‘10’ se las pidió porque necesitaba enviar algunos documentos de urgencia.

Con esta información, el ciberdelincuente de 23 años que se hizo pasar por el futbolista, se robó las cuentas y las usó para ofrecer “productos tecnológicos, celulares, e inclusive fichajes en Europa”, como lo cuenta Óscar Castillo, abogado de las víctimas.

“Se estableció que un ciudadano haciendo uso de la ingeniería social logró acceder a la cuenta oficial de Twitter de James Rodríguez. Una vez tiene control de esta cuenta lo que hace es comunicarse con otros jugadores o con otras figuras públicas de este gremio para pedirles el favor de que les preste algún tipo de cuenta de correo electrónico y tomar control de otra serie de cuentas o de redes sociales”, agregó el defensor.

El ciberdelincuente de 23 años fue capturado y en audiencia aceptó los delitos de acceso abusivo a un sistema informático, violación de datos personales y transferencia no consentida de activos.

2.1.1.2 A nivel internacional

- **2016 (Cuidado con los ladrones ‘surfistas’ en el ATM, los Ángeles (California)):** El ardid es simple, alguien espía cuando pones tu PIN (código) en el cajero automático y cuando acabas tu transacción, pero justo antes de que la máquina regrese al punto inicial, llegan y la usan para sacarte dinero de tu cuenta. O bien, colocan dispositivos especiales para copiar datos de las tarjetas financieras y de pequeñas cámaras de video.
  En inglés le llaman a esto “shoulder surfing” y es un problema que está pasando con frecuencia en Los Ángeles, advirtió el procurador municipal.

  Es la advertencia de la Procuraduría donde presentó cargos contra dos hombres acusados de robar dinero a dos personas que espiaron para obtener las claves de sus tarjetas bancarias.

  Si parece que hay algo que no es parte del resto del ATM [cajero automático], si se mueve, puede que sea un fraude”, dijo el funcionario, alertando que podría tratarse de un dispositivo que obtiene la información de la tarjeta bancaria.
  “También revise si hay cámaras de video externas, es posible que individuos busquen robar información poniendo cámaras pequeñas en los ATM”, agregó.

  Feuer mencionó que esta práctica ilegal se ha extendido por todo el estado. “La víctima ni se entera de lo que pasó hasta que es demasiado tarde”, señaló el fiscal.

- **2017 (Felicia García fue acosada mediante la difusión de un vídeo sexual por Internet)** Una joven de 15 años de edad, residente de Estado Unidos, se suicidó por ser víctima de ciberbullying. Fue porque se difundieron varias imágenes sexuales de ella, tomadas de un vídeo el cual también fue difundido. En el vídeo se mostraba a la chica teniendo relaciones sexuales con 4 chicos de entre 15 y 17 años, los cuales evidentemente grabaron el acto y lo difundieron en las redes sociales, exponiendo a la chica ante los ojos de mucha gente. No pasaron muchos días después de lo sucedido cuando la víctima decidió quitarse la vida arrojándose a las vías de un tren.

  Esta chica antes de quitarse la vida había sido víctima de casos de ciberbullying de distintas formas. Ya que usualmente insultos por medio de Facebook.

  Actualmente los chicos que se muestran en el vídeo están en libertad. Es porque en el vídeo no hay señal de violación o forcejeo, ella tuvo las relaciones por su propia voluntad. Sin embargo, el caso se está investigando todavía.

- **2018 (Nuevo caso de vishing contra usuarios de HSBC):** La Condusef detectó un nuevo caso de vishing contra los usuarios de la banca por Internet de HSBC, en el que se les informa de una supuesta desactivación de la tarjeta bancaria y se les solicita la validación de su identidad.

  En un comunicado, el organismo explicó que a través de un mensaje de texto (SMS) se le indica al tarjetahabiente que su plástico fue desactivado por seguridad, y que para activarlo de nuevo debe validar su identidad.

  No obstante, el objetivo de esto es obtener datos personales y bancarios de titular y “vaciar su cuenta, o realizar consumos con cargo a la tarjeta o a la cuenta del usuario”.

  Cabe señalar que el número telefónico del remitente es el 221 275 1296.

Capítulo 3 Técnicas de Ingeniería Social

3.1 ¿Qué es Ingeniería Social?

Es el "arte del engaño", hace referencia al arte de manipular personas para eludir los sistemas de seguridad, consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo.

3.1.1 Técnicas de Ingeniería Social

3.1.1.1 Pretexting

Se presenta cuando un supuesto representante de una institución financiera, de una compañía de teléfonos o algún otro servicio, pregunta por información de la cuenta del cliente.

3.1.1.2 Tailgaiting

Aprovechando la solidaridad o inconsciencia de un empleado, un atacante puede evadir controles de acceso físico como puertas electrónicas e ingresar a una organización sin autorización.

3.1.1.3 Dumpster diving

Se refiere al acto de husmear entre la basura, de esta manera se pueden obtener documentos con información personal o financiera de una persona.

3.1.1.4 Shoulder surfing

Consiste en mirar por encima del hombro a un usuario descuidado mientras ingresa el patrón de desbloqueo, pin o alguna otra contraseña.

3.1.1.5 Baiting

Técnica que consiste en colocar memorias externas con malware instalado en lugares donde personas escogidas específicamente puedan encontrarlo e infectar sus ordenadores.

3.1.1.6 Phishing

Consiste en engañar a un grupo masivo de personas mediante correos electrónicos, páginas web, perfiles sociales o sms falsos con fin de robar información confidencial.

3.1.1.7 Vishing

Llamadas telefónicas mediante las que se buscan engañar a la víctima suplantando a compañías de servicios o de gobierno para que revele información privada

3.1.1.8 Redes sociales

Es una técnica que tiene dos grandes objetivos, por un lado, obtener información de la víctima y por otro lado generar una relación con la misma por otro.

Existen muchas personas “fanáticas” de las redes sociales, las cuales dan a conocer su vida minuto a minuto, en este caso este tipo de persona es “Oro en Polvo” para los atacantes ya que si la misma es el objetivo se podrá obtener muchísima información que será de gran utilidad.

3.1.1.9 Ciberbullyng/Ciberacoso

Engloba el uso de las tecnologías de información y comunicación, para causar daño de manera repetida, deliberada y hostil. Esto puede incluir, pero no limitarse, al uso de Internet, teléfonos móviles u otros dispositivos electrónicos para difundir o colocar textos o imágenes que dañan o avergüenzan a una persona.

3.1.1.10 Grooming

Conjunto de estrategias que una persona adulta realiza para ganarse la confianza de un niño, niña o adolescente, a través del uso de las tecnologías de la comunicación información, con el propósito de abusar o explotar sexualmente de él o ella. El adulto suele crear un perfil falso en una red social, foro, sala de chat u otro, se hace pasar por un chico o una chica y entablan una relación de amistad y confianza con el niño o niña con la intención de acosarlo.

3.1.1.11 Sexting

Comprende el envío y/o recepción de contenido sexual a través de medios electrónicos. El mismo consiste en el intercambio de imágenes y vídeos sexuales a través de mensajes, redes sociales, e-mail y sobre todo con el teléfono móvil.

3.1.1.12 Sextortion

Forma de extorsión en la que se chantajea a una persona por medio de una imagen o vídeo de sí misma desnuda, que puedo a ver compartido a través de Internet o mensajes. La víctima es coaccionada a ejecutar acciones que den gratificación sexual al malhechor (tener relaciones sexuales con el chantajista, producir pornografía u otras acciones que ponen en serio peligro a la víctima).

3.1.2 Técnicas en función de la interacción que se tiene con la víctima

3.1.2.1 Pasivas

Se basan en la observación y el análisis del comportamiento de la víctima, con el fin de establecer un perfil psicológico, sus gustos, aficiones y hábitos.

3.1.2.2 No presenciales

Son aquellas que, basándose en solicitudes de información, mediante llamadas telefónicas, correos electrónicos, suplantación de identidad digital, etc., tratan de obtener información de la víctima. Esta es la técnica de ingeniera social más extendida (El Phishing forma parte de esta categoría).

3.1.2.3 Presenciales no agresivas

Se basan en el seguimiento de la víctima. Aquí se incluye la vigilancia de domicilios, la búsqueda de información en su entorno (oficina, libretas, vecinos, basura, etc.).

3.1.2.4 Agresivas

Se basan en la presión psicológica y suplantación de identidad física ya sea de la propia víctima, como de familiares o técnicos de compañías de servicios.

Capítulo 4 Metodología

4.1 Tipo de investigación

La metodología utilizada para la elaboración del presente trabajo de grado, es de tipo descriptiva donde a través de la investigación del concepto de Ingeniería social, los roles, sus características, métodos, estrategias, tipo de información que un atacante puede obtener, los riesgos que se pueden presentar al ser víctima por algún tipo de técnica y ataque recibido, recomendaciones si fue, está o ha sido víctima de Ingeniería Social, así como las leyes que persiguen esta temática, se podrá recoleccionar y analizar la información de casos reales que se han presentado, cuáles han sido sus consecuencias y aprendizaje de ello.

4.1.1 Población y muestra

En el caso de la simulación la población serán los niños, niñas y adolescentes de algunos colegios, "*de acuerdo al código de la infancia y la adolescencia "ley 1098/2006", expedido por el congreso de Colombia, Artículo 3°. Sujetos titulares de derechos, sin perjuicio de lo establecido en el artículo 34 del Código Civil, especifica que se entiende por* ***niño o niña*** *las personas entre los* ***0 y los 12 años****, y por* ***adolescente*** *las personas entre* ***12 y 18 años*** *de edad".*
Específicamente los *niños o niñas* entre la edad de 10 y 11 años pertenecientes a los grados 5° de primaria y 6° de bachillerato, así mismo los *adolescentes* estarán entre el rango de edad 12 a los 16 años de edad, correspondientes entre a los grados de 7° a 11° de bachillerato, de acuerdo a lo anterior *la información fue tenida en cuenta del Ministerio de Educación de Colombia (Sistema Nacional de indicadores educativos para los niveles de preescolar, básica y media en Colombia), correspondiente a la Clasificación Internacional para la Normalización de la Educación.*

De modo general el proyecto de grado es dirigido a todas las personas que tengan acceso a internet, teniendo en cuenta que pueden ser víctimas latentes de un atacante informático.

4.1.2 Fuentes y técnicas de recolección de información

Los instrumentos de recolección de información utilizados serán las encuestas teniendo en cuenta el tema de investigación correspondiente a metodologías de Ingeniería Social.

Capítulo 5 Marco legal

5.1 Nivel nacional

NORMATIVIDAD	NOMBRE	DESCRIPCIÓN
Ley 1273 de 2009	Delitos Informáticos	Con esta nueva ley se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
Ley 109 2010	Por la cual se consagra la edad mínima para registrarse y ser miembro de redes sociales en internet	Muchos son los niños y niñas menores de 14 años que tienen abierto un perfil en alguna red social, lo cual es probable que muchos adultos no le den importancia a este tema, como también es probable que muchos padres y madres no saben que en Colombia existe una ley, denominada ley 109 de 2010 del Congreso de la República de Colombia, por la cual se consagra la edad mínima para registrarse y ser miembro de redes sociales en internet.

5.2 Nivel Internacional

NORMATIVIDAD	NOMBRE	DESCRIPCIÓN
Ley Orgánica No. 10/1995	Delitos Informáticos (España)	Código Penal. /Título X - Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Capítulo I - Del descubrimiento y revelación de secretos. Artículos 197 y 198. Título XI - Delitos contra el honor Capítulo III - Disposiciones generales. Artículos 200 y 201. Título XI - Delitos contra el honor. Capítulo III - Disposiciones generales. Artículos 211 y 212. Título XIII - Delitos contra el patrimonio y contra el orden socioeconómico. Capítulo II - De los robos. Artículos 238 y 239. Capítulo VI - De las defraudaciones. Sección 1ª - De las estafas. Artículos 248, 255, 256, 263 y 264. Capítulo XI - De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores. Sección 1ª - De los delitos relativos a la propiedad intelectual. Artículos 270 y 278. Título XVIII - De las falsedades. Capítulo III - Disposiciones generales. Artículo 400. Capítulo V - De los delitos cometidos por los funcionarios públicos contra las garantías Constitucionales. Sección 2ª - De los delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad.

Capítulo 6 Campaña de concientización

6.1 Diagnóstico

En primer lugar, se debe detectar la temática para trabajar en la Campaña de concientización en este caso será las *metodologías de Ingeniería Social*.

Actividades a realizar:

- Realizar encuestas a adolescentes y adultos sobre *metodologías de Ingeniería Social* con el fin de determinar el conocimiento que tiene al respecto del tema.

- Llevar a cabo el análisis de información de acuerdo a los resultados obtenidos de las encuestas

- Cumplir estrictamente con el calendario de concientización y sensibilización tema de seguridad.

6.2 Población

Para este caso en la campaña de concientización y sensibilización la población serán adolescentes y adultos los cuales alguno de ellos son padres de familia, a su vez esta población será una guía para ayudar a prevenir a la población en general sobre la temática de la concientización.

6.3 Medios y estrategias

1. Realizar conferencias, capacitaciones, charlas y/o talleres donde se evidencien casos reales presentados sobre la problemática de Ingeniería Social.

2. Utilizar material didáctico y audiovisual, con el fin de que la campaña genere mayor impacto.

3. Tener un lenguaje claro y entendible en el contenido de la temática abordar.

6.4. Ejecución de la campaña

- **Agenda de charlas**

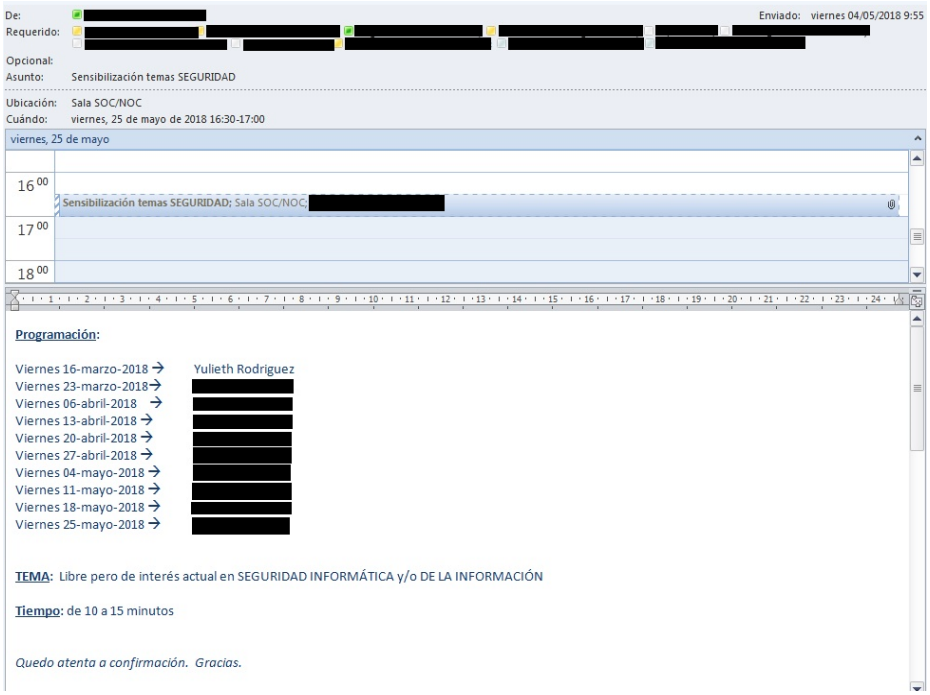


Ilustración 1 Cronograma charlas

Una vez realizado el cronograma para dictar las charlas, estas se llevaron a cabo al personal de adolescentes y adultos, donde los temas eran libres pero de interés actual en Seguridad Informática y/o Información.

