TÉCNICAS DE INGENIERÍA SOCIAL APLICADA EN LOS ESTUDIANTES DE GRADO 11° DE LA CIUDAD DE SAN JUAN DE PASTO

LEYDI DAYANA TAMAYO ARGOTI

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO
2020

TÉCNICAS DE INGENIERÍA SOCIAL APLICADA EN LOS ESTUDIANTES DE GRADO 11° DE LA CIUDAD DE SAN JUAN DE PASTO

LEYDI DAYANA TAMAYO ARGOTI

Monografía presentada como requisito para optar por el título de:
Especialista En Seguridad Informática

Edgar Roberto Dulce Villarreal
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO
2020

Nota de Aceptación

_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

San Juan de Pasto, agosto de 2020

DEDICATORIA

A Dios

Por ser mi guía, mi padre y mi escudo protector, gracias por darme la bendición de salud y vida para poder alcanzar cada una de mis metas, gracias por ser la inspiración para salir adelante, gracias padre omnipotente por cuidar de mí en cada instante y por permitirme obtener conocimientos importantes para mi progreso.

A mi madre

Por su amor, constancia y entrega, por ser una persona inigualable gracias por enseñarme que las metas no son difíciles de lograr siempre y cuando haya un sueño por alcanzar. Este triunfo es para ti mami gracias por brindarme tu mano amiga y por acompañarme en cada instante de mi vida.

A mi padre

Por todo su apoyo por su comprensión, sus concejos que han sido de mucha ayuda en mi formación como persona, por ser un padre ejemplar y por guiarme siempre por el mejor camino, por ser un ejemplo a seguir, por su paciencia, perseverancia y constancia que siempre lo han caracterizado.

A mi hermana

Por ser la persona por la que lucho día a día para que sepa guiar sus pasos juntos a los míos y se forme como una persona integral, por su constancia, empeño y entrega, gracias por ser la causa principal y el motor que me ha impulsado para poder continuar con cada uno de mis proyectos.

A mi novio

Por ser una persona excepcional, por acompañarme en cada paso que doy brindándome siempre su mano amiga, gracias por cada palabra de aliento por estar conmigo en cada momento de mi vida, pero sobre todo gracias por tu amor que ha sido uno de mis impulsos para continuar luchando por cada uno de mis proyectos.

Leydi Dayana Tamayo Argoti

AGRADECIMIENTOS

Agradezco de manera muy especial al Mg. Edgar Roberto Dulce director de la presente monografía, quien con su seguimiento y orientación ha contribuido al buen desarrollo del presente proyecto.

A aquellos docentes, que, con su profesionalismo, exigencia y comprensión, me permitieron crecer y mejorar mis conocimientos y desarrollar mis capacidades como profesional.

A mis compañeros y amigos quienes me brindaron un espacio y con los cuales compartimos momentos agradables en este proceso de formación profesional a todos ellos, muchas gracias.

Expreso mis más sinceros agradecimientos a mi familia que han sido mi motor para continuar y luchar para alcanzar cada meta propuesta.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ATAQUE-CIBERNÉTICO: Se conoce como la acción que busca infringir un sistema de información o una red de datos para beneficio propio.

CIBER-ATACANTE: Persona que posee gran conocimiento relacionado con las tecnologías de información mediante las cuales se utilizan ordenadores y redes de datos para cometer delitos informáticos.

INGENIERÍA SOCIAL (IS): Se conoce como la metodología que permite manipular a la víctima a través de diferentes técnicas para robo o manipulación de información con el fin de agredir y manipular.

SPAM: Se define como mensajes no deseados enviados a partir un correo electrónico, desde un remitente desconocido, mediante el cual algunas personas realizan ataques, que van desde la infección con virus o un tipo de ataque mediante ingeniería social como el phishing.

MALWARE: Software malicioso que tiene como objetivo infiltrarse y causar daño a un sistema de información o generar fallas en su funcionamiento.

NATIVOS DIGITALES**:** Se define a la generación que cuenta con nuevas formas de relación y de comunicación, son la primera generación que ha crecido y ha ido en evolución en conjunto con las tecnologías.

PHISHING: Tipo de ingeniería social, la cual tiene la finalidad de llevar a cabo un engaño y lograr que el usuario otorgue información de modo fraudulento, las acciones más implementadas son: envío de correos electrónicos con enlaces de sitios webs falsos y con esto recolectar usuarios y contraseñas.

RESUMEN

La Ingeniería Social, es un ataque cibernético en el cual se obtiene datos confidenciales a través de la manipulación a la víctima mediante técnicas de persuasión y engaño, es una de las herramientas más utilizadas por los ciber-delincuentes, ya que a través del tiempo debido a la evolución tecnológica se ha ido mejorando e incrementando el robo de información, es por ello mediante el presente estudio monográfico se presenta la problemática e impacto de la ingeniería social en los estudiantes de grado 11° de la ciudad de San Juan de Pasto, para identificar los riesgos y amenazas que existen y así detectar las posibles vulnerabilidades, realizando un estudio de las metodologías usadas de tal manera que se logre determinar los tipos de técnicas aplicables a través de Ingeniería social.

Mediante el presente proyecto de grado se comprenden temáticas importantes como referencias históricas y relevantes de ataques informáticos, teniendo en cuenta conceptos de seguridad informática, técnicas de ataque, tipos de ataque, ciber atacantes o ciber-delincuentes, finalmente se realizarán recomendaciones de cómo evitar ser víctimas de este tipo de ataque y proteger la información adecuadamente.

PALABRAS CLAVE: Ingeniería Social, seguridad informática, ciber-atacante, vulnerabilidad, phishing, delito informático, ataque, confidencialidad, integridad, disponibilidad.

ABSTRACT

Social Engineering is a cyber attack in which confidential data is obtained through manipulation of the victim through persuasion and deception techniques, it is one of the tools most used by cyber-criminals, since over time due The technological evolution has been improving and increasing the theft of information, which is why this monographic study presents the problem and impact of social engineering on 11th grade students in the city of San Juan de Pasto, to Identify the risks and threats that exist and thus detect possible vulnerabilities, carrying out a study of the methodologies used in such a way that it is possible to determine the types of techniques applicable through Social Engineering.

Through this degree project, important topics such as historical and relevant references of computer attacks are understood, taking into account computer security concepts, attack techniques, types of attack, cyber attackers or cyber-criminals, finally recommendations will be made on how to avoid being victims of this type of attack and protect the information properly.

KEYWORDS: Social engineering, computer security, cyber-attacker, vulnerability, phishing, cybercrime, attack, confidentiality, integrity, availability

INTRODUCCIÓN

Hoy en día las personas hacen uso de los diferentes medios de comunicación informática tales como internet, dispositivos móviles, equipos de cómputo o tabletas los cuales son de ayuda en las actividades educativas o de comunicación; sin embargo, debido al uso inadecuado, pueden convertirse en una amenaza latente ya que traerá nuevas vulnerabilidades y riesgos debido a la fácil accesibilidad y exposición de información sensible trayendo consigo consecuencias negativas para los jóvenes.[1]

El desconocimiento en cuanto la buena práctica de protección de información; ha permitido que se vea de alguna manera expuesta a diferentes riesgos y amenazas, siendo de esta forma un componente vital para la manipulación o alteración de los datos por personas inescrupulosas, dado lo anterior es fundamental tener en cuenta los 3 pilares de seguridad de información: Confidencialidad, integridad, disponibilidad.