Respecto al tema de concientización a continuación se puede evidenciar alguno de los materiales expuestos en las charlas.

Ilustración 2 Ingeniería Social

Ilustración 3 Folleto Ingeniería Social

Ilustración 4 Presentación tipos de hackers

QUE ES UN HACKER

Persona experta en alguna rama de la tecnología, se dedica a intervenir o realizar alteraciones técnicas con buenas o malas intenciones.

. Viene desde 1960 por un grupo de pioneros del MIT y proviene de "hack", el sonido que hacían técnicos de las empresas telefónicas al golpear los aparatos

TIPOS DE HACKERS

WHITE HAT

Hacker de sombrero blanco se refiere a un hacker ético, que se centra en asegurar y proteger los sistemas de Tecnologías de información y comunicación. Estas personas suelen trabajar para diversas empresas de informática.

BLACK HAT

Hacker de sombrero negro, es un hacker no ético, muestran sus habilidades en informática rompiendo, sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, También son llamados "crackers".

GREY HAT

Hacker de sombrero gris, es un hacker neutral, puede realizar actividades delictivas o dentro de la ley, este tipo de hacker se destaca muchas veces por "romper" un sistema informático con el único fin de notificar al administrador que su sistema ha sido crackeado, luego se ofrece para reparar su sistema por interés económico.

HACKTIVISTA

Es un hacker que utiliza la tecnología para anunciar un mensaje social, ideológico o político, utiliza las mismas herramientas y técnicas de un hacker, pero lo hace con el fin de interrumpir los servicios y brindar atención a una causa política o social.

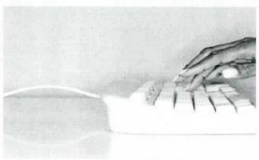
LAMMER O SCRIPT KIDDIES

Son inexpertos que irrumpen en los sistemas informáticos mediante el uso de herramientas automatizadas y escritas por otros. Son aprendices que presumen ser lo que no son.

PHREAKER

Son personas con conocimientos en sistemas telefónicos, telefonía móvil, tecnologías inalámbricas y el Voz sobre IP (VoIP). Por lo general trabajan en el mercado negro de celulares, desbloqueando, clonando o programando nuevamente los celulares robados.

Ilustración 5 Documento tipos de hackers



Proceso de ataque

Estudio de la víctima
Al tratarse de un ataque específico dirigido, el atacante debe conocer en profundidad su objetivo, desde la configuración de los sistemas hasta sus políticas de seguridad. Esto le permite elegir el punto más débil en la cadena para atacar. → Aquí se deducen las empresas, vulnerabilidades

Infección
Consiste en instalarse o esconderse en alguna máquina de la red interna, desde donde se intenta obtener el objetivo deseado (la información). Esta máquina puede infectarse ejecutando un simple archivo, que contiene las instrucciones para futuras etapas de la infección. También incluye la lógica necesaria para descargar nuevas funcionalidades, si fuesen necesarias. → identificar modelo a través de Phishing

Propagación
Una vez infectado un equipo o sistema, la propagación consiste en extenderse a más equipos, ya sean en la red colindante (LAN) o a través de Internet. Con esto se consigue más información. Como contrapartida, el atacante asume un mayor riesgo a ser detectado. → por medio de red a varios equipos

Etapas de las APT´S

Una amenaza persistente avanzada típica puede componerse de las cuatro etapas siguientes:

- **Reconocimiento:** Investigación de las vulnerabilidades de una organización. Esto puede incluir la investigación básica, incluida las consultas de dominios, sobre los análisis de puertos y vulnerabilidades
- **Entrada inicial:** Aprovechamiento de las debilidades para obtener un punto de apoyo en la red objetivo. Puede llevarse a cabo mediante métodos técnicos sofisticados o técnicas como el spear phishing (ataques directos de phishing) que tienen como resultado el acceso habitual de un usuario a un único sistema. La ingeniería social, o el aprovechamiento de las personas, es también otro método común para obtener acceso.
- **La elevación de los privilegios y la expansión del control:** Una vez que el atacante penetra en el perímetro de la red, intenta obtener privilegios adicionales y lograr el control sobre sistemas importantes. Este paso también puede suponer la instalación de herramientas de puerta trasera para simplificar el acceso futuro a la red.
- **Aprovechamiento continuo:** Una vez que se ha establecido el control, un atacante puede exportar continuamente datos confidenciales. La tercera y cuarta etapas pueden suceder

Privilegios de administrador

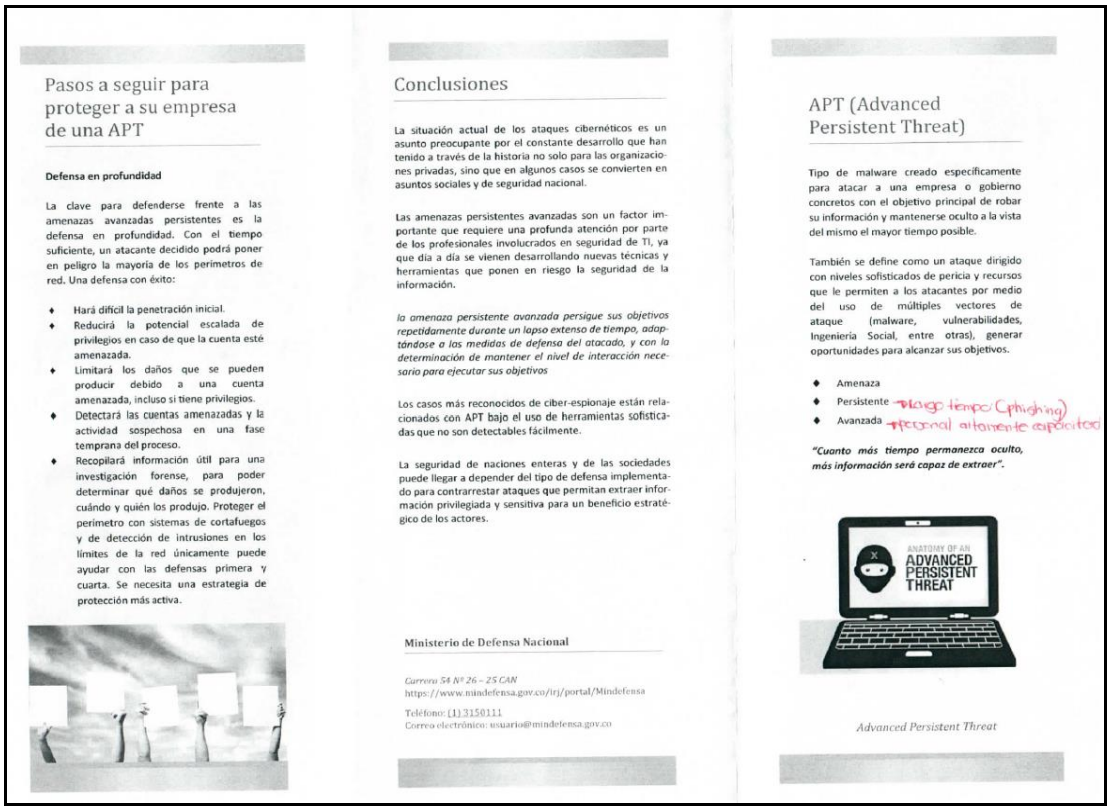
¿Cómo ingresa una APT dentro de la empresa?

Las APTs logran ingresar dentro de las empresas a través de distintos vectores de infección, incluso en aquellos escenarios protegidos con buenas estrategias de seguridad. Al menos pueden distinguirse tres grandes grupos o vectores de introducción de una APT en una organización:

- **Infección de malware proveniente de Internet**
- **Infección de malware por medios "físicos"**
- **Infección por exploit externo.**

Indicios de ataque de un APT

- Incremento en el flujo de datos a través de internet.
- Aumento en el volumen de información provocado por las copias de datos que se realizan durante el ataque.
- Aparición de ficheros extraños o desconocidos.
- La detección puntual de virus o troyanos en alguno de nuestros ordenadores.



Pasos a seguir para proteger a su empresa de una APT

Defensa en profundidad

La clave para defenderse frente a las amenazas avanzadas persistentes es la defensa en profundidad. Con el tiempo suficiente, un atacante decidido podrá poner en peligro la mayoría de los perímetros de red. Una defensa con éxito:

- Hará difícil la penetración inicial.
- Reducirá la potencial escalada de privilegios en caso de que la cuenta esté amenazada.
- Limitará los daños que se pueden producir debido a una cuenta amenazada, incluso si tiene privilegios.
- Detectará las cuentas amenazadas y la actividad sospechosa en una fase temprana del proceso.
- Recopilará información útil para una investigación forense, para poder determinar qué daños se produjeron, cuándo y quién los produjo. Proteger el perímetro con sistemas de cortafuegos y de detección de intrusiones en los límites de la red únicamente puede ayudar con las defensas primera y cuarta. Se necesita una estrategia de protección más activa.

Conclusiones

La situación actual de los ataques cibernéticos es un asunto preocupante por el constante desarrollo que han tenido a través de la historia no solo para las organizaciones privadas, sino que en algunos casos se convierten en asuntos sociales y de seguridad nacional.

Las amenazas persistentes avanzadas son un factor importante que requiere una profunda atención por parte de los profesionales involucrados en seguridad de TI, ya que día a día se vienen desarrollando nuevas técnicas y herramientas que ponen en riesgo la seguridad de la información.

la amenaza persistente avanzada persigue sus objetivos repetidamente durante un lapso extenso de tiempo, adaptándose a las medidas de defensa del atacado, y con la determinación de mantener el nivel de interacción necesario para ejecutar sus objetivos

Los casos más reconocidos de ciber-espionaje están relacionados con APT bajo el uso de herramientas sofisticadas que no son detectables fácilmente.

La seguridad de naciones enteras y de las sociedades puede llegar a depender del tipo de defensa implementado para contrarrestar ataques que permitan extraer información privilegiada y sensitiva para un beneficio estratégico de los actores.

Ministerio de Defensa Nacional

Carrera 54 N° 26 – 25 CAN
https://www.mindefensa.gov.co/irj/portal/Mindefensa
Teléfono: (1) 3150111
Correo electrónico: usuario@mindefensa.gov.co

APT (Advanced Persistent Threat)

Tipo de malware creado específicamente para atacar a una empresa o gobierno concretos con el objetivo principal de robar su información y mantenerse oculto a la vista del mismo el mayor tiempo posible.

También se define como un ataque dirigido con niveles sofisticados de pericia y recursos que le permiten a los atacantes por medio del uso de múltiples vectores de ataque (malware, vulnerabilidades, Ingeniería Social, entre otras), generar oportunidades para alcanzar sus objetivos.

- Amenaza
- Persistente
- Avanzada

"Cuanto más tiempo permanezca oculto, más información será capaz de extraer".

Advanced Persistent Threat

Ilustración 6 Folleto APT

Así mismo se recomiendan los siguientes tips las cuales ayudarán a profundizar la concientización y sensibilización de la temática expuesta, para niños, niñas, jóvenes y adultos dentro de los cuales se encuentran padres de familia.

- **Programa Mundo hacker:** Mundo Hacker es el único programa en el mundo donde hackers profesionales, no actores, cuentan cómo operan el cibercrimen y los cibercriminales en internet para cometer delitos. Y la vez siempre previene y dan las pautas para ayudar a los ciudadanos y las empresas a no ser la próxima víctima. Este programa es presentado en el canal trece en Colombia, específicamente los episodios 7 "Peligros de los menores en la red - 1ra parte" y 8 "Peligros de los menores en la red - 2da parte", hablan sobre la temática de Ingeniería Social en los menores de edad.

- **Bajemos el tono:** El Ministerio TIC de Colombia ha creado un espacio para promover la convivencia digital. En el podrás encontrar, descargar, crear y compartir contenido para responderle a los usuarios de redes sociales que utilizan lenguaje violento y agresivo.
  Tus creencias, ideas, costumbres o gustos sexuales, no son motivo para violentarte en redes sociales. Cuando insultamos y agredimos nos alejamos de la discusión principal. Por esto te invitamos a que hagas parte de este movimiento.

- **Enticconfio:** Es la estrategia de promoción de uso responsable de internet y de las nuevas tecnologías del Ministerio de las Tecnologías de la Información y las Comunicaciones. Ofrece a la ciudadanía herramientas para elevar su **#PoderDigital**: enfrentar los riesgos asociados al uso de nuevas tecnologías, como el grooming, el sexting, el phishing, el ciberacoso, la ciberdependencia y el material de abuso sexual infantil.

- **Red papaz:** Es una corporación sin ánimo de lucro fundada en el 2003 que tiene como propósito superior abogar por la protección de los derechos de niñas, niños y adolescentes en Colombia, y fortalecer las capacidades de los adultos y actores sociales para garantizar su efectivo cumplimiento.

- **Te protejo:** El 18 de mayo de 2012, en el marco del evento Escudos del Alma, se llevó a cabo el lanzamiento de *www.teprotejo.org*, la línea de denuncias para la protección de la infancia y adolescencia en Colombia, Te Protejo cuenta con un aplicativo móvil para equipos con sistemas operativos iOS, Android y BlackBerry con el fin de facilitar el proceso de denuncia, ya que los usuarios de teléfono móvil podrán informar sobre situaciones que afectan a menores de 18 años desde su dispositivo.

Capítulo 7 Recursos Disponibles

7.1 Recursos

7.1.1 TIC

- Servidor web (hosting).
- Dominio (www.xxxx.com).
- Base de datos (Almacenamiento de datos).
- Dispositivo tecnológico, con acceso a internet, que cuente con tecnología de punta – última generación, con el cual se realizará el seguimiento y monitoreo de las personas que han sido víctimas del ataque informático.
- Servidor de correo.
- Correo electrónico.

7.1.2 Humanos

- Diseñador web
- Web master

} Diseño de campaña

7.2 Planificación y cronograma

La planificación de tareas se realizó por medio de 5 etapas definidas de la siguiente forma: en la primera etapa se llevó a cabo el plan de trabajo, el cual incluye: identificación del problema, objetivos, metodología, tareas para alcanzar los objetivos descritos, planificación de tareas y dependencias, estado del arte, recursos necesarios, presupuesto del proyecto y análisis de viabilidad y riesgos, para la segunda etapa se realizó el diseño de la campaña del cual se desprenden tres fases: 1. Identificación del objetivo, 2. Reconocimiento del objetivo (qué, quién, cómo, cuándo, dónde, porqué, para qué), 3. Diseñar la campaña; la tercera etapa hace referencia a la ejecución correspondiente a la simulación del ataque informático de la técnica de Ingeniería Social, posteriormente en la cuarta etapa se realizó el análisis de la información obtenida y finalmente en la quinta etapa se entregó el informe final con los resultados, conclusiones y recomendaciones sobre la investigación relacionada con las metodologías de la Ingeniería Social.

ACTIVIDADES	CRONOGRAMA			
	Marzo	Abril	Mayo	Junio
Etapa 1: Plan de trabajo	**12**			
Etapa 2 y 3: Diseño de campaña y ejecución		**09**		
Etapa 4: Análisis de la información			**07**	
Etapa 5: Entrega Informe final				**04**

7.3 Presupuesto

En el caso que se vaya a realizar el diseño e implementación de algún tipo de ataque correspondiente a las técnicas de Ingeniería Social, el presupuesto aproximado sería el siguiente:

7.3.1 Recursos TIC

- Servidor web (hosting).

PLAN	ESPACIO	CORREOS CORPORATIVOS	CALIDAD CERTIFICADA
$92.250	5 GB	5	ISO 9001:2015
$180.000	20 GB	20	ISO 9001:2015
$285.000	40 GB	40	ISO 9001:2015
$516.750	60 GB	150	ISO 9001:2015

- *Dominio (www.xxx.com):* El dominio está incluido en el servidor web (hosting), pero si tal vez se requiere por aparte los costos son los siguientes:

NOMBRE DE DOMINIO	PRECIO POR 1 AÑO
.org	$68.359
.info	$68.359
.at	$72.059
.academy	$148.299
.apartments	$207.699
.cafe	$148.299
.careers	$207.699
.football	$88.919
.games	$88.919
.gratis	$88.919
.porn	$445.199
.viajes	$207.699
.university	$207.699

- *Servidor de correo y Base de datos (almacenamiento de datos)*

El servidor de correo cuenta con una o varias cuentas de correo y la Base de datos se encuentran incluidas dentro del servidor web (hosting), por lo cual se debe realizar la configuración pertinente en la administración del hosting para que sincronice el servidor de correo y la Base de datos.

7.3.1 Recursos humanos

PROFESION	SALARIO MENSUAL
1 - Diseñador web	De acuerdo al estudio de mercado realizado sobre el salario de un diseñador web oscila entre $1.500.000 a $3.000.000 teniendo en cuenta la experiencia.
1 - Web master	De acuerdo al estudio de mercado realizado sobre el salario de un diseñador web oscila entre $2.500.000 a $6.000.000 teniendo en cuenta la experiencia.

El rol del atacante será realizar el monitoreo, análisis y seguimiento del ataque realizado, esperando que personas terminan accediendo y de esta forma siendo víctimas de Ingeniería Social.

Capítulo 8 Resultados y evidencias

8.1 Caso práctico (simulación)

- FASE 1: Identificación del objetivo

En este caso el objetivo seleccionado serán los niños, niñas y adolescentes de algunos colegios, "*de acuerdo al código de la infancia y la adolescencia "ley 1098/2006", expedido por el congreso de Colombia, Artículo 3°. Sujetos titulares de derechos, sin perjuicio de lo establecido en el artículo 34 del Código Civil, especifica que se entiende por* ***niño o niña*** *las personas entre los* ***0 y los 12 años****, y por* ***adolescente*** *las personas entre* ***12 y 18 años*** *de edad".*

Pero en este caso el objetivo en el caso de *niños o niñas* será entre la edad de 10 y 11 años pertenecientes a los grados 5° de primaria y 6° de bachillerato, así mismo los *adolescentes* estarán entre el rango de edad 12 a los 16 años de edad, correspondientes entre a los grados de 7° a 11° de bachillerato, de acuerdo a lo anterior *la información fue tenida en cuenta del Ministerio de Educación de Colombia (Sistema Nacional de indicadores educativos para los niveles de preescolar, básica y media en Colombia), correspondiente a la Clasificación Internacional para la Normalización de la Educación.*

Fuente: MEN-OAPF
CINE: Clasificación Internacional para la Normalización de la Educación

Ilustración 7 Clasificación Internacional Normalización de Educación

- FASE 2: Reconocimiento de información del objetivo

  Teniendo en cuenta que el objetivo a atacar son *niños o niñas* entre la edad de 10 y 11 años pertenecientes a los grados 5° de primaria y 6° de bachillerato, así mismo los *adolescentes* estarán entre el rango de edad 12 a los 16 años de edad, correspondientes entre a los grados de 7° a 11° de bachillerato, es necesario dar respuesta a los interrogantes ¿qué?, ¿quién?, ¿cómo?, ¿cuándo?, ¿dónde?, ¿por qué?, ¿para qué?

  ☑ **¿Qué les gusta?:** Se debe identificar qué les gusta a los niños, niñas y adolescentes para llevar a cabo el diseño de la campaña, en este caso como por ejemplo pueden ser los juegos que están de moda o los más descargados en el último año, como por ejemplo: *Minecraf, Super Mario Run, Clash Royale,* Subway Sufres.
  ☑ **¿En quién confían?:** En sus redes sociales y cuentas de correo electrónico ya que están a nombre de ellos.
  ☑ **¿Cómo acceden a las TIC?** Pueden acceder a las TIC a través de su smartphone, computador o ipad.
  ☑ **¿Cuándo lo hacen?** Los niños, niñas y/o adolescentes lo pueden hacer en cualquier momento del día de su tiempo libre.
  ☑ **¿Dónde lo hacen?** Los niños, niñas y/o adolescentes lo harán en cualquier lugar puede ser desde el colegio, la casa o en la calle.
  ☑ **¿Por qué entrarían o darían clic en nuestra campaña** Los niños, niñas y/o adolescentes darían clic en la campaña por inocencia, confianza en sus redes sociales y cuentas de correo electrónico, desinformación, falta de cultura y concientización sobre los riesgos que conlleva el mal uso de la tecnología.
  ☑ **¿Para qué la necesitan?** Los niños, niñas y/o adolescentes, necesitarían los juegos por diversión, distracción y curiosidad.

- FASE 3: Diseñar la campaña

  Para llevar a cabo el diseño de la campaña es necesario contar con ciertos recursos tecnológicos y humanos, así:

  Recursos TIC

  - Servidor web (hosting).
  - Dominio (www.xxxx.com).
  - Base de datos (almacenamiento de datos niños, niñas y/o adolescentes).
  - Dispositivo tecnológico, con acceso a internet, que cuente con tecnología de punta – última generación, con el cual se realizará el seguimiento y monitoreo de las personas que han sido víctimas del ataque informático.
  - Servidor de correo.
  - Correo electrónico (ataque).

- Diseño de correo electrónico (campaña – Banner de publicidad).
- Lista de correos electrónicos de las víctimas, es este caso correspondiente a los niños, niñas y adolescentes de algunos colegios de forma seleccionada.

  ¿COMO LOS VOY A ADQUIRIR?, se podrían adquirir de 3 formas diferentes, así:

1) Solicitándolos de forma ética.
2) Sacándolos de internet (fuente pública).
3) Hackeando de forma seleccionada las Bases de datos pertenecientes a los colegios.

Recursos Humanos

- Diseñador web
- Web master

} Diseño de campaña

El diseño de la campaña se basará en una de las técnicas de Ingeniería Social *(phishing),* a través de un banner correspondiente al juego *minecraft* uno de los juegos más populares en Europa, Asia y en estos momentos en Colombia, el cual será enviado a los correos electrónicos de las víctimas intentando ganar confianza con ellos por medio del banner del juego muy similar al del sitio oficial, para que den clic en la imagen.

El diseño del banner *phishing* es el siguiente:

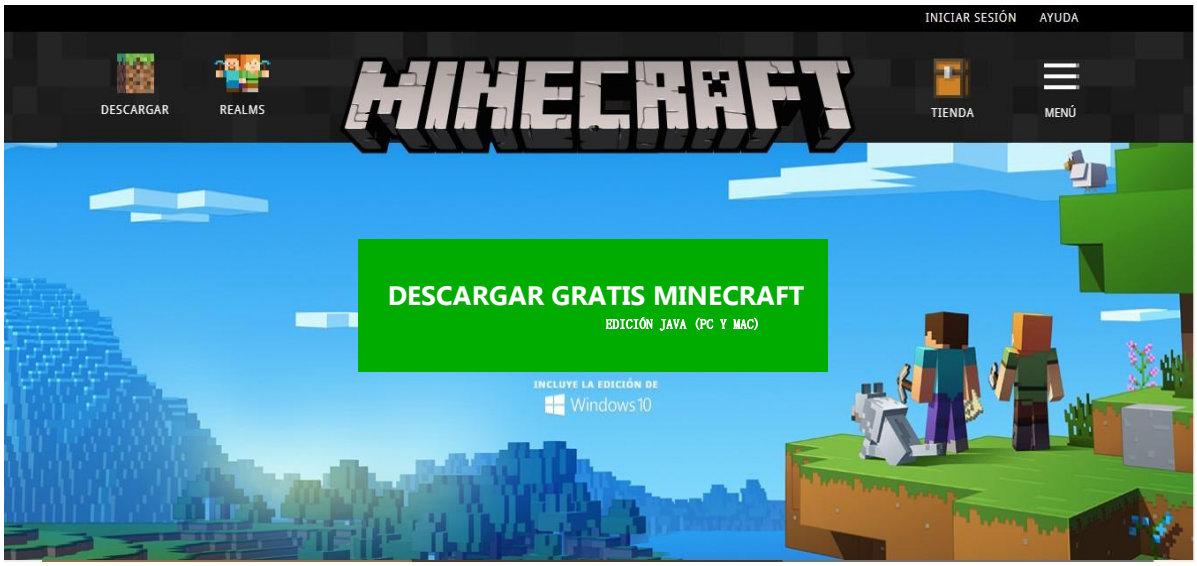


Ilustración 8 Banner Phishing

En cuanto al diseño del correo electrónico, se creó la cuenta con nombre de *microsoftregala@gmail.com,* teniendo en cuenta que Microsoft es el que vende

este juego, por lo cual cuando llegue al remitente (víctima) será más creíble y generará mayor confianza; el banner del juego *minecraft* que se incluyó en el mensaje es el siguiente:

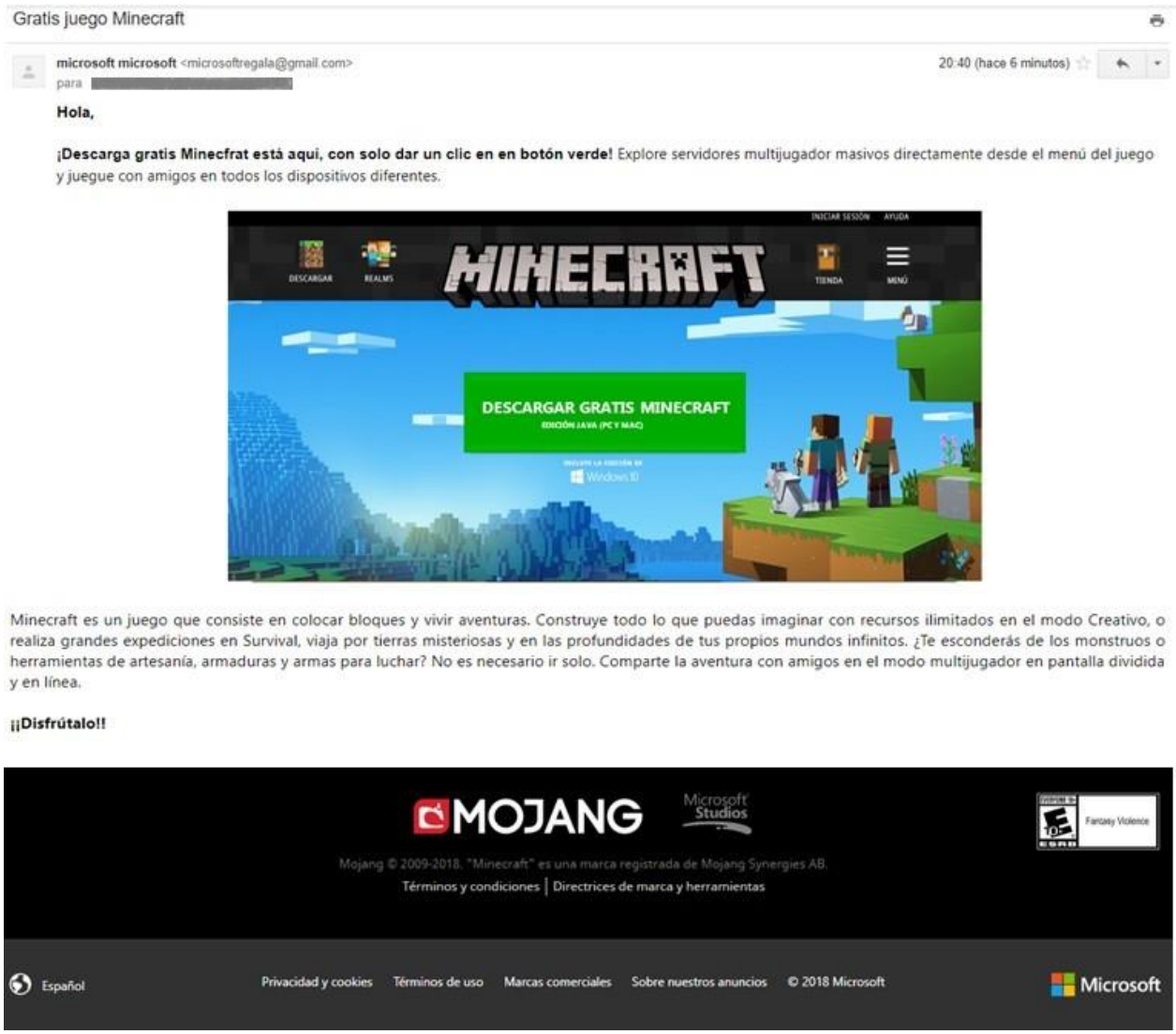


Ilustración 9 Mensaje email

Una vez finalizado el diseño de la campaña se llevará a cabo la correspondiente *ejecución* del caso práctico (simulación) del ataque informático de la técnica seleccionada de Ingeniería Social.

Para llevar a cabo la técnica de Ingeniería Social *phishing,* se utilizará el banner del juego *minecraft*, realizando algunas modificaciones en el botón verde “comprar minecraft” y en el login, para que las víctimas caigan en la trampa.

Como se puede evidenciar este es el sitio oficial del juego *minecraft,* con url: *https://minecraft.net/es-es/*

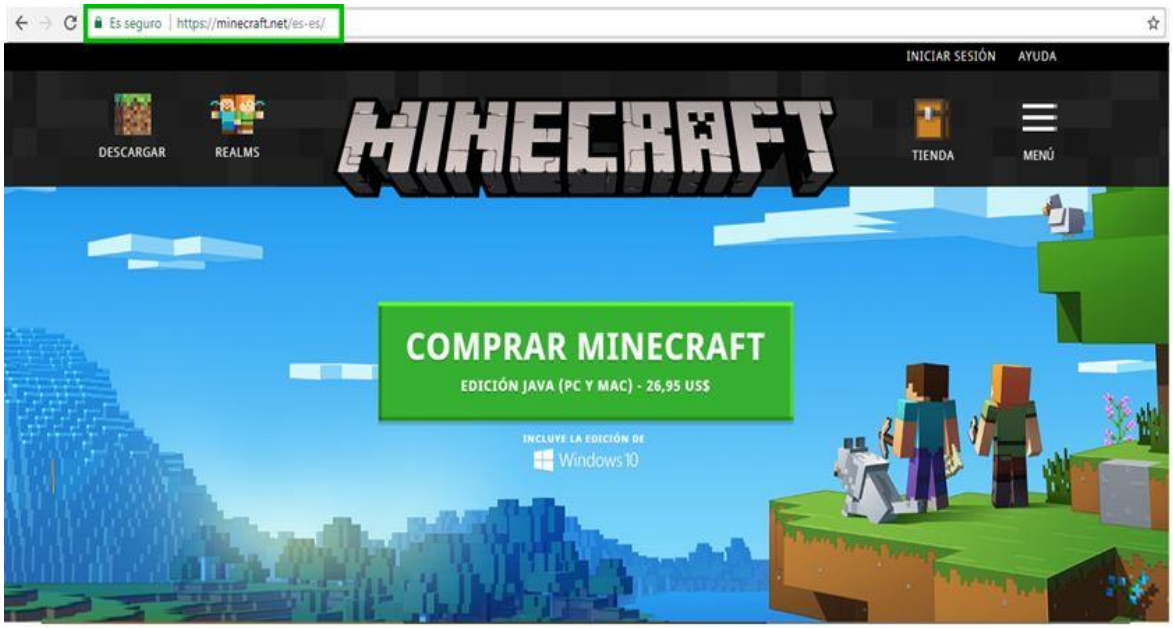


Ilustración 10 Sitio oficial Minecraft

La url correspondiente a la página del login del juego es *https://minecraft.net/es-es/login/?ref=gm*