La información que a diario se comparte a través de redes sociales tiene relación con los siguientes aspectos:

- Lugares que frecuenta
- Actividades que realiza diariamente
- Relaciones personales
- Publicación de fotografías, las cuales pueden ser difundidas y utilizadas por los ciber-atacantes para vulnerar su integridad.

Con la elaboración de esta monografía, se pretende identificar las técnicas de ingeniería social utilizadas por los ciber-delincuentes, permitiendo evidenciar las amenazas y vulnerabilidades presentes en sitios informáticos las cuales podrían perturbar la privacidad de los jóvenes; Dado lo anterior se generará soluciones y recomendaciones para prevención de riesgos y vulnerabilidad de la información personal de los estudiantes. de grado 11° de la ciudad de San Juan de Pasto.

[1] García, Pilar. Los adolescentes: uso y abuso de las nuevas tecnologías y redes sociales [en línea] [citado el 5 de diciembre de 2019]. Disponible en: https://www.avanza-psicologia.es/adolescentes-uso-abuso-nuevas-tecnologias-redes-sociales/

TÍTULO DEL PROYECTO

Técnicas de ingeniería social aplicada en los estudiantes de grado 11° de la ciudad de San Juan de Pasto.

ÁREA DE CONOCIMIENTO: Seguridad Informática.
LÍNEA DE INVESTIGACIÓN: Estudio monográfico de ingeniera social.

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

En la actualidad las tecnologías se han convertido en parte fundamental del diario vivir, logrando cambios importantes en el ambiente social, cultural, modelos de enseñanza educativos, por la gran evolución de la tecnología teniendo acceso a un sinfín de datos sin salir de casa. Las nuevas generaciones o nativos digitales conviven desde que nacen con las TIC siendo más adaptables a los nuevos avances; sin duda los jóvenes tienen un haz sobre la manga, sin embargo, han dejado a un lado la gestión de seguridad y privacidad de la información, trayendo consigo innumerables consecuencias negativas que interfieren en su vida cotidiana.

La ingeniería social se entiende como la obtención de información privada por medio del control a la víctima sin levantar sospechas, comúnmente se realiza a través de medios tecnológicos tales como: celulares, tabletas, equipos de cómputo, etc. Para lo cual es evidente que las nuevas generaciones se han visto expuestas a la manipulación o robo de información confidencial o personal, de acuerdo al artículo de Computer World Colombia[2], el cual menciona que

> La ingeniería social está al servicio del crimen, en el cual se nombra que las causas de la ciberdelincuencia en el año 2017 han incrementado las pérdidas económicas y riesgos informáticos en el mundo corporativo, puesto que mediante un ataque se estima que la cifra de casos de ingeniería social a través de phishing "aumentó de 2015 a 2016 un 22,6% registrando más de 200 denuncias mensuales, por su parte RSA (Rivest, Shamir y Adleman- Sistema criptográfico de clave pública) señala que este tipo de ataques cibernéticos aumentan entre un 30% y un 40% cada año [3], por ende, equivale a un nuevo ataque de phishing cada 30 segundos" llegando a la conclusión que este tipo de acoso a incrementado mundialmente.

Sin embargo, en la actualidad existen muchas carencias de procedimientos que permitan la mitigación de vulnerabilidades ante posibles ataques sin garantizar la privacidad de datos personales, no se han tenido en cuenta procesos o estrategias para la protección de la información; estas inseguridades deben ser analizadas y revisadas por medio de técnicas que implementen métodos de control de riesgos que afectan actualmente a los estudiantes de grado 11° de la ciudad de San Juan de Pasto.

---

[2] La ingeniería social al servicio del cibercrimen, [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: https://computerworld.co/la-ingenieria-social-al-servicio-del-cibercrimen/

[3] Los colaboradores de las compañías son el principal objetivo de la ciberdelincuencia en 2017, [en línea] [con acceso el 11 de enero de 2020]. Disponible en: https://revistadelogistica.com/actualidad/los-colaboradores-de-las-companias-son-el-principal-objetivo-de-la-ciberdelincuencia-en-2017/

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué hábitos de seguridad de la información se deben tener en cuenta para minimizar las vulnerabilidades ante ataques mediante ingeniería social a los estudiantes de grado 11° de la ciudad de San Juan de Pasto?

2. JUSTIFICACIÓN

Desde el punto de vista las nuevas tecnologías son un eje fundamental en la sociedad, sin dejar atrás que a diario en los hogares se presenta una alta demanda en cuanto a la conectividad y acceso a internet, lo que es una excelente ayuda para el avance en la educación, pero también presenta una gran desventaja para los jóvenes que se conectan y comparten con sus amigos y conocidos información privada en la red, lo cual hace que queden completamente vulnerables ante cualquier atacante o delincuente informático; las personas por naturaleza son frágiles frente a la seguridad informática. Los incontables ataques cibernéticos que han ocurrido a través de la historia podrían haberse evitado si se hubiese tenido una cultura preventiva antes de brindar cualquier tipo de información; el conocer las técnicas de ataque y cómo prevenirlas es de gran importancia para poder gestionar políticas de seguridad.

Actualmente cada vez es común el uso de la internet y los diferentes ataques que se generan por la vulnerabilidad en la información que se comparten a través de las redes de datos mediante los diferentes dispositivos tecnológicos como equipos de cómputo, tabletas, teléfonos inteligentes, entre otros, siendo transformadas en la vida cotidiana de cada ser humano, Jeffrey Sanabria[4] sin embargo, como dice el adagio popular "no todo lo que brilla es oro", ya que en meses recientes, se ha visto vulnerada la información publicada por los usuarios y controles de seguridad entre otros.

Por todo lo anterior, es necesario investigar sobre las técnicas más comunes aplicadas en la ingeniería social que se aplican actualmente en cuanto a la manipulación del ciberespacio en los jóvenes por parte de los atacantes informáticos; esto con el fin de realizar un estudio previo y posteriormente para dar soluciones, las cuales contribuirán a controlar y mantener alertas a las víctimas ante posibles ataques informáticos; gracias a estas estrategias se podrá determinar cómo afecta la confidencialidad de la información tales como fotos, vídeos, chats, entre otros.

[4] Seguridad Cultura y prevención para TI.” Redes sociales, entre la ingeniería social y los riesgos a la privacidad”, [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: https://revista.seguridad.unam.mx/numero-12/redes-sociales-entre-la-ingenierí-social-y-los-riesgos-la-privacidad

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Investigar sobre los métodos aplicados a la ingeniería social utilizados en la red que permitan mitigar el riesgo de vulnerabilidades y fallas de la seguridad de la información mediante el uso de internet en los estudiantes de grado 11° de la ciudad de San Juan de Pasto.

3.2 OBJETIVOS ESPECÍFICOS

- Indagar sobre las técnicas de ingeniería social y como se aplican, para identificar los riesgos ante el uso de la red por parte de los estudiantes de grado 11° de la ciudad de San Juan de Pasto.

- Determinar metodologías de ingeniería social para aplicar a los estudiantes de grado 11° en algunos colegios de la ciudad de San Juan de Pasto.