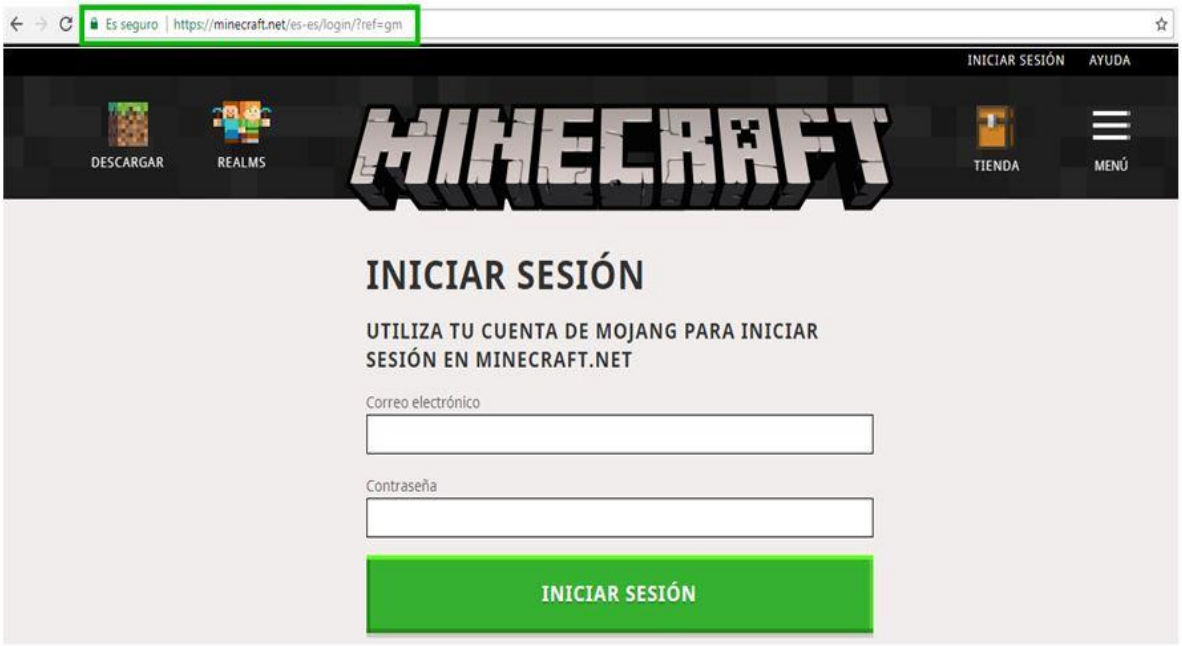


Ilustración 11 Página login juego

A continuación, se ilustrará el banner que será utilizado para que la víctima de clic en el banner, una vez realizado este proceso la víctima será redireccionado(a) supuestamente al "sitio oficial" del juego el cual es una página phishing con url: *http://minecraftgratisphishing.com/*, una vez ubicado allí la víctima dará clic en el recuadro *"DESCARGAR GRATIS MINECRAFT"*

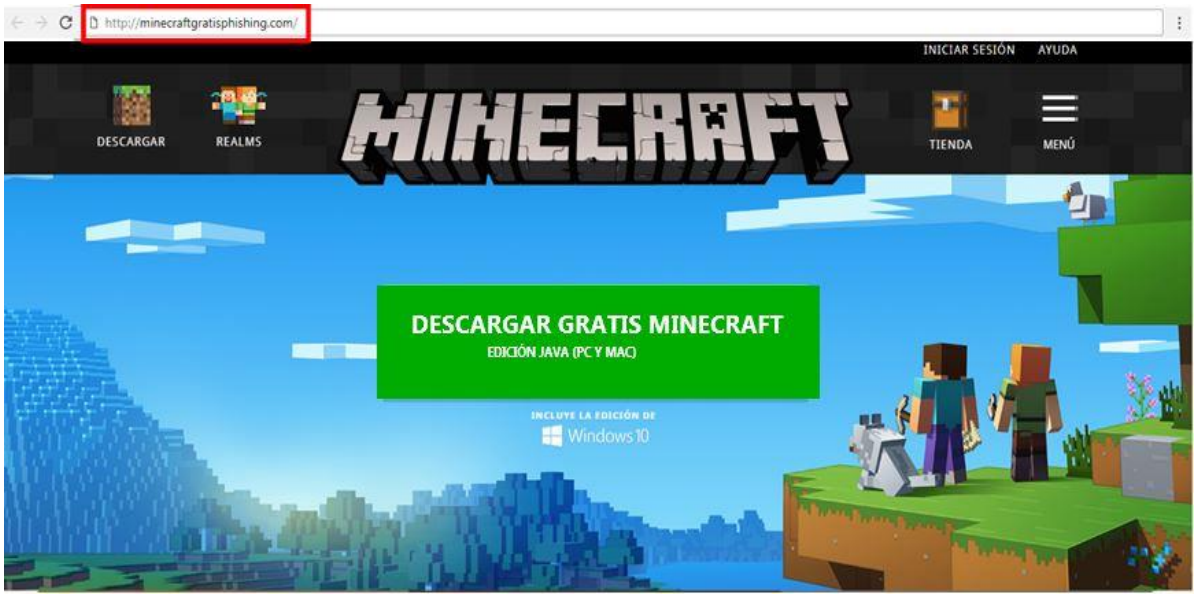


Ilustración 12 Descargar gratis Minecraft

Posteriormente la víctima será redireccionado(a) a la pá*gina con* url: *http://minecraftgratisphishing.com/login*, con el fin de que ingrese la información correspondiente al correo electrónico y la contraseña del mismo.
Para este caso se debe diseñar un formulario en la web para la recolección de información.

Ilustración 13 Iniciar sesión

Una vez diligenciada la información solicitada el atacante habrá obtenido las credenciales de la víctima.

Así mismo le será descargado a la víctima un archivo.exe (troyano) donde se aloja el juego el cual una vez sea ejecutado, el atacante tendrá el control de la

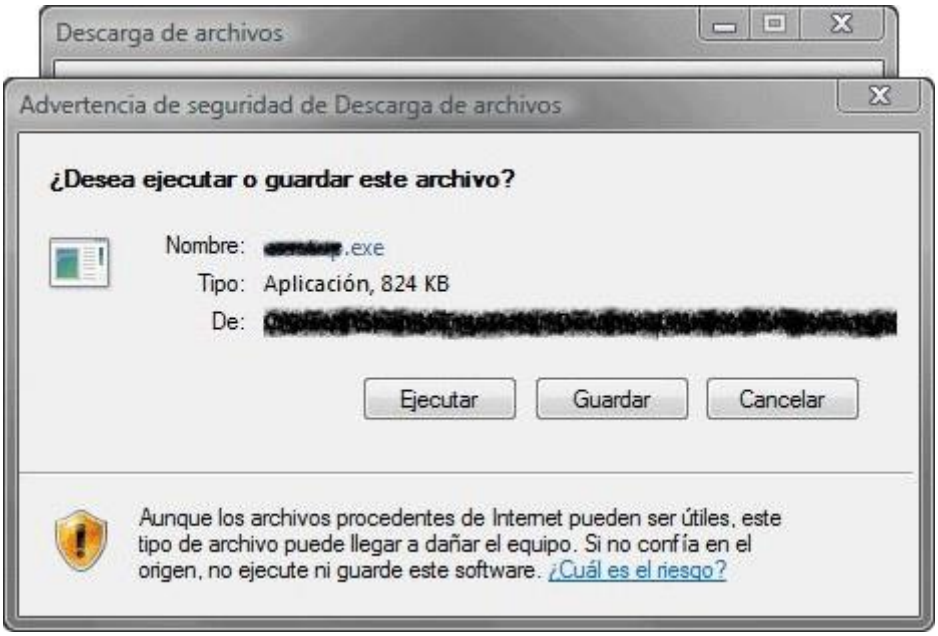


Ilustración 14 Ejecutar archivo

máquina (smartphone, computador o ipad) de la víctima, realizando acciones como son tomar fotos a la víctima (niños, niñas y adolescentes), captura de información relevante (cuentas de redes sociales, contraseñas, correos electrónicos, cuentas bancarias, etc), como se puede evidenciar a continuación:

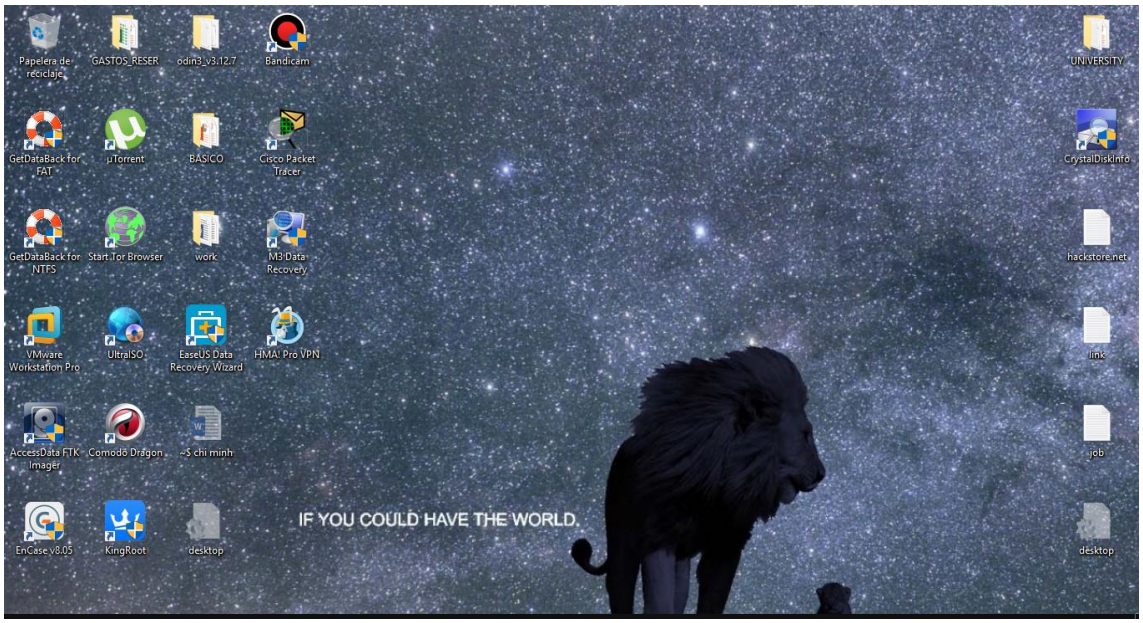


Ilustración 15 Evidencia 1

Ilustración 16 Evidencia 2

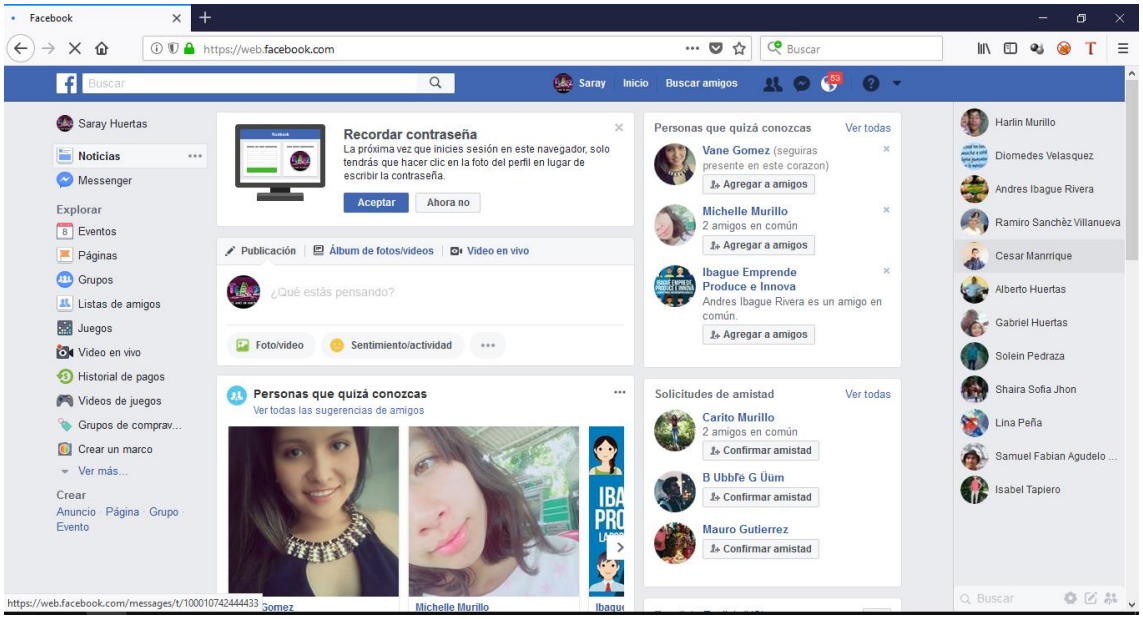


Ilustración 17 Evidencia 3

Ilustración 18 Evidencia 4

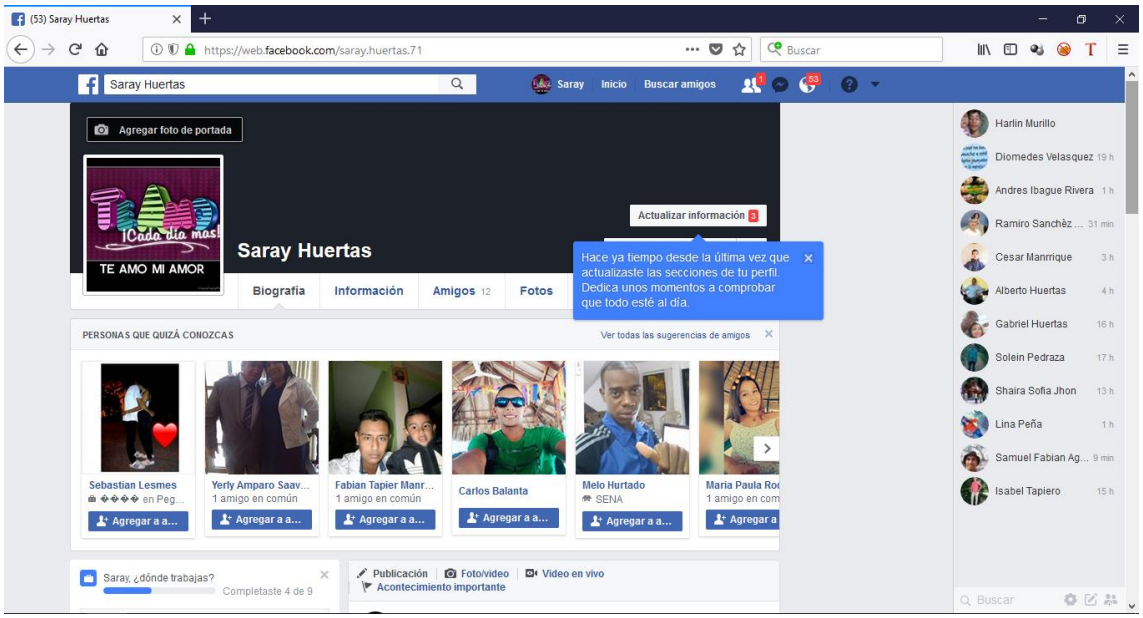


Ilustración 19 Evidencia 5

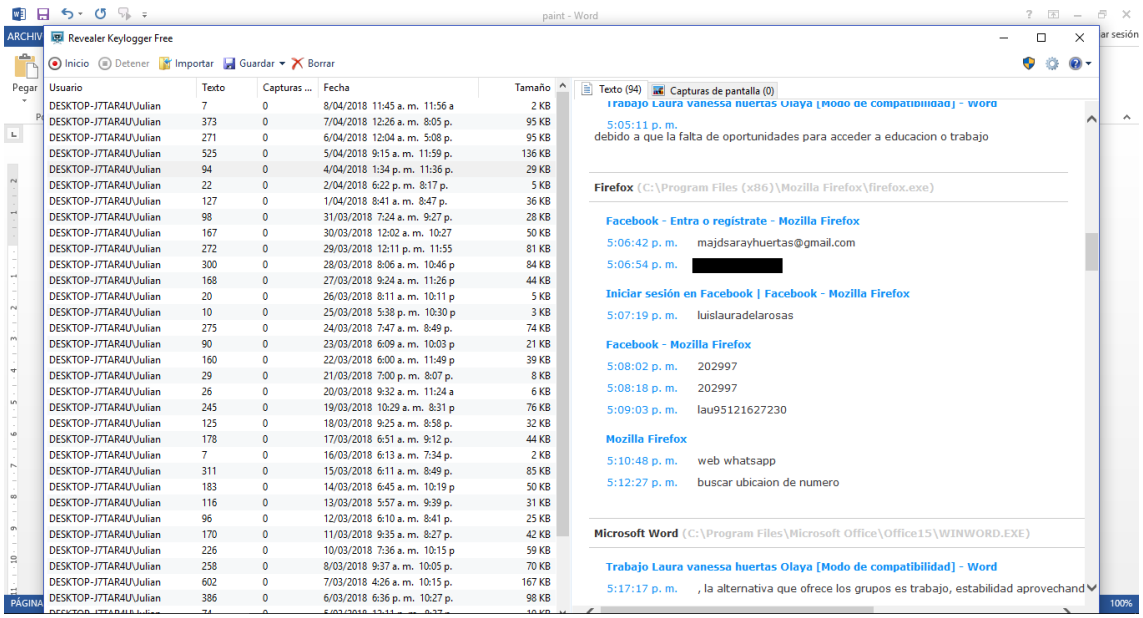


Ilustración 20 Evidencia 6

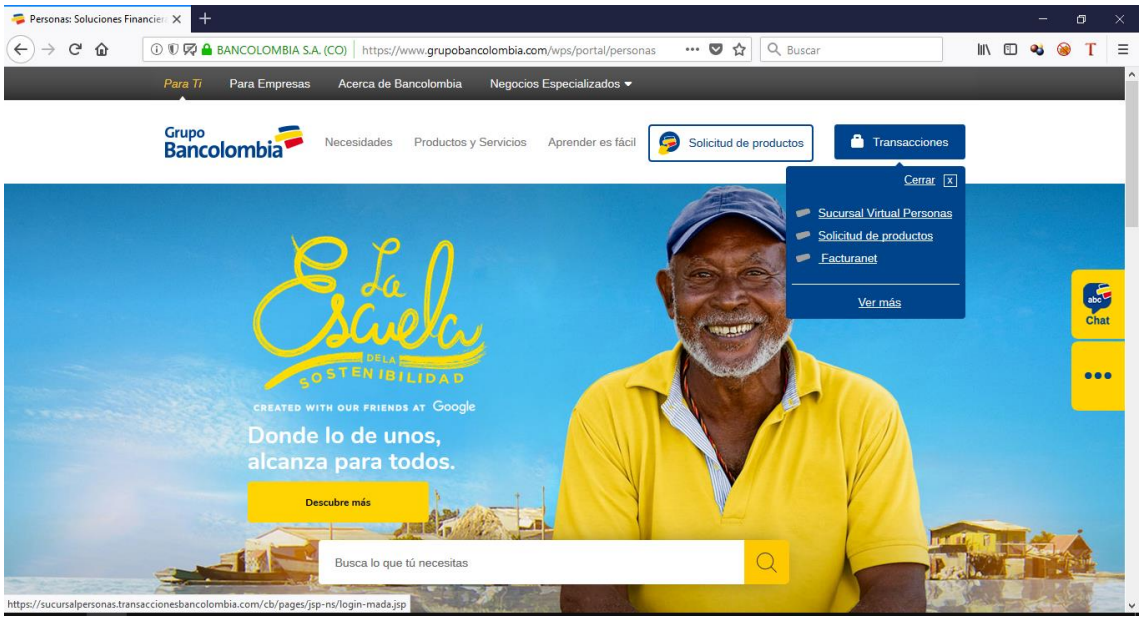


Ilustración 21 Evidencia 7

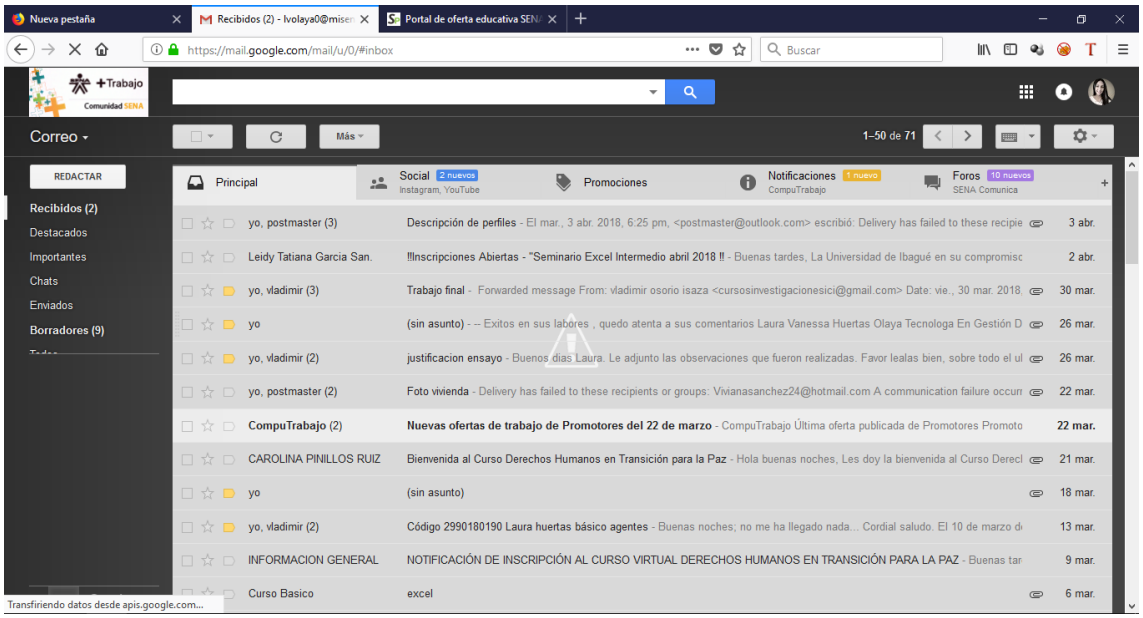


Ilustración 22 Evidencia 8

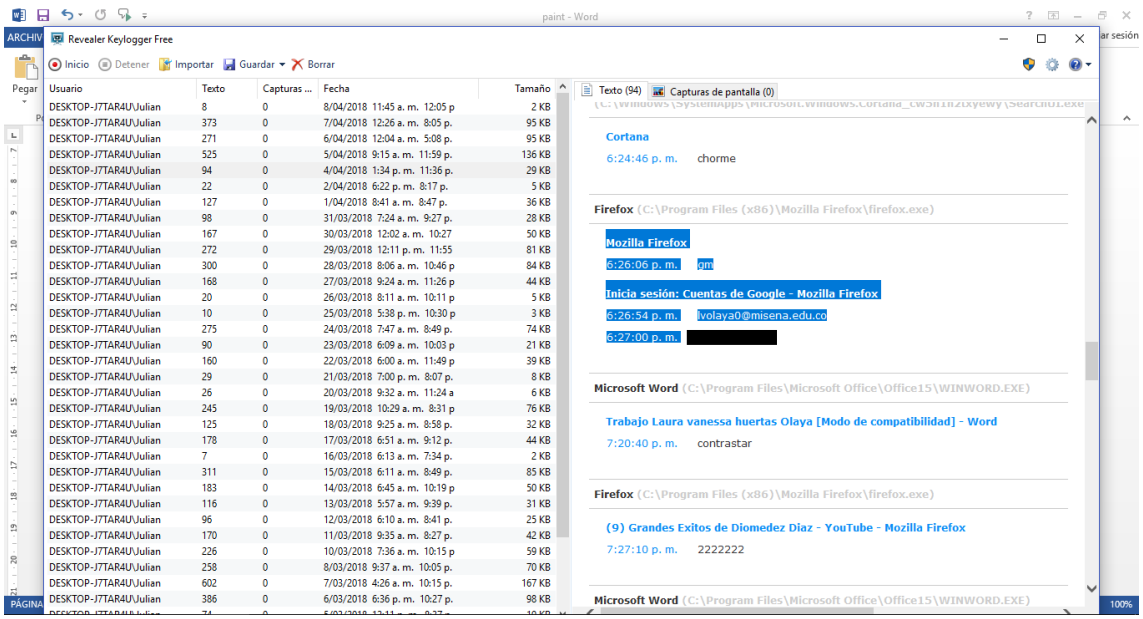


Ilustración 23 Evidencia 9

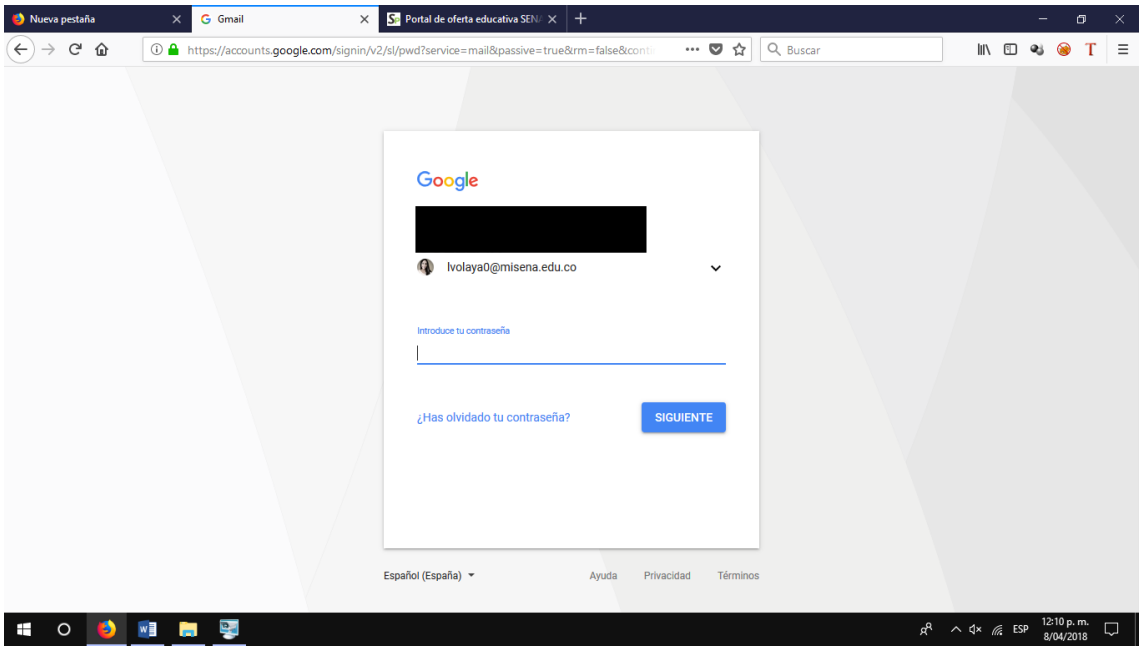


Ilustración 24 Evidencia 10

Lo preocupante del caso es que la mayoría de las veces no se tiene conocimiento en manos de quien cae la información nombrada anteriormente, la cual es valiosa y confidencial para las víctimas; si se da el caso que el atacante tenga propósitos oscuros puede llegar a difundir, comercializar y vender dicha información entre ello fotografías, usándolas como medio de extorsión a niños, niñas adolescentes y adultos, es acá donde se lleva a cabo la técnica de Ingeniería Social *sextortion*, estos riesgos se pueden evitar siendo conscientes de la realidad actual del manejo inadecuado que dan muchas personas a sus redes sociales y correo electrónico, es por ello que se debe tomar acciones correctivas y preventivas para evitar desenlaces irreversibles.

8.1.1 Recomendaciones del caso práctico

Como se pudo evidenciar en el diseño de campaña, es necesario realizar un diseño acorde con lo que esté de moda en el momento o lo que está presentando auge, de acuerdo a la víctima o grupo de víctimas a las cuales vaya dirigido, puede ser entre rango de edades, personalidad, géneros, cursos o grados de los colegios, religión, política, nacionalidad, gustos y demás, de igual forma la campaña debe demostrar credibilidad y confianza para que la víctima caiga en ella.

Una vez llegue al correo electrónico de la víctima el banner de descarga gratis del juego *minecraft,* es muy alta la posibilidad que la persona *(en este caso niños o niñas será entre la edad de 10 y 11 años pertenecientes a los grados 5° de primaria y 6° de bachillerato, así mismo los adolescentes estarán entre el rango de edad 12 a los 16 años de edad, correspondientes entre a los grados de 7° a 11° de bachillerato)* ingrese la información solicitada correspondiente al

correo electrónico y contraseña para iniciar sesión y descarga automática del juego (troyano), una vez realizado este proceso por parte de la víctima, el atacante ya tiene el control completo del equipo, visualizando y accediendo a información sensible y confidencial de la víctima y de otras personas que hagan uso del equipo, sin que estas se percaten de lo sucedido.
Este caso práctico (simulación) presentado en uno de las tantas metodologías de phishing, realizadas por los atacantes con el fin de obtener beneficio *económico, en busca de vulnerabilidades, por diversión o simplemente por causar algún tipo de daño.*

Para evitar ser víctima de este tipo de Ingeniería Social, es necesario tener en cuenta las siguientes recomendaciones:

- No abrir correos electrónicos de remitentes desconocidos.
- No abrir correos electrónicos cuando no han sido solicitados.
- No abrir archivos adjuntos sospechosos.
- Mantener actualizado el sistema operativo del equipo.
- Mantener actualizado el antivirus.
- Utilizar activamente los filtros antispam.
- Verificar que la URL del sitio visitado sea el auténtico.
- No dar clic a enlaces de páginas web que lleguen a través de vía e-mail en el soliciten datos personales.
- No envíe información sensible a través de internet antes de verificar la seguridad del sitio web.
- Verificar que el sitio web cuente con certificado SSL.
- Estar actualizado en temas de Ingeniería Social, con el fin de tener conocimiento de cómo actuar al momento que se presente algún tipo de ataque.

De igual forma si está siendo víctima de Ingeniería Social, es importante tener en cuenta lo siguiente:

- *En persona:* Si nos sentimos inseguros o amenazados, lo que debemos hacer es romper el contacto y notificarlo a las autoridades.