- Analizar los resultados obtenidos ante los ataques informáticos presentados por el uso inadecuado de datos personales por parte de los estudiantes de grado 11° de la ciudad de San Juan de Pasto.

4. MARCO REFERENCIAL

Se describirán las referencias con respecto técnicas de ingeniería social aplicada en los estudiantes de grado 11° de la ciudad de San Juan de Pasto, contribuyendo a dar solución o mejoramiento al presente proyecto.

4.1 MARCO TEÓRICO

Actualmente, el tener conocimiento en seguridad de la información es de gran importancia, genera confianza en el individuo permitiendo así mantener un espacio de interacción y aprendizaje, contribuyendo a un mejor desarrollo personal.

Por lo tanto, se deduce que, mediante el conocimiento de la ingeniería social, permiten aprovechar el uso de las TIC, contribuyendo al desarrollo continuo y adaptándose a las necesidades presentes en el día a día, con el fin de contribuir a la seguridad de los jóvenes.

> A mitad del año 2019 los ataques cibernéticos de phishing fueron dirigidos principalmente a usuarios de computadores Mac y los dispositivos móviles basados en iOS en servicios web basados en un 9% hasta alcanzar los 1,6 millones de ataques destinados a robar datos financieros de los usuarios.
>
> La investigación se basa en estadísticas de amenazas compartidas voluntariamente por los usuarios de Kaspersky Security Network, una infraestructura global en la nube diseñada para dar una respuesta inmediata a las amenazas cibernéticas emergentes. [5]

Technocio[6] Otro ataque más reciente se presentó entre abril y junio del año 2019, en el cual se considera que el mayor número de ciberataques detectados en Colombia se realiza mediante la técnica de exploits, el cual es una llave para que los ciber atacantes logren apoderarse de la información, los ataques de malware más comunes que se utilizan de ingeniería social son los realizados a través del correo electrónico siguen siendo los más frecuentes en el país.

[5] EL UNIVERSAL. “Colombia sufrió 42 billones de intentos de ciberataques”. [en línea] [con acceso el 21 septiembre de 2019]. Disponible en: https://www.eluniversal.com.co/tecnologia/colombia-sufrio-42-billones-de-amenazas-de-ciberataques-IF1698794

[6] Ataques de phishing a usuarios de Mac e iOS aumentaron un 9%. [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: http://technocio.com/ataques-de-phishing-a-usuarios-de-mac-e-ios-aumentaron-un-9/

4.1.1 ENUNCIADOS DE LOS SUPUESTOS TEÓRICOS DE LA INVESTIGACIÓN

A continuación, se presenta la descripción de conceptos más comunes asociados a la presente problemática a tratar.

- **Pilares fundamentales de la seguridad de la Información**: se compone de los 3 conceptos más importantes que son: confidencialidad, integridad y disponibilidad los cuáles se verán representados a través de la siguiente figura.

Figura 1. Pilares fundamentales de seguridad de la información.

Fuente: Domínguez, R (2019). Las TIC.

- **Confidencialidad:** es la protección de la información personal tal modo que no se tenga acceso a la misma sin la debida autorización. (Blog especializado en Sistemas de Gestión de la Información, 2018)

- **Disponibilidad:** permite que la información se mantenga sin ser alterada, para ello es necesario que se ofrezca recursos a usuarios autorizados.

- **Integridad:** garantiza que los datos no hayan sido alterados ni modificados sin autorización, solo se modificará la información de forma autorizada.

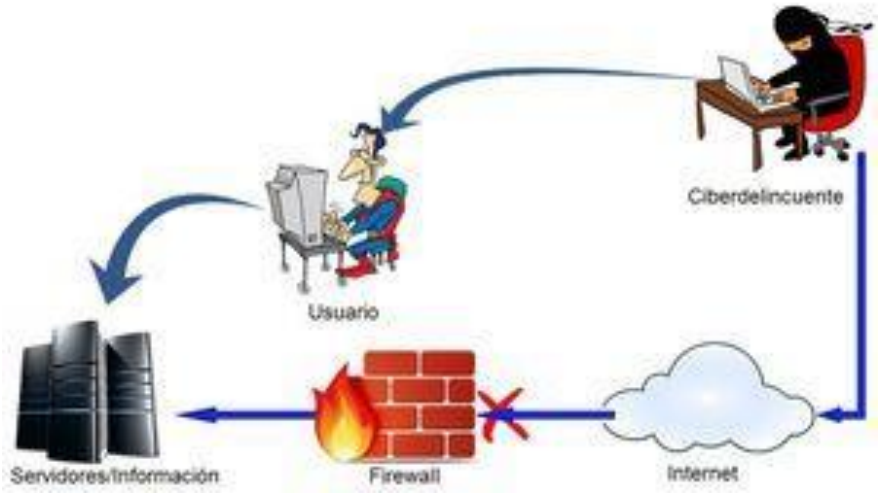
- **Ingeniería social**: acto de manipular a una persona mediante diferentes acciones las cuales le permitirán al atacante la obtención de información privada o acceso a sistemas de información; para minimizar este tipo de riesgos es indispensable realizar capacitaciones, encuestas o entrevistas que permitan a las personas conocer este tipo de técnicas y así evitar caer en las pequeñas

trampas que utiliza el atacante para poder robar información confidencial. (Sandoval Castellanos, 2018)

En la actualidad existen diferentes maneras de realizar un ataque cibernético, por ejemplo: El atacante o ciber-delincuente puede suplir la identidad de una persona con el fin de generar confianza en la víctima obteniendo de esta manera información confidencial como acceso a cuentas bancarias, correo electrónico, redes sociales, datos personales entre otros, otra forma en que el atacante tome control de información confidencial puede ser cuando la víctima ingresa a avisos publicitarios, videos prohibidos de tal forma que el usuario ingrese datos importantes como usuario y contraseña de esta manera el atacante toma el control absoluto de la información.

La siguiente figura representa un tipo de ciberataque de ingeniería social mediante el cual un ciber-delincuente obtiene la información así el sistema a atacar cuente con firewall o cortafuegos de seguridad como se puede observar este sólo sirve de defensa perimetral de las redes, mas no defiende de ataques o errores, tampoco ofrece protección una vez que el atacante lo traspasa interactúa directamente con la víctima obteniendo información concreta.

Figura 2. Técnica de ingeniería social.



Fuente: Árbol de Noticias (2018).

Para evitar ser víctima ante las técnicas de ingeniería social se debe tener en cuenta:

- No enviar mediante correo electrónico, chats o redes sociales datos personales o confidenciales tales como: claves de acceso, cuentas bancarias, información personal, etc.
- No abrir enlaces de emails desconocidos que soliciten datos personales.
- Desconfiar de todos los mensajes que ofrecen oportunidad de ganar dinero, carro o viajes de forma rápida y fácil.
- Verificar que los documentos en físico que se decida arrojar a la basura no posean ningún tipo de información confidencial ya que puede ser utilizada como una pista por los expertos en ingeniería social para lograr captar información.
- Instalar un Antivirus de tal manera que contenga la función de antispyware y antimalware para minimizar riesgos y evitar la pérdida de información.
- Utilizar el sentido común, de tal manera que al recibir mensajes, emails, chats o llamadas telefónicas se evite hacer entrega de información confidencial.