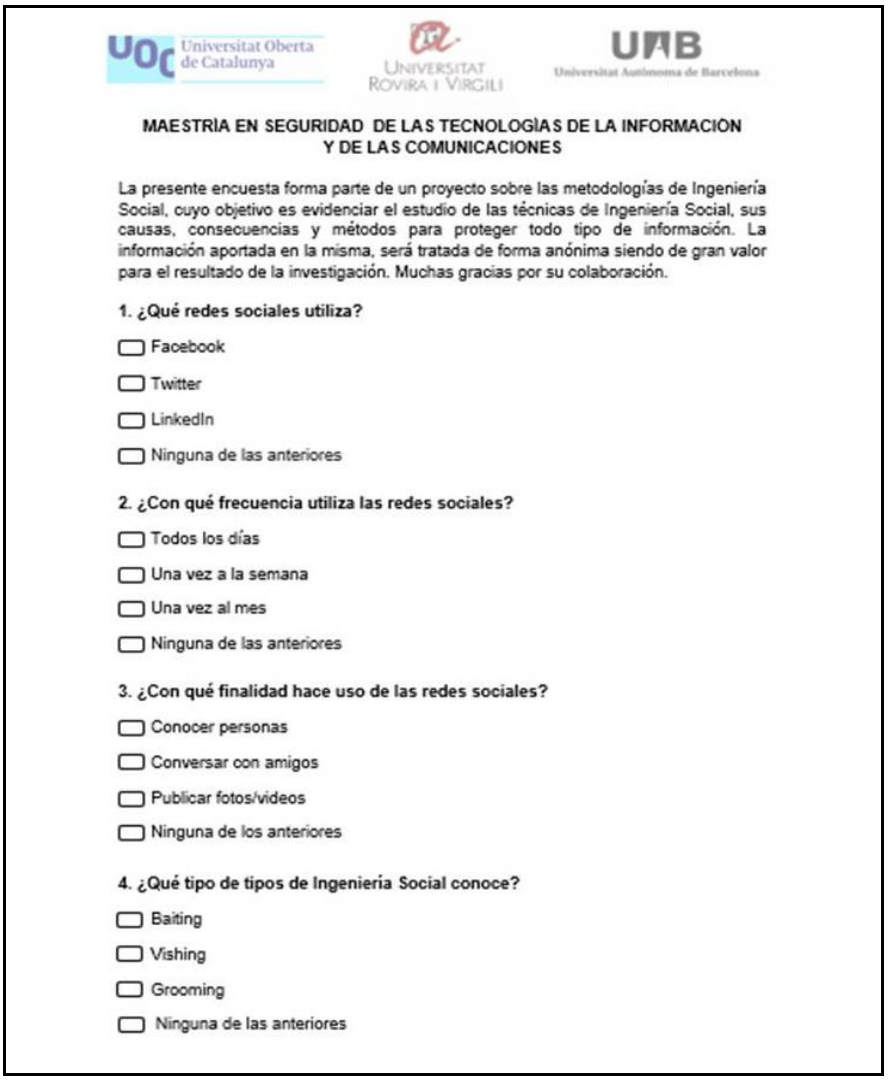
- *Por escrito o en las redes sociales:* Tenemos que ignorarlo y borrarlo. Si el ataque se produce utilizando el nombre de alguien que conocemos, debemos contactar con él y averiguar si la petición es legítima.

- *Por teléfono:* Se debe colgar inmediatamente. Si el llamante es persistente, es necesario pedirle un número directo al que se le pueda llamar.

- *Por correo electrónico:* Contactemos al el remitente mediante otro medio, normalmente mediante una llamada de teléfono para confirmar si su correo es legítimo.

8.2 Resultados de la encuesta

Formato



MAESTRÍA EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

La presente encuesta forma parte de un proyecto sobre las metodologías de Ingeniería Social, cuyo objetivo es evidenciar el estudio de las técnicas de Ingeniería Social, sus causas, consecuencias y métodos para proteger todo tipo de información. La información aportada en la misma, será tratada de forma anónima siendo de gran valor para el resultado de la investigación. Muchas gracias por su colaboración.

1. ¿Qué redes sociales utiliza?

- ☐ Facebook
- ☐ Twitter
- ☐ LinkedIn
- ☐ Ninguna de las anteriores

2. ¿Con qué frecuencia utiliza las redes sociales?

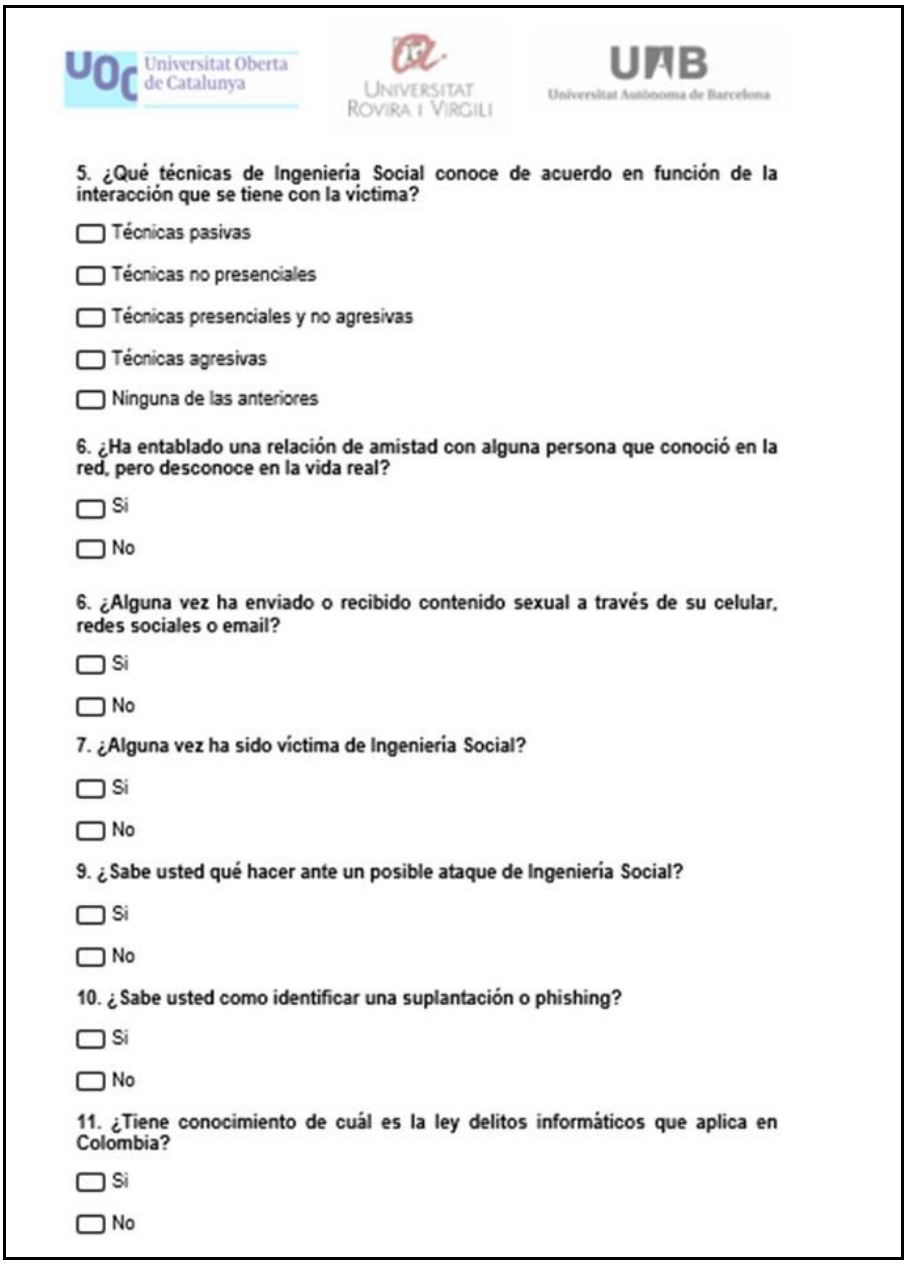
- ☐ Todos los días
- ☐ Una vez a la semana
- ☐ Una vez al mes
- ☐ Ninguna de las anteriores

3. ¿Con qué finalidad hace uso de las redes sociales?

- ☐ Conocer personas
- ☐ Conversar con amigos
- ☐ Publicar fotos/videos
- ☐ Ninguna de los anteriores

4. ¿Qué tipo de tipos de Ingeniería Social conoce?

- ☐ Baiting
- ☐ Vishing
- ☐ Grooming
- ☐ Ninguna de las anteriores



5. ¿Qué técnicas de Ingeniería Social conoce de acuerdo en función de la interacción que se tiene con la víctima?

- ☐ Técnicas pasivas
- ☐ Técnicas no presenciales
- ☐ Técnicas presenciales y no agresivas
- ☐ Técnicas agresivas
- ☐ Ninguna de las anteriores

6. ¿Ha entablado una relación de amistad con alguna persona que conoció en la red, pero desconoce en la vida real?

- ☐ Si
- ☐ No

6. ¿Alguna vez ha enviado o recibido contenido sexual a través de su celular, redes sociales o email?

- ☐ Si
- ☐ No

7. ¿Alguna vez ha sido víctima de Ingeniería Social?

- ☐ Si
- ☐ No

9. ¿Sabe usted qué hacer ante un posible ataque de Ingeniería Social?

- ☐ Si
- ☐ No

10. ¿Sabe usted como identificar una suplantación o phishing?

- ☐ Si
- ☐ No

11. ¿Tiene conocimiento de cuál es la ley delitos informáticos que aplica en Colombia?

- ☐ Si
- ☐ No

Ilustración 25 Formato encuesta

Teniendo en cuenta la estructura que se evidencia anteriormente de la encuesta cuyo objetivo es *evidenciar el estudio de las técnicas de Ingeniería Social, sus causas, consecuencias y métodos para proteger todo tipo de información,* fue realizada a 30 personas, incluyendo adolescentes de la Universidad Autónoma del pregrado de Ingeniería Industrial y adultos pertenecientes a una entidad estatal de la ciudad de Bogotá D.C.

La encuesta consta de 11 preguntas correspondiente al tema de Ingeniería Social.

Cabe aclarar que para obtener un análisis real y verídico fue necesario incluir casillas en algunas de las preguntas, para evidenciar el resultado obtenido del

total de las personas encuestadas, esto teniendo en cuenta que algunas personas marcaron más de una respuesta.

Los resultados fueron los siguientes:

- **De acuerdo a la pregunta No. 1 *¿Qué redes sociales utiliza?*, las respuestas fueron las siguientes:**

¿Qué redes sociales utiliza?	Respuestas
Facebook	19
Facebook y twitter	2
Twitter	2
Facebook, twitter y linkedln	2
Ninguna de las anteriores	5
TOTAL	**30**

Se logra evidenciar que, mientras 19 personas hacen uso exclusivo de la red social *Facebook,* 2 personas usan las dos redes sociales f*acebook y twitter,* 2 personas utilizan exclusivamente la red social *twitter,* mientras que 2 personas utilizan las tres redes sociales *facebook, twitter y linkedln,* y para finalizar 5 personas no utiliza ninguna de las redes sociales mencionadas.

Ilustración 26 Gráfico de barras pregunta No.1

Ilustración 27 Gráfico circular pregunta No.1

De acuerdo a la ilustración 2, se puede concluir que el 63% de las personas encuestadas utiliza exclusivamente la red social *facebook*, el 17% de las personas no utiliza ninguna red social, el 7% hace uso exclusivo de la red social *twitter*, así mismo otro 7% de las personas encuestadas utilizan las redes sociales *facebook, twitter y linkedln*, por último, el 6% utiliza las redes sociales *facebook* y *twitter*.

- **De acuerdo a la pregunta No. 2 *¿Con qué frecuencia utiliza las redes sociales?,* las respuestas fueron las siguientes:**

¿Con qué frecuencia utiliza las redes sociales?	Respuestas
Todos los días	20
Una vez a la semana	5
Una vez al mes	0
Ninguna de las anteriores	5
TOTAL	**30**

En cuanto a la frecuencia con la que utiliza las redes sociales se puede evidenciar que 20 personas de las encuestadas las utilizan *todos los días,* 5 personas *una vez a la semana,* 5 personas *no utilizan ninguna* de las respuestas mencionadas y 0 personas *una vez al mes*.

Ilustración 28 Gráfico de barras pregunta No.2

Ilustración 29 Gráfico circular pregunta No.2

Teniendo en cuenta la ilustración 4, se puede evidenciar que el 67%, de las personas encuestadas utilizan las redes sociales *todos los días*, mientras que el 17% *no utiliza ninguna* de las opciones nombradas, por otro lado, un 16% utiliza la frecuencia *una vez a la semana* y finalmente un 0% *una vez al mes*.

- **De acuerdo a la pregunta No. 3 *¿Con qué finalidad hace uso de las redes sociales?,* las respuestas fueron las siguientes:**

¿Con qué finalidad hace uso de las redes sociales?	Respuestas
Conocer personas	4
Conservar con amigos	3
Conocer personas y conservar con amigos	3
Conversar con amigos y publicar fotos/videos	2
Publicar fotos/videos	3
Ninguna de las anteriores	15
TOTAL	**30**

Teniendo en cuenta los resultados arrojados de la pregunta No. 3, se puede deducir que, 4 personas lo hacen por *conocer personas*, 3 para *conservar con amigos*, 3 para *conocer personas y conservar con amigos*, 2 personas para *conversar con amigos y publicar fotos/videos*, 3 *publicar fotos/videos* y finalmente 15 personas *no hacen ningún uso* de acuerdo a las opciones brindadas.

Ilustración 30 Gráfico de barras pregunta No.3

Ilustración 31 Gráfico circular pregunta No.3

Teniendo en cuenta la ilustración 6, se puede evidenciar que el 50% de las personas encuestadas *no utilizan ninguna* de las opciones brindadas referente a la finalidad de uso que les dan a las redes sociales, el 13% hacen uso de ellas para *conocer personas*, el 10% para *conversar con amigos*, otro 10% *para conocer personas y conversar con amigos*, así mismo un 10% para *publicar fotos/videos* y finalmente un 7% para *conversar con amigos y publicar fotos/videos.*

- **De acuerdo a la pregunta No. 4 *¿Qué tipo de tipos de Ingeniería Social conoce?,* las respuestas fueron las siguientes:**

¿Qué tipo de tipos de Ingeniería Social conoce?	Respuestas
Baiting	2
Vishing	1
Grooming	3
Baiting, vishing y grooming	4
Ninguna de las anteriores	20
TOTAL	**30**

Teniendo en cuenta las respuestas de la pregunta No. 4, se pueden evidenciar que: 2 de las personas encuestadas conoce el tipo de Ingeniería Social *baiting*, 1 persona conoce el *vishing*, 3 conocen *grooming*, por otro lado 4 conocen *baiting, vishing* y *grooming*, finalmente 20 personas no conocen ningún tipo.