Clasificación de la ingeniería social:

- Tipo: se considera como el aspecto más importante en cuanto al desarrollo del ataque ya que depende de cualidades físicas, sociales o técnicas.
- Operador: principalmente se realiza el ataque por una persona o ciber delincuente o mediante un software automatizado para realizar este tipo de procesos.
- Canal: medio por el cual se realiza el ataque puede ser vía e-mail, redes sociales, páginas web, dispositivos como tabletas, computadores o celulares, la nube.

Como contramedida, para reducir el aumento ante ataques de ingeniería social es mediante la educación, es decir se debe capacitar a las personas en cuanto a las debilidades y las técnicas de engaño más comunes empleadas por los ciber-delincuentes con el fin de lograr identificarlos y dar aviso ante la autoridad.

- **Tipos de ingeniería social:** se debe tener en cuenta que el ser humano es la base más importante cuando se trata de seguridad informática ya que de nada sirve si se tiene firewall, antivirus y otras herramientas de seguridad actualizados si la persona encargada de la información se convierte en víctima entregando toda la información posible al atacante sin darse cuenta.

- **Ingeniería social en personas:** técnicas que tienen en cuenta características comunes de un individuo como, por ejemplo: deseo, codicia, avaricia, miedo, entre otros, con el fin de obtener información sensible o confidencial. (Guedez, 2018)

    - **Suplantación de identidad**: método mediante el cual el atacante asume el rol de la persona que represente autoridad, por ejemplo, puede fingir ser un

coordinador de un área cualquiera y solicitar información específica mediante correo electrónico o formularios webs.[7]

- **Mirar por encima del hombro (Shoulder Surfing):** método mediante el cual se obtiene información confidencial de una persona en concreto ya que, no demanda esfuerzo, es una técnica de vigilancia directa es puesto en práctica fácilmente ya que el atacante se acerca sigilosamente atrás de la espalda de la víctima y observa detenidamente su accionar a través de los diferentes dispositivos que esté utilizando como: dispositivo móvil, monitor entre otros, es así como se podría obtener información confidencial como contraseñas de acceso, códigos de seguridad, generalmente se utiliza en filas de bancos o cajeros automáticos, café-internet o bibliotecas, oficinas, actualmente se usan medios electrónicos como es los celulares o cámaras espías para almacenar información confidencial.[8]

- **Ingeniería Social Inversa (Reverse Social Engineering):** método más desarrollado de la ingeniería social, el atacante convence a su víctima de que posee problemas con su sistema y que necesita de conocimientos técnicos avanzados para poder repararlo de inmediato y este a su vez es capaz de resolver el problema.

  Esta se realiza a través de los siguientes pasos:

  - El atacante daña el equipo del objetivo.
  - Luego se anuncia como la persona encargada de resolver el problema inicial.
  - Se gana la confianza del objetivo obteniendo así información confidencial. (UCERTIFY, 2009)

- **Desarrollar Confianza (Establishing Trust):** la confianza juega un papel muy importante cuando se habla de ingeniería social pues quien la práctica tiene la capacidad de expresarse con claridad, persuadir manteniendo así un bajo perfil siendo amable con su víctima pasando desapercibido.

- **Ingeniería Social en computadores**: técnica que se aplica mediante el uso de una computadora o dispositivos electrónicos tecnológicos.

[7] Méndez Collo, H., & Flórez Ramírez, C. P. Estudio de ingeniería social en el uso de las redes sociales.

[8] Ministerio de Tecnologías de la Información. [en línea] [citado el 25 septiembre de 2019]. Disponible en: (https://www.mintic.gov.co/portal/604/w3-propertyvalue-19215.html)

- **Phishing**: técnica mediante la cual se busca engañar a un grupo masivo de personas a través del envió de emails engañosos, perfiles sociales falsos o mensajes con el fin de robar información confidencial.[9]

- **Dumpester diving**: técnica mediante la cual el atacante husmea en la basura obteniendo así documentos con información personal.[10]

- **Shulder surfing:** técnica que consiste en robar el patrón de desbloqueo, contraseña de un usuario mientras se encuentra descuidado.[11]

- **Redes sociales:** técnica mediante la cual se obtiene información puntual de la víctima a través de una red social falsa además de tener contacto directo con la misma generando un alto grado de confianza, hoy en día las redes sociales son el mayor canal para intercambio de información, permite estar informados, pero también a través del tiempo se ha convertido en una adición para ciertos usuarios; llegando a un punto en que han contribuido a la creación de la identidad, existen usuarios tan "fanáticos" que hasta comparten en sus redes minuto a minuto las actividades que realizan, este tipo de personas son el objetivo principal para los atacantes ya que podrán obtener bastante información y aprovecharse de su víctima.

- **Baiting:** técnica mediante la cual conecta memorias externas con malware sobre el equipo de la víctima con el fin de infectar el ordenador y obtener información**.**

- **Grooming:** técnica mediante la cual el atacante mayor de edad realiza estrategias para persuadir y ganarse la confianza de un infante o joven, posteriormente iniciará un proceso de análisis para aislar a su víctima y averiguara sigilosamente si alguien más hace uso del dispositivo u ordenador con el fin no ser descubierto e inicia su acto macabro el cual tiene el propósito de explotar o abusar sexualmente de la víctima. (Grooming que es como detectarlo y prevenirlo)

- **Sextortion:** técnica mediante la cual el atacante extorsiona a la víctima mediante un contenido erótico o sexual de sí mismo enviándolo a través de diferentes plataformas en internet con el fin de coaccionar a la víctima y obtener lucro de ello.

---

[9] PHISHING "¿Qué es el phishing?", [en línea] [con acceso el 30 septiembre de 2019]. Disponible en: https://www.avast.com/es-es/c-phishing

[10] Portafolio, [en línea] [con acceso el 30 septiembre de 2019]. Disponible en: (https://www.portafolio.co/tendencias/usuarios-el-puntodebil-para-que-entren-cibercriminales-510863)

[11] Ministerio de Tecnologías de la Información. [en línea] [con acceso el 30 septiembre de 2019]. Disponible en: (https://www.mintic.gov.co/portal/604/w3-propertyvalue-19215.html)

- **Ciberacoso:** técnica mediante la cual el atacante causa daño a su víctima de manera repetida, colocando mensajes o contenido multimedia que avergüence a la víctima.

- **Técnicas de ingeniería social de interacción con la víctima.**

  - **Pasivas:** se basa en la observación y análisis a la víctima.
  - **No presenciales:** se basa en la solicitud de información mediante llamadas, chats, e-mails, etc. suplantado la identidad de la víctima.
  - **Presenciales no agresivas:** se basa en el seguimiento constante a la víctima ya sea en su residencia, lugar de trabajo o lugares que frecuenta.
  - **Agresivas:** se basa en la presión psicológica y suplantación de identidad.

- **Recomendaciones de Seguridad:** las recomendaciones de seguridad son pasos elementales a seguir ya que si se tienen en cuenta se podrá mantener absoluta tranquilidad en la privacidad de la información.[12]

- **Seguridad en el equipo:** generalmente los equipos de cómputo son de uso personal y deben cumplir con políticas de seguridad que garanticen que la información que se maneja en ellos es personal e intransferible, es indispensable tener en cuenta:

  - Tener instalado un sistema operativo y aplicaciones con licencia activa legal no pirata.
  - Mantener la configuración de firewall actualizada permanentemente de tal manera que se permita la restricción de accesos no autorizados.
  - Generar contraseñas seguras en cuenta de usuario, utilizando combinaciones de números, letras, caracteres especiales, entre otros.
  - Instalar y mantener actualizado la protección de antivirus.

- **Seguridad en internet:** el acceso a internet hoy en día es uno de los aspectos más relevantes, ya que es común que las personas accedan para búsqueda de información, pasatiempo o comunicación, el ingreso a la red permite mayor vulnerabilidad en la información para ello es para ello es importante verificar los siguientes aspectos:

  - Configurar el nivel de seguridad del navegador.
  - No acceder a sitios web sospechosos

[12]Concepto de norma de seguridad, [en línea] [con acceso el 7 septiembre de 2019]. Disponible en: (https://blogs.imf-formacion.com/blog/prevencion-riesgos-laborales/actualidad-laboral/concepto-de-norma-de-seguridad/)

- Eliminar ventanas emergentes o pop’ups o configurar el bloqueo de ventanas emergentes en el navegador.
- Eliminar periódicamente el historial de navegación, cookies o ficheros temporales.
- Verificar que las páginas a las que se accede son sitios seguros, estos deben contener https://
- No descargar ni ejecutar ficheros de sitios web sospechosos.
- No permitir el almacenamiento de contraseñas a los sitios web que se ingresa.
- Verificar en el enlace del sitio web que se accede, un icono de candado cerrado, este indica que la conexión es segura.

- **Seguridad en e-mail:** e-mail permite enviar y recibir mensajes como mensajes de texto, imágenes, documentos, videos entre otros; se utiliza como medio de comunicación o instrumento de mercadeo, es importante ser prudente a la hora de enviar información confidencial por correo electrónico, ya que viaja a través de varios sistemas conectados en red antes de llegar a su destino, por lo que es posible que alguien lo intercepte y lo lea. Por lo tanto, se debe tener en cuenta las siguientes recomendaciones como protección de seguridad en emails.

  - No abrir emails enviados como spam.
  - No responder emails de contactos desconocidos o publicidad y promociones.
  - No compartir información personal como lugar donde trabaja, dirección exacta de su residencia, teléfono de contacto, número de identificación.
  - No responder a emails enviados por entidades financieras o bancarias, sitios de venta online en los cuales pidan información personal.

4.2 MARCO CONCEPTUAL

Definición de conceptos añadidos al presente proyecto de investigación.

- **Ataque**: método mediante el cual el atacante obtiene información por medio de herramientas tecnológicas las cuales tienen como fin dañar, manipular información confidencial de un sistema de información o si es el caso de información personal.[13]

- **Delitos**: operación que va en contra de la ley o estatuto estipulado en una nación, se realiza con el fin de ocasionar daño a la víctima, los delitos penales se clasifican en dolosos y culposos dependiendo de la acción realizada.[14]

- **Tecnologías de la Información y las Comunicaciones (TIC):** son herramientas digitales las cuales han cambiado la forma de en qué las personas acceden a la información antiguamente se usaba como medios de información las bibliotecas, prensa, televisión o radio hoy por hoy el acceso es más eficiente ya que el internet y sus diferentes canales de acceso como ordenadores, móviles, herramientas y plataformas digitales han facilitado el aprendizaje colaborativo y la apropiación del conocimiento, actualmente las TIC incluyen recursos virtuales en los cuales se encuentran: bases de datos, bibliotecas virtuales, literatura electrónica entre otros y herramientas comunicacionales como chats, e-mails, listas de interés, redes sociales así como también aprendizaje multimedia como videoconferencias o videos interactivos, audios, imágenes etc. (Pedagogía educativa, 2015).

- **Deep Web:** es el contenido de páginas web no indexadas en la red de tal manera que sean invisibles a todos los usuarios.[15]

- **Email o correo electrónico con malware:** los correos electrónicos o e-mails con malware tienen un impacto ya que aplican ingeniería social, generalmente sucede cuando los archivos adjuntos que contienen tren consigo cierto tipo de programas con malware como, por ejemplo: spyware, virus, gusanos, troyanos, entre otros.[16], Es recomendable tener en cuenta que no se debe abrir e-mails

---

[13] Que son los ataques informáticos https://www.hn.pe/blog/que-son-los-ataques-informaticos

[14] Delitos informáticos, [en línea] [con acceso el 1 septiembre de 2019]. Disponible en: (https://www.vendesfacil.com/plataformas-empresariales/delitos-informaticos-caracteristicas/)

[15] ADSL ZONE. Que es Deep Web. [en línea] [con acceso el 1 septiembre de 2019]. Disponible en:(https://www.adslzone.net/como-se-hace/internet/guia-deep-web)

[16] NORFI PC.COM. Evitar la infección por virus o malware a través del correo electrónico, [en línea] [con acceso el 1 septiembre de 2019]. Disponible en: (https://norfipc.com/virus/evitar-infeccion-virus-malware-email-correo-electronico.html)

procedentes de desconocidos, no reenviar cadenas, tener instalado y activo el sistema de protección de antivirus, no abrir links que nos soliciten información o abran videos.

- **Vulnerabilidad:** se relaciona con el riesgo, amenaza o fallo en un sistema informático, comprometiendo así la integridad, disponibilidad o confidencialidad. (Tecnologia + Informática)

- **Ciberseguridad o seguridad informática:** Su principal característica es la protección de información digital la cual se almacena en computadoras, servidores o dispositivos móviles o que se comparte en la nube esta incluye prácticas de ataques, en cuanto a la seguridad es utilizado con aspectos defensivos ante ataques maliciosos.[17]

- **Ciberacoso:** se denomina como acoso cibernético, se realiza mediante el uso de redes sociales las cuales se utilizan para manipular a la víctima mediante ataques personales tales como divulgar información privada, robo de identidad, etc.[18]

- **Phishing:** técnica utilizada por los ciber delincuentes o ciber atacantes para conseguir información confidencial, por ejemplo: claves y detalles de tarjetas de crédito, dando confianza en la víctima[19]

- **Sexting**: se refiere al envío de fotos o videos con contenido erótico o pornográfico por medio de teléfonos móviles o equipos de cómputo a través de aplicaciones de mensajería instantánea, correos electrónicos o redes sociales generalmente se realiza de forma intima, aunque en ciertas ocasiones como es habitual llega a manos de terceros por no respetar dicha intimidad; el remitente se encarga de enviar el contenido a diferentes individuos con el fin de afectar la reputación de una persona.[20]

---

[17] Welivesecurity.com. ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia. Electrónico, [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: (https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/)

[18] Que es el ciberacoso. [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: (https://espanol.stopbullying.gov/acoso-por-internet/qué-es-ur6/índice.html).