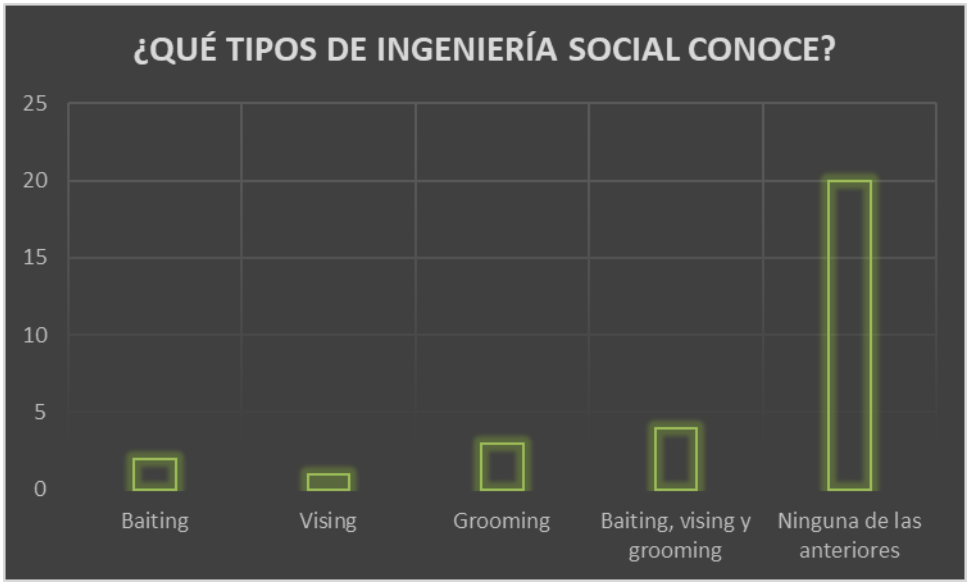


Ilustración 32 Gráfico de barras pregunta No.4

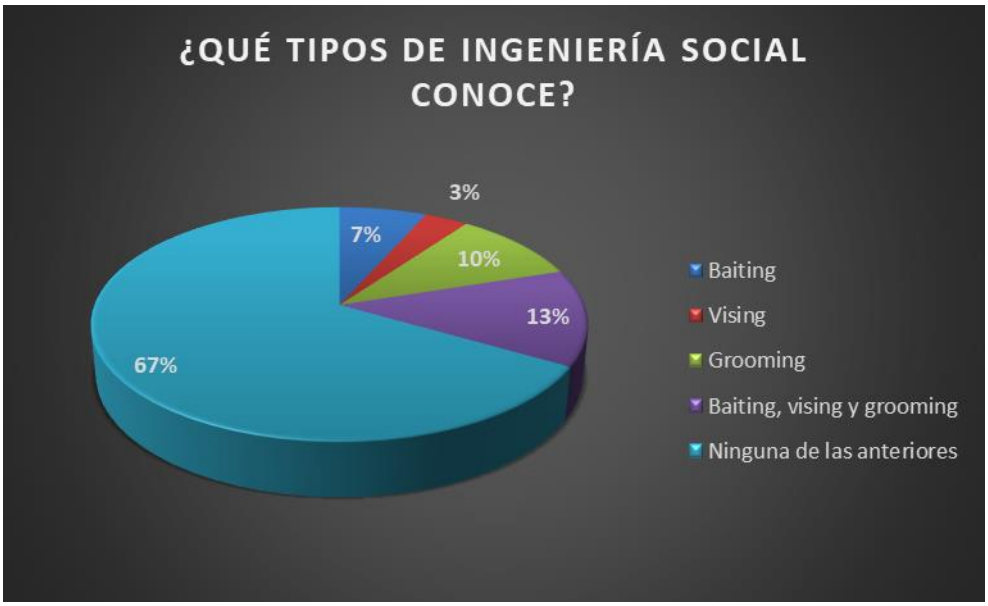


Ilustración 33 Gráfico circular pregunta No.4

Teniendo como referencia la ilustración 8, se puede observar que el 67% de las personas encuestadas no conoce ninguno de los tipos de Ingeniería Social nombrados en la encuesta, más sin embargo un 13% de las personas conoce los tipos de Ingeniería Social *baiting, vishing* y *grooming*, un 10% conoce exclusivamente *grooming*, por otro lado, el 7% conoce exclusivamente *baiting* y un 3% conoce el *vishing.*

- **De acuerdo a la pregunta No. 5 *¿Qué técnicas de Ingeniería Social conoce de acuerdo en función de la interacción que se tiene con la víctima?,* las respuestas fueron las siguiente:**

¿Qué técnicas de Ingeniería Social conoce de acuerdo en función de la interacción que se tiene con la víctima?	Respuestas
Técnicas pasivas	2
Técnicas no presenciales	2
Técnicas presenciales y no agresivas	1
Técnicas agresivas	1
Técnicas pasivas, técnicas no presenciales, técnicas presenciales y no agresivas, técnicas agresivas	1
Técnicas pasivas, técnicas no presenciales, técnicas presenciales y no agresivas	1
Técnicas pasivas, técnicas no presenciales, técnicas agresivas.	1
No responde	1
Ningunas de las anteriores	20
TOTAL	**30**

Respecto a la pregunta No. 5 los resultados obtenidos son los siguientes:

2 personas de las encuestadas conocen las técnicas pasivas, 2 conocen las *técnicas no presenciales*, 1 persona conoce las *técnicas presenciales y no agresivas*, 1 conoce las *técnicas agresivas*, 1 persona conoce las *técnicas pasivas, no presenciales, presenciales, agresivas y no agresivas*, por otro lado 1 persona conoce las *técnicas pasivas, no presenciales, presenciales y no agresivas*; 1 persona conoce las *técnicas pasivas, técnicas no presenciales, técnicas agresivas*, más sin embargo 1 persona *no responde* esta pregunta y 20 personas *no conocen ninguna* de las técnicas mencionadas.

Ilustración 34 Gráfico de barras pregunta No.5

Ilustración 35 Gráfico circular pregunta No.5

En referencia la ilustración 10, se puede evidenciar que el 67% de las personas encuestadas *no conoce ninguna* de las técnicas de Ingeniería Social de acuerdo en función con la interacción que se tiene con la víctima, evidenciadas en la encuesta, el 7% conoce las *técnicas pasivas*, otro 7% conoce sobre las *técnicas no presenciales*, el 4% dice conocer las *técnicas presenciales y no agresivas*, un 3% conoce las *técnicas agresivas*, otro 3% conoce las *técnicas pasivas, no presenciales, presenciales, no agresivas y agresivas*, también un 3% conoce las *técnicas pasivas, no presenciales, presenciales y no agresivas*, el 3% conoce las *técnicas pasivas, no presenciales y agresivas*, finalizando un 3% *no responde* a esta pregunta.

- **De acuerdo a la pregunta No. 6 *¿Ha entablado una relación de amistad con alguna persona que conoció en la red, pero desconoce en la vida real?,* las respuestas fueron las siguientes:**

¿Ha entablado una relación de amistad con alguna persona que conoció en la red, pero desconoce en la vida real?	Respuestas
Si	9
No	21
TOTAL	**30**

Teniendo en cuenta la pregunta No. 6, se pueden evidenciar que 9 de las personas encuestadas respondieron *si*, mientras que 21 respondieron *no*, a la pregunta: ha entablado una relación de amistad con alguna persona que conoció en la red, pero desconoce en la vida real.

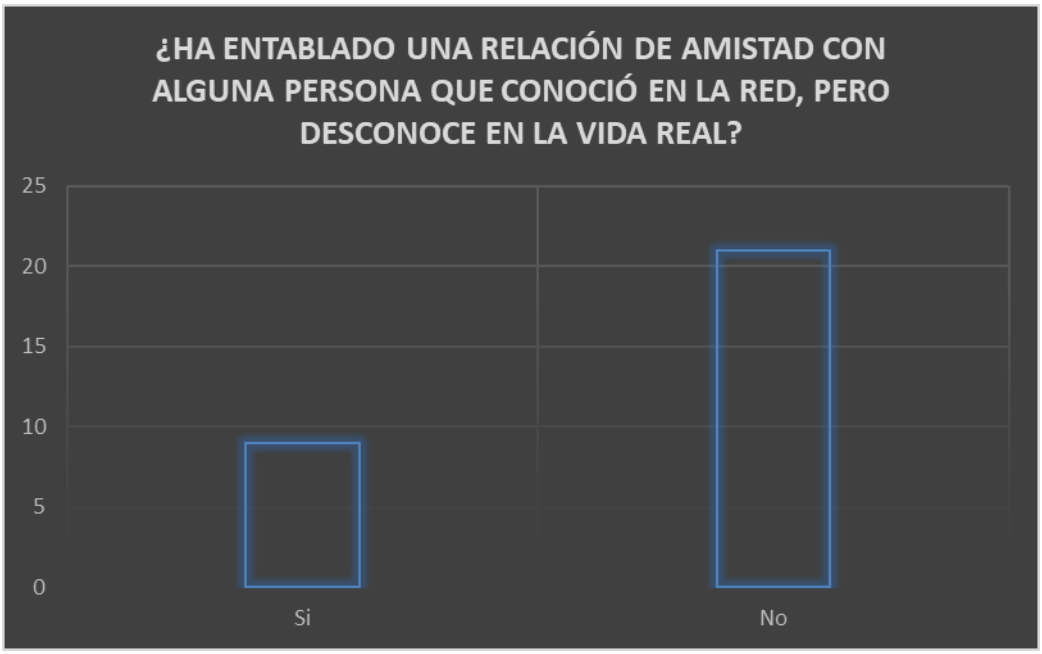


Ilustración 36 Gráfico de barras pregunta No.6

Ilustración 37 Gráfico circular pregunta No.6

En referencia a la ilustración 12, se observa que el 70% de las personas encuestadas respondieron que *no*, mientras que el 30% respondió *sí*, a la pregunta: ha entablado una relación de amistad con alguna persona que conoció en la red, pero desconoce en la vida real

- **De acuerdo a la pregunta No. 7 *¿Alguna vez ha enviado o recibido contenido sexual a través de su celular, redes sociales o email?,* las respuestas fueron las siguientes:**

¿Alguna vez ha enviado o recibido contenido sexual a través de su celular, redes sociales o email?	Respuestas
Si	13
No	17
TOTAL	**30**

Se puede evidenciar que de acuerdo a la pregunta No. 7, 13 de las personas encuestadas respondieron *si*, mientras que 17 personas respondieron *no,* a la pregunta: alguna vez ha enviado o recibido contenido sexual a través de su celular, redes sociales o email.

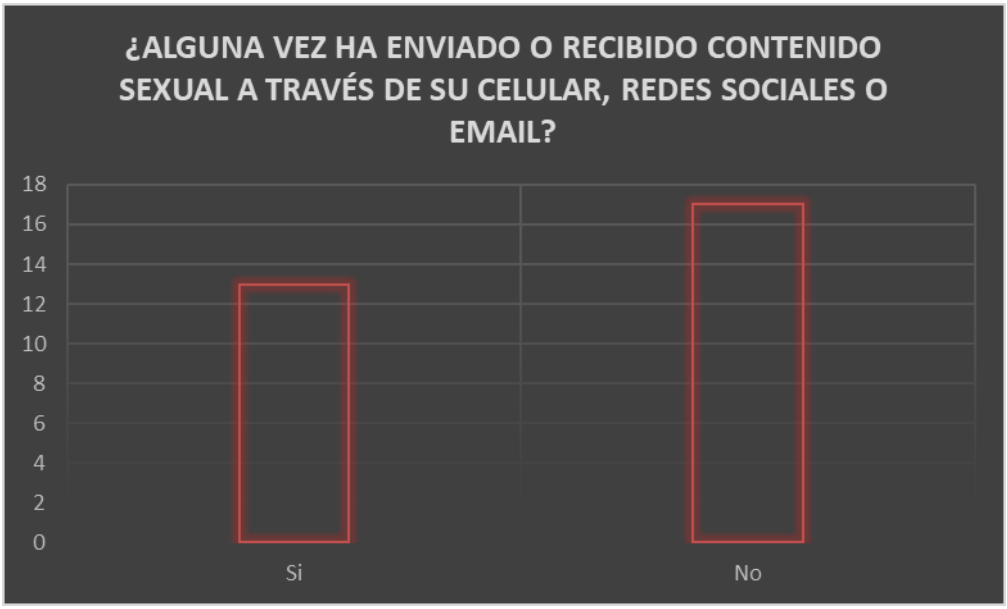


Ilustración 38 Gráfico de barras pregunta No.7

Ilustración 39 Gráfico circular pregunta No.7

En la ilustración 14 se puede evidenciar que el 57% de las personas encuestadas respondió *no*, mientras que el 43% respondió *si,* a la pregunta: alguna vez ha enviado o recibido contenido sexual a través de su celular, redes sociales o email.

- **De acuerdo a la pregunta No. 8 *¿Alguna vez ha sido víctima de Ingeniería Social?*, las respuestas fueron las siguientes:**

¿Alguna vez ha sido víctima de Ingeniería Social?	Respuestas
Si	3
No	27
TOTAL	**30**

Respecto a la pregunta No. 8, los resultados son los siguientes: 3 personas respondieron que *sí*, mientras que 27 respondieron que *no.*

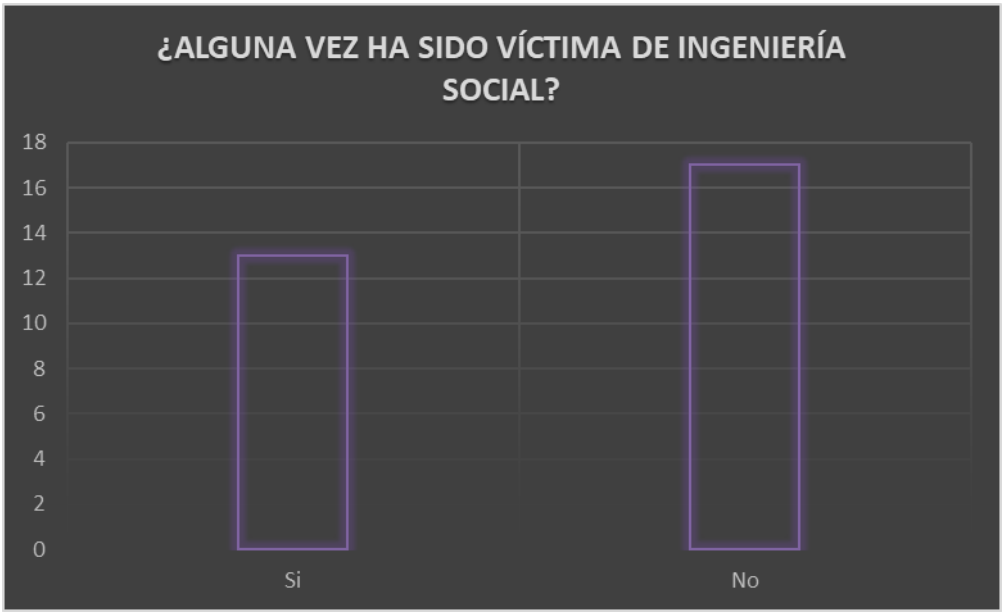


Ilustración 40 Gráfico de barras pregunta No.8

Ilustración 41 Gráfico circular pregunta No.8

En la ilustración 16 se puede evidenciar que el 90% de las personas encuestadas respondió *no*, mientras que el 10% respondió *si,* a la pregunta: alguna vez ha sido víctima de Ingeniería Social.

- **De acuerdo a la pregunta No. 9 *¿Sabe usted qué hacer ante un posible ataque de Ingeniería Social?,* las respuestas fueron las siguientes:**

¿Sabe usted qué hacer ante un posible ataque de Ingeniería Social?	Respuestas
Si	13
No	17
TOTAL	**30**

Teniendo en cuenta a la pregunta No. 9, se obtuvieron los siguientes resultados: 13 personas respondieron que *sí*, mientras que 17 respondieron que *no*, a la pregunta: Sabe usted qué hacer ante un posible ataque de Ingeniería Social.

Ilustración 42 Gráfico de barras pregunta No.9

Ilustración 43 Gráfico circular pregunta No.9

En la ilustración 18 se observa que el 57% de las personas encuestadas respondió *no*, mientras que el 43% respondió *si,* a la pregunta: sabe usted qué hacer ante un posible ataque de Ingeniería Social.

- **De acuerdo a la pregunta No. 10 *¿Sabe usted como identificar una suplantación o phishing?*, las respuestas fueron las siguientes:**

¿Sabe usted como identificar una suplantación o phishing?	Respuestas
Si	15
No	15
TOTAL	**30**

Teniendo en cuenta la pregunta No. 10, se pueden evidenciar que 15 de las personas encuestadas respondieron *si*, mientras que 15 respondieron *no*, a la pregunta: sabe usted como identificar una suplantación o phishing.