[19] ¿Qué es el phishing?, [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: https://www.infospyware.com/articulos/que-es-el-phishing/

[20] El Mercurio, Emolo. [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: (https://www.emol.com/noticias/Internacional/2018/07/27/914811/Sextorsion-El-delitoinformatico-que-atormenta-a-usuarios-de-internet-en-diversas-partes-del-mundo.html)

- **Spam:** es el tipo de mensaje de correo electrónico que se envía como mensaje no solicitado a esto se le denomina spam y se almacena como mensaje basura generalmente es de tipo publicitario, se envía masivamente por lo cual perjudica de una u otra forma al receptor, otro tipo de tecnologías se han visto afectadas por los spams tales como foros, motores de búsqueda, blogs y a través de pop-ups.[21]

- **Pop – Up's**. se denominan como elementos emergentes que aparecen repentinamente en los sitios web o en la pantalla del ordenador indicando publicidad de una marca o negocio al usuario. Generalmente son un inicio de contagio de "malware" como por ejemplo virus o troyanos. Actualmente es común que los exploradores web contengan bloqueadores de ventanas emergentes activados, estos generalmente se pueden desactivar al ingresar a sitios web seguros ya que el uso de Pop-U'ps es normal en ambientes web bancarios o educativos, se usan con el fin de proteger la información de los usuarios y por ende evitar fraudes.[22]

- **Autoprotección**: conjunto de medidas de seguridad que una persona opta para enfrentar los riesgos a los cuales se expone ante cualquier hecho. Es importante tener en cuenta que las vulnerabilidades y las amenazas van cambiando a través del tiempo y las circunstancias, por lo cual es necesario revisar periódicamente los factores de riesgo para que las medidas adoptadas sean las apropiadas y permitan su disminución.[23]

[21] Spam, [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: (http://cefire.edu.gva.es/pluginfile.php/51091/mod_imscp/content/1/prctica_34_actividad_de_introduccin_qu_es_el_correo_masivo.html)

[22] POP UP'S, [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: (https://neoattack.com/neowiki/pop-up/)

[23] Que es autoprotección. [en línea] [con acceso el 7 de septiembre de 2019]. Disponible en: https://autoproteccion-a.fandom.com/es/wiki/ ¿Qué_es_autoprotección%3F

4.3. ANTECEDENTES

Durante el desarrollo del presente documento se ha tomado de referencia estudios realizados relacionados con la temática del presente proyecto evidenciado en la compilación bibliográfica:

- Trabajo de grado denominado “Problemas de ingeniería social y su impacto en la adolescencia colombiana” realizado por Carolina Montes y Viviana Vargas. Bogotá, 2018, 57p.

> Esta monografía presenta un análisis de los problemas a los que se ven abocados los adolescentes a causa de la ingeniería social, en el contexto de las actuales costumbres del manejo de las redes en Colombia.[24]

- Trabajo de grado denominado “Victimización de menores por actos de ciber-acoso continuado y actividades cotidianas en el ciberespacio” realizado por Natalia García Guilabert. España, 2014, 502p.

> El cibercrimen, como concepto a toda la criminalidad cometida en el ámbito del ciberespacio, ha adquirido un inusitado protagonismo en los últimos años. es cierto que no se trata de un fenómeno completamente nuevo, dado que sus primeras manifestaciones surgieron casi al tiempo que Internet comenzaba a dar sus primeros pasos. Sin embargo, ha sido con la popularización de la Red de redes y con su conversión en un nuevo ámbito esencial para la intercomunicación personal, cuando hemos comprendido que más que ante un nuevo tipo de delitos, nos encontramos ante un nuevo tipo de lugar en el que los crímenes se cometen. Una vez más la tecnología modifica los hábitos sociales, hace surgir nuevos intereses, nuevas necesidades, nuevas formas de comunicación social y, también, nuevos crímenes o diferentes concreciones de los mismos.[25]

- Trabajo de grado denominado “Estudio de ingeniería social en el uso de redes sociales” realizado Claudia Ramírez y Harold Collo. Bogotá,2017.

> mediante la cual se investiga acerca de los tipos de ataques, a través de ingeniería social comúnmente conocido como phishing, en el cual se comparte información confidencial y se crea confianza en la víctima, de tal manera que la víctima no se dé cuenta de ello, además de esto se realiza a través de chat, correo electrónico, entre otros.[26]

---

[24] MONTES. Carolina, VARGAS. Viviana. Problemas de ingeniería social y su impacto en la adolescencia colombiana. Bogotá, Dc, 2018, 57p. Trabajo de grado. Universidad Nacional abierta y a distancia. Facultad ciencias básicas tecnología e ingeniería. Especialización en seguridad informática, [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/22583/1/41946700.pdf

[25]GARCÍA GUILABERT. Natalia. Victimización de menores por actos de cibera coso continuado y actividades cotidianas en el ciberespacio. 2014, 502p. Trabajo de grado. Universidad Nacional abierta y a distancia. Facultad ciencias básicas tecnología e ingeniería. Especialización en seguridad informática.

[26]Tesis Ramírez Claudia, Collo Harold, Estudio de ingeniería social en el uso de redes sociales.

- Estudios realizados en la página web, Ciberataques un mal creciente en Colombia[27], realizada por la autora María F. Herrera, indican que los ciberataques en Colombia crecieron alrededor de un 28% en 2017. Según este estudio las amenazas que tuvieron un alto índice de productividad fueron la suplantación de correo corporativo, comercialización de información de tarjetas débito y crédito y estafas por internet.

- Trabajo de grado denominado "Ciberacoso de niños, niñas y adolescentes en las redes sociales: un estudio sobre los sistemas de protección y prevención judicial" realizado por Danyorsa Mabel Rojas Morales.2015,37p.

> Mediante la presente investigación se hará un análisis del ciberacoso contra niños, niñas y adolescentes en las redes sociales, específicamente se enfocará en el estudio sobre los sistemas de protección y los mecanismos de prevención judicial. Se pondrán en consideración algunos delitos que coadyuvan al ciberacoso y por consiguiente se relaciona el internet a partir del cual se funda y desarrollan todas las redes sociales, al mismo tiempo el vehículo por medio del cual los menores acceden y se convierten en víctimas del ciberacoso. [28]

- Estudios realizados en el artículo web denominado la Ingeniería Social: El Ataque Informático Más Peligroso. Según Digital Guardián, el 97% de los ataques informáticos se generan a través de métodos de ingeniería social para conseguir vulnerar información privada. [29]

Bogotá 2017 trabajo de grado. Universidad Nacional abierta y a distancia. Facultad ciencias básicas tecnología e ingeniería.

[27] HERRERA, MaríaF. Ciberataques un mal creciente en Colombia. [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: https://www.lafm.com.co/economia/ciberataques-un-mal-creciente-en-colombia.

[28] MORALES. Rojas. Danyorsa.Mabel. Ciberacoso de niños, niñas y adolescentes en las redes sociales: Un estudio sobre los sistemas de protección y prevención judicial. Bogotá, Dc.2015 Trabajo de grado Universidad Católica de Colombia. Facultad de derecho}. [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: https://repository.ucatolica.edu.co/browse?type=author&value=Rojas+Morales%2C+Danyorsa+Mabel.

[29]La Ingeniería Social: El Ataque Informático Más Peligroso. Julio 2016, [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: https://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

4.4. MARCO LEGAL

Durante los últimos años, la legislación colombiana ha realizado cambios que se ajustan al control de acceso a la información para la defensa de menores de edad en cuanto a conexión a redes sociales, ciberacoso, ciberbullying y todos aquellos delitos que atenten en contra intimidad y el honor de los menores de edad implicados.

La legislación colombiana actuó, en la actualización de las siguientes leyes; las cuales aplican penas y multas más altas a quienes las infrinjan, con base en esto las leyes que se han generado o modificado en Colombia son las siguientes:

4.4.1 LEY 679 DE 2001

> Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.[30]

4.4.2 LEY 1336 DE 2009

> Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.[31]

4.4.3 LEY 1273 DE 2009. ARTÍCULO 269F

> Por medio de la 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**"[32]**

---

[30] [En línea] [con acceso el 11 de Julio de 2019]. Copiado textualmente de: http://www.oas.org/juridico/spanish/cyb_col_ley_679_2001.pdf

[31] [En línea] [con acceso el 11 de Julio de 2019]. Copiado textualmente de: https://www.oas.org/dil/esp/LEY_1336_DE_2009_Colombia.pdf

[32] [En línea] [con acceso el 11 de Julio de 2019]. Copiado textualmente de: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

4.4.4 LEY 599 DE 2000

Se estipula que los delitos que están consagrados en el Código Penal Colombiano, tienen plena aplicación bajo el entendido en que se cumplan las condiciones establecidas para aquellos actos criminales sin importar si se comete en medios electrónicos o tradicionales.[33]

[33] [En línea] [con acceso el 11 de Julio de 2019]. Copiado textualmente de: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

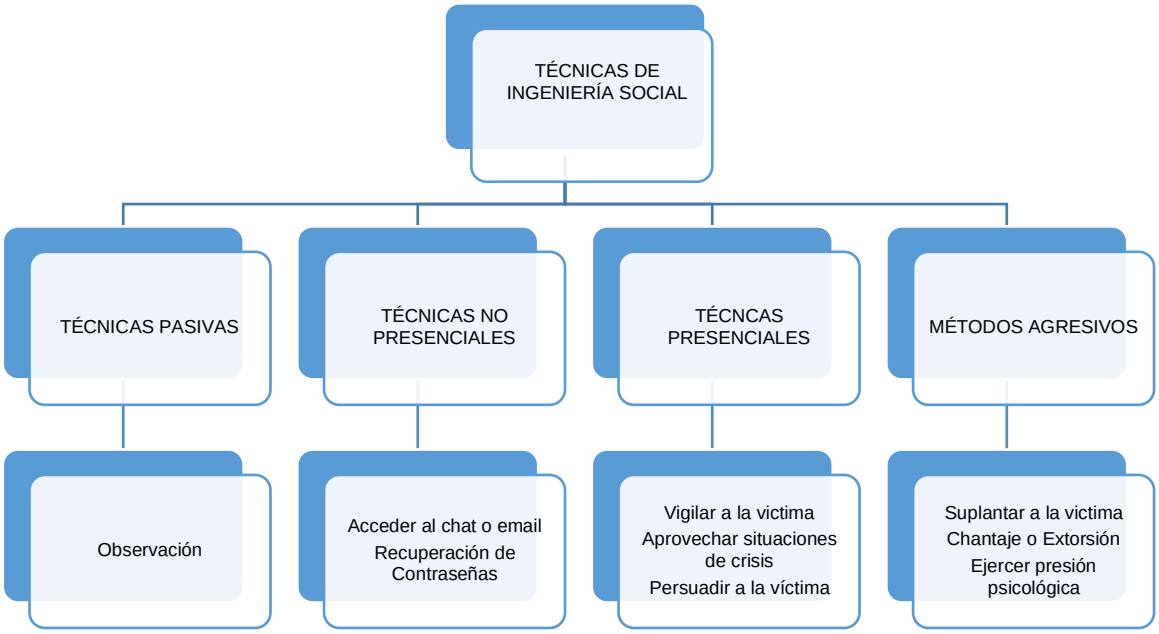
5. RESULTADOS Y EVIDENCIAS

5.1 INFORMACIÓN SOBRE TÉCNICAS DE INGENIERÍA SOCIAL

Actualmente este tipo de técnicas de ataque son las más empleadas ya que es usada con el fin de manipular a la víctima y obtener información confidencial con propósitos personales.

Mediante el siguiente gráfico se puede evidenciar las técnicas de ingeniería social más utilizadas.

Figura 3. Técnicas de ingeniería social.



Fuente: Elaboración propia.

5.2 COMO EVITAR UN ATAQUE DE INGENIERÍA SOCIAL

La ingeniería social se encarga del uso de técnicas de engaño y manipulación que se realizan con los datos de los usuarios y, ante esto, es necesario principalmente proteger y tener sentido común y recordar que la Internet no es segura, por tal motivo es recomendable llevar a cabo estos principales consejos:

- Desconfianza de ofertas laborales o publicidad engañosa que se encuentren en las redes sociales, es recomendable visitar el sitio web o fan page de la entidad para comprobar si se está llevando a cabo algún descuento o promoción en marcha. Si la oferta no existe en el perfil oficial de la empresa es una publicación falsa, es decir, no existe.

- Peligro con la recepción de emails o correos que contengan en el asunto urgente o confidencial procedente de entidades bancarias o instituciones. Se debe tener en cuenta que las entidades financieras no piden las claves de acceso a través del email, por lo tanto, hay que evitar el ingreso a estos enlaces y si existe alguna duda hay que ponerse en contacto con las entidades para verificar la validez de la información.

- Evitar participar en juegos y promociones virales que se lleven a cabo en perfiles falsos de amigos, familiares o conocidos en redes sociales. Ya que en la mayoría de los casos cuando se accede a esto se está autorizando claves de entrada a los perfiles personales.

- En los mensajes SMS no es conveniente el ingreso a los diferentes enlaces que incorporan, al igual que en los casos anteriores, es adecuado, en lo posible, realizar la comunicación con el remitente. (Andalucía es Digital, 2018)

5.3 TÉCNICAS DE INGENIERÍA SOCIAL

Actualmente algunas técnicas de la ingeniería social más utilizadas para atacar son: *Spoofing, Pretexting, Media Dropping y Tailgating.*

5.3.1 SPOOFING

Técnica mediante la cual se envía un email con un enlace determinado. La intención de este ataque es que la víctima ingrese al link enviado mediante el email de tal manera que se obtenga la contraseña del correo electrónico y así tomar control sobre la información que se desee, hay que tener en cuenta que para no caer en esta técnica se debe abrir emails de contactos conocidos.[34]

La solución para esta técnica es la caracterización del correo dirigido hacia el usuario, es importante tener en cuenta abrir solo correos conocidos, debido a que el atacante se disfraza y puede redactar correos electrónicos como originales.

5.3.2 PRETEXTING

Está técnica es conocida como “pretextos” es la que permite la manipulación de la víctima generalmente mediante llamadas o chats buscando pedir información que realiza una simulación de pertenecer al grupo familiar o de amigos que busca ayuda, la forma más sencilla de prevenirlo es utilizar aplicaciones de identificación de llamadas que permitan evidenciar quien está realizando la llamada. [35]

5.3.3 MEDIA DROPPING

Técnica mediante la cual el atacante instala un software en la red de la víctima y ejecuta mediante acceso remoto al equipo víctima con el fin de obtener información confidencial de los medios extraíbles que se conecten.[36]

---

[34] Iglesias Fernández, José Luis. "Técnicas de autenticación criptográfica en señales abiertas GNSS: el fenómeno del spoofing y métodos de defensa."

[35] Revista de Logística. [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: (https://revistadelogistica.com/actualidad/loscolaboradores-de-las-companias-son-el-principal-objetivo-de-la-ciberdelincuencia-en-2017/)

[36] Pruebas de penetración en ingeniería social: cuatro técnicas efectivas. [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: (https://searchdatacenter.techtarget.com/es/consejo/Pruebas-de-penetracion-en-ingenieria-social-cuatro-tecnicas-efectivas)

5.3.4 TAILGATING

Técnica mediante la cual el atacante accede a una instalación física o área restringida mediante engaños con el fin de ingresar e instalar dispositivos para obtener información. [37]

5.4 ANÁLISIS Y PLANTEAMIENTO DE LA ENCUESTA

Se realizó una encuesta (ver anexo B) basada en una serie de preguntas abiertas y cerradas con el fin de tener claridad en cuanto a los conocimientos en seguridad de la información aplicado a los ataques de ingeniería social, se aplica a un grupo determinado de 150 estudiantes de grado 11° que hacen parte de las diferentes instituciones educativas de la ciudad de San Juan de Pasto.

5.5 ANÁLISIS DE RESULTADOS

5.5.1 ENCUESTA DIRIGIDA A LOS ESTUDIANTES DE GRADO 11° DE LAS INSTITUCIONES EDUCATIVAS DE LA CIUDAD DE SAN JUAN DE PASTO.

1. ¿Cuál es su edad?

Tabla 1. Cuál es su edad.

RESPUESTAS	Grado 11°	
	f	h(%)
Entre (14-15) años	50	33%
Entre (15-16) años	90	60%
Entre (17-18) años	10	7%
Total	150	100%

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta, donde f es igual a frecuencia y h es el promedio en porcentaje.

[37] Seguridad Informática, Gf0s. [en línea] [con acceso el 11 de Julio de 2019]. Disponible en: (https://gf0s.com/2016/08/05/tailgating-acceso-a-zonas-restringidas/)

Figura 4. Edad.

Fuente: Elaboración propia.

Esta figura contiene las edades de los estudiantes que fueron encuestados, representados en porcentaje y rango de edad en gráfica pastel.

El resultado del gráfico indica que un 33% de los estudiantes encuestados, tiene una edad promedio entre 14 y 15 años de edad, por otra parte, el 60% de los estudiantes encuestados está entre los 15 y 16 años de edad, mientras que un 7% se encuentra entre los 17 y 18 años de edad.

2. ¿Tiene acceso a las diferentes redes sociales?

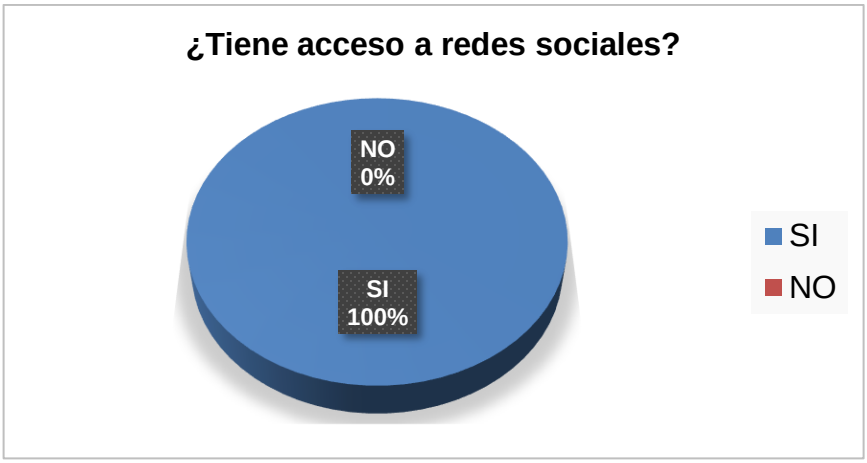
Tabla 2. Tiene acceso a redes sociales.

RESPUESTAS	**Grado 11°**	
	f	h(%)
Si	150	100%
No	0	0%
Total	150	100%

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿si tiene acceso a redes sociales?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 5. Acceso a redes sociales



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Tiene acceso a redes sociales?, de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

El resultado del gráfico indica que el 100% de los estudiantes encuestados tienen cuenta y acceso a redes sociales, existe un 0% de encuestados que respondieron negativamente, el resultado de la encuesta afirma que todos los encuestados utilizan cuentas de redes sociales; el utilizarlas genera un gran impacto, debido a que permiten la comunicación, participación e intercambio de ideas lo cual facilita la ampliación de conocimientos pero si estas son utilizadas de forma inadecuada pondrá en un alto índice de riesgo la información; ya que en las instituciones educativas no existen controles sobre el acceso a ellas es importante aprovechar dicho uso de tal modo que en el plantel educativo se tome ciertas medidas para dar a conocer a los estudiantes los peligros ante el acceso y mal uso de redes sociales.
.

3. ¿Qué información tiene usted visible en su perfil de redes sociales?

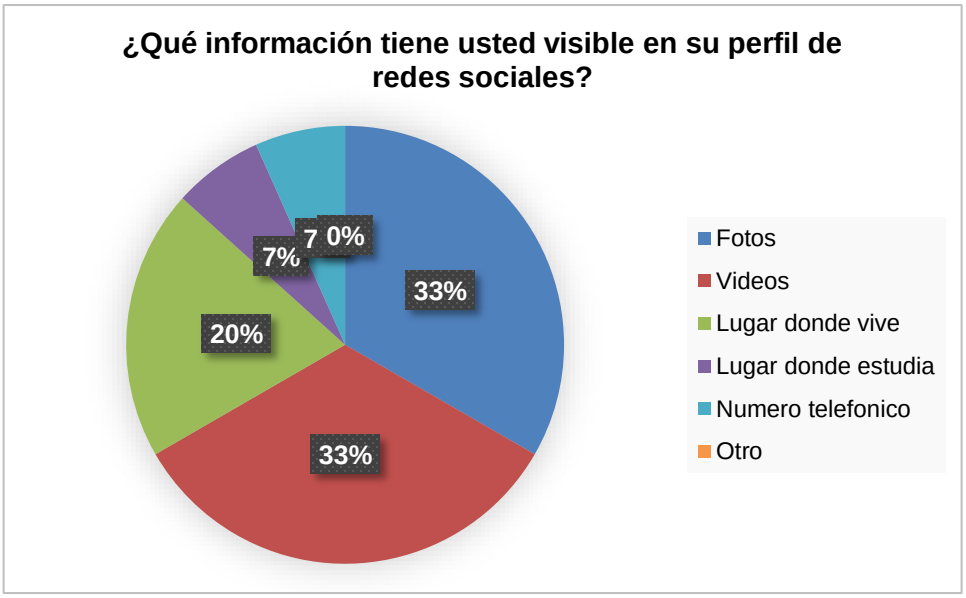
Tabla 3. Información visible en redes sociales.

RESPUESTAS	**Grado 11°**	
	f	h(%)
Fotos	50	33%
Videos	50	33%
Lugar donde vive	30	20%
Lugar donde estudia	10	7%
Número telefónico	10	7%
Otro	0	0%
Total	**150**	**100%**

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Qué información tiene usted visible en su perfil de redes sociales?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 6. Información visible en redes sociales.



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Qué información tiene usted visible en su perfil de redes sociales?, de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

El resultado del gráfico indica que el 33% de los estudiantes encuestados