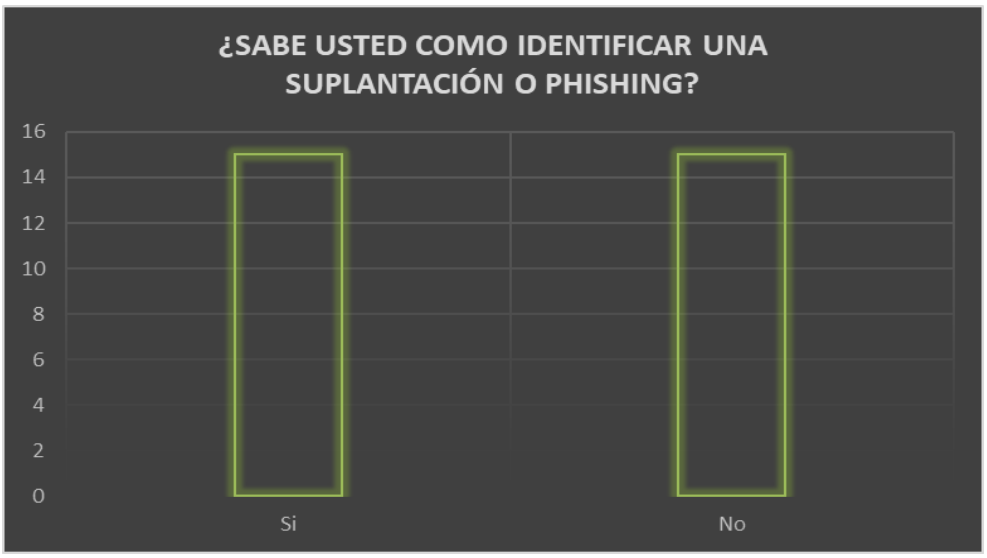


Ilustración 44 Gráfico de barras pregunta No.10

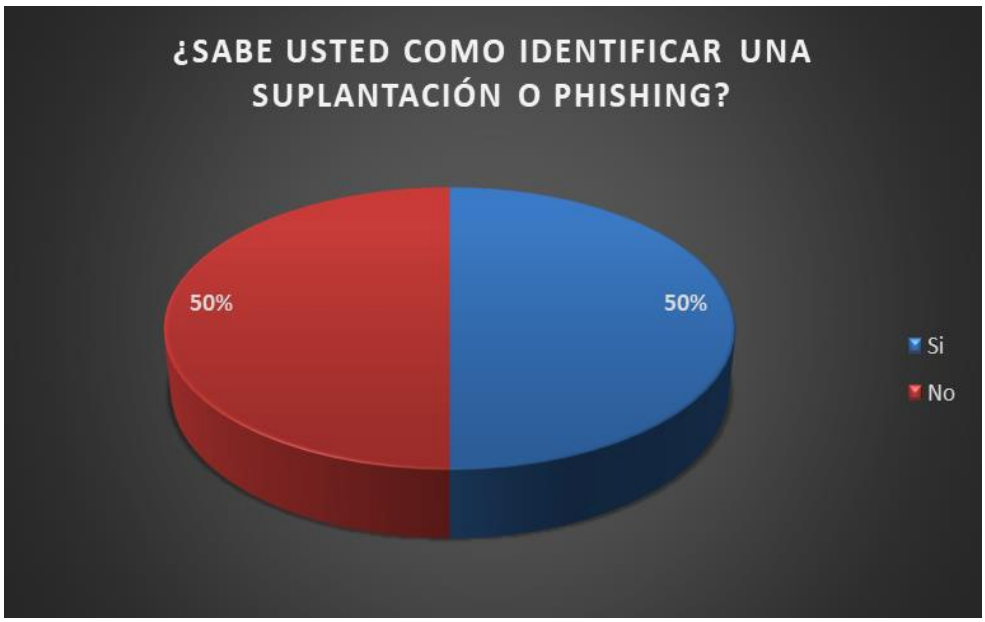


Ilustración 45 Gráfico circular pregunta No.10

En la ilustración 20 se observa que el 50% de las personas encuestadas respondió *si*, y por otro lado un 50% respondió *no,* a la pregunta: sabe usted como identificar una suplantación o phishing.

▪ **De acuerdo a la pregunta No. 11 *¿Tiene conocimiento de cuál es la ley delitos informáticos que aplica en Colombia?,* las respuestas fueron las siguientes:**

¿Tiene conocimiento de cuál es la ley delitos informáticos que aplica en Colombia?	Respuestas
Si	14
No	16
TOTAL	**30**

Teniendo en cuenta a la pregunta No. 11, se obtuvieron los siguientes resultados: 14 personas respondieron que *sí*, mientras que 16 respondieron que *no*, a la pregunta: tiene conocimiento de cuál es la ley delitos informáticos que aplica en Colombia

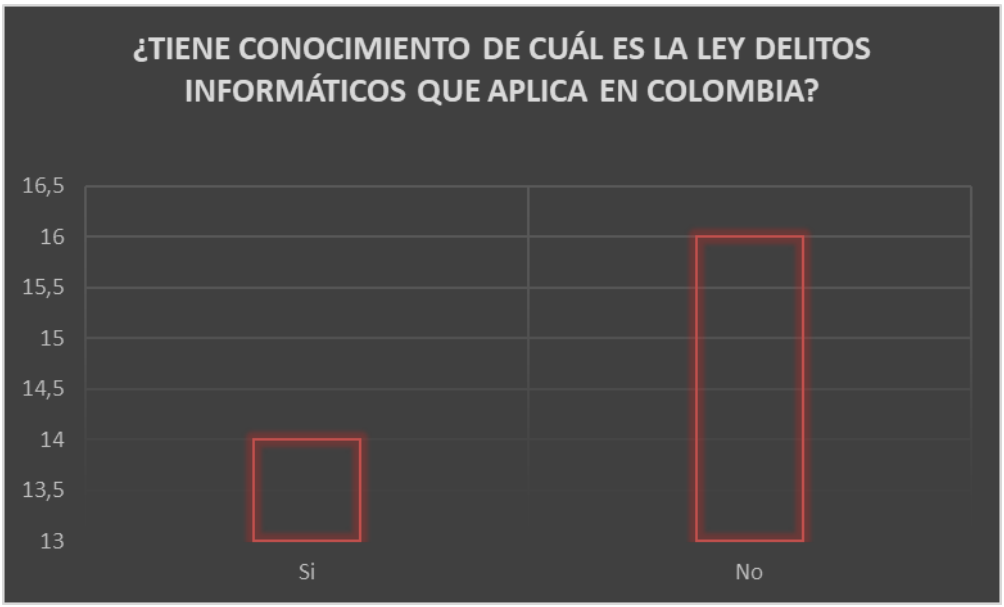


Ilustración 46 Gráfico de barras pregunta No.11

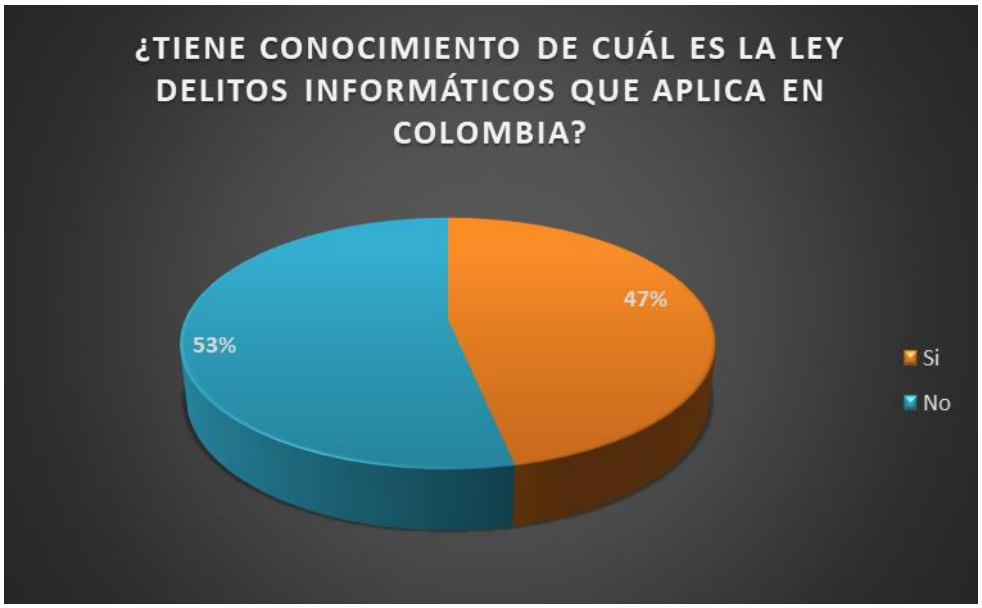


Ilustración 47 Gráfico circular pregunta No.11

En referencia a la ilustración 22 se evidencia que el 53% de las personas encuestadas respondió *no*, mientras que el 47% respondió *sí,* a la pregunta: tiene conocimiento de cuál es la ley delitos informáticos que aplica en Colombia.

Mediante la aplicación de la encuesta a estudiantes de la Universidad Autónoma pertenecientes al pregrado de Ingeniería Industrial y adultos pertenecientes a una entidad estatal de la ciudad de Bogotá D.C, existen vacíos y/o desconocimiento por parte de la sociedad sobre los tipos, técnicas, causas, legislación, consecuencias y peligros que abarca la Ingeniería Social.

8.2.1 Recomendaciones de las encuestas

- Las redes sociales no son un juego, hay que utilizarlas con precaución.

- No compartir información confidencial a través de las redes sociales, ya que el enemigo está al volante.

- No comentar, ni publicar información sobre ubicación donde se encuentra teniendo en cuenta que el enemigo puede aprovechar de ello para causar daño.

- Educar a los niños y adolescentes acerca el uso correcto de las redes sociales, los peligros que acechan en ellas, así mismo sobre los tipos de Ingeniería Social existentes para estar alertas, y no caer en la trampa.

- Los padres de familia deben capacitarse y actualizarse en temas de tecnología, internet e Ingeniería Social para evitar que sus hijos y ellos mismos no caigan en manos criminales, saber cómo actuar y que hacer frente a ello.

- No aceptar invitaciones de amistad a personas desconocidas.

- No entablar conversaciones con desconocidos ya que no se sabe cual es la intención de la otra persona.

- Evitar publicar fotos de tipo personal y familiares.

- No compartir archivos sospechosos que provengan de fuentes desconocidas, ya que se podría estar propagando algún virus.

- Administrar de forma segura la cuenta correspondiente a la red social, evitando que sea pública.

- No descargar o dar clic en archivos y/o link de personas desconocidas, es necesario verificar su fuente.

- No prestar sus redes sociales con nadie.

- No comparta los usuarios ni passwords con nadie.

- Utilizar contraseñas robustas que contengan letras, números y caracteres especiales.

- Conocer y comprender la normatividad de delitos informáticos.

- Sospeche de llamadas telefónicas y visitas no programadas.

- Desconfíe de cualquier mensaje de texto SMS, e-mail o llamada telefónica donde le indiquen que ha ganado algo con facilidad, si ni siquiera ha sido participe de ello.

- No responda información sensible y confidencial a través de correos electrónicos a remitentes desconocidos, antes de hacerlo verifique directamente con la persona o compañía solicitante.

  De igual forma se pueden tener en cuenta las recomendaciones brindadas del caso práctico, así mismo los tips nombrados en la campaña de concientización y sensibilización.

Capítulo 9 Conclusiones

Con el desarrollo del presente trabajo de grado se logró:

- Identificar y diferenciar las técnicas de Ingeniería Social, así mismo las técnicas en función de la interacción que se tiene con la víctima.

- Creación del caso práctico donde el objetivo seleccionado fueron niños, niñas y adolescentes de algunos colegios, entre la edad de 10 y 11 años pertenecientes a los grados 5° de primaria y 6° de bachillerato, así mismo los *adolescentes* estarán entre el rango de edad 12 a los 16 años de edad, correspondientes entre a los grados de 7° a 11° de bachillerato, donde se evidencio que es muy fácil que las personas sean victimas de ataques, siendo este caso práctico un ejemplo de tantos casos existentes.

- La ejecución de la encuesta donde se evidencio que las personas no son conscientes que pueden ser víctimas de Ingeniería Social, de igual forma existen vacíos y/o desconocimiento por parte de los encuestados sobre los tipos, técnicas, causas, legislación, consecuencias y peligros que abarca esta temática.

- Brindar recomendaciones con el fin de que las personas no sean víctimas de Ingeniería Social.

- Realizar campaña real de concientización a estudiantes de la Universidad Autónoma pertenecientes al pregrado de Ingeniería Industrial y adultos pertenecientes a una entidad estatal, por medio de charlas sobre la temática de Ingeniería Social, utilizando como medio de material didáctico y audiovisual generado de esta forma mayor impacto.

- Identificar y conocer la normatividad que persigue las acciones de la Ingeniería Social siendo estas actividades catalogadas como delitos que nos castigados por entes reguladores.

Glosario

- **Antivirus:** Software que está en condiciones de buscar y eliminar virus en un sistema informático. Cabe destacar que estos virus son programas que se alojan en la memoria de un ordenador (computadora) con el objetivo de dañar datos o de alterar el normal funcionamiento del equipo.

- **Atacante:** Se hacen pasar por otra persona y convencen a la víctima para entregar información sensible de la organización o sus contraseñas.

- **Ataque:** Es un intento organizado e intencionado causada por una o más personas para causar daño o problemas a un sistema informático o red.

- **Contraseña:** Serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa.

- **Malware:** Son programas informáticos diseñados por ciberdelincuentes para causarle algún daño o perjuicio al usuario como el robo de información, modificaciones al sistema operativo y las aplicaciones instaladas o tomar el control total del equipo.

- **Remtasu**: Es un troyano diseñado para robar información sensible, es una de amenazas más propagadas en Colombia en los últimos meses.

- **TIC:** Las Tecnologías de la Información y la Comunicación, son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos, tales como: computadoras, teléfonos móviles, televisores, reproductores portátiles de audio y video o consolas de juego.

- **Víctima:** Puede ser cualquier persona física o jurídica que haya establecido una conexión a Internet (ya que es la principal ventana de entrada para estas conductas), una conexión entre computadoras, o que en definitiva cuenta con un sistema informático para el tratamiento de sus datos.

- **Virus:** Programas maliciosos que infectan a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo “víctima” (normalmente un ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección.

- **Vulnerabilidad:** Debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

Referencias Bibliográficas

1. https://www.cert.org.mx/historico/documento/index.html-id=16 (04/marzo/2018)

2. https://delitopenal.com/los-delitos-informaticos-tras-la-reforma-del-codigo-penal/ (04/marzo/2018)

3. https://www.unodc.org/documents/ropan/guia.pdf (08/marzo/2018)

4. https://www.mediostic.com/edad-legal-nino-use-redes-sociales-colombia/ (25/marzo/2018)

5. https://canaltrece.com.co/programas/mundo-hacker-colombia/ (25/marzo/2018)

6. https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf (31/marzo/2018)

7. https://bullyingandmobbing.com/casos-de-ciberbullying-ciberacoso-mexico/
(07/abril/2018)

8. http://haycanal.com/noticias/9518/que-hacer-ante-los-ataques-de-ingenieria-social (07/abril/2018)

9. https://idconline.mx/corporativo/2018/04/23/nuevo-caso-de-vishing-contra-usuarios-de-hsbc (14/abril/2018)

10. https://laopinion.com/2016/02/26/cuidado-con-los-ladrones-surfistas-en-el-atm/ (14/abril/2018)

11. https://noticias.caracoltv.com/colombia/creyeron-ser-los-nuevos-amigos-de-james-rodriguez-y-terminaron-estafados-por-un-ciberdelincuente-ie11269 (28/abril/2018)

12. https://definicion.de/antivirus/ (05/mayol/2018)

13. http://www.masadelante.com/faqs/password (05/mayol/2018)

14. https://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913-3 (05/mayol/2018)

15. http://tutorial.cch.unam.mx/bloque4/lasTIC (05/mayol/2018)

16. https://www.infospyware.com/articulos/%C2%BFque-son-los-virus-informaticos/ (05/mayol/2018)

17. https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo (05/mayol/2018)

18. http://bcn.gob.ar/uploads/Dossier-063---Legislacion-Extranjera---Delitos-Informaticos.pdf (20/mayo/2018)

19. http://www.sallent.net/web/blog/?tag=ingenieria-social (20/mayo/2018)

20. http://www.teprotejo.org/index.php/es/ (21/mayo/2018)

21. http://www.urnadecristal.gov.co/bajemos-el-tono (21/mayo/2018)

22. http://www.enticconfio.gov.co/quienes-somos (21/mayo/2018)

23. https://www.redpapaz.org/ (21/mayo/2018)

24. http://www.teprotejo.org/index.php/es/ (21/mayo/2018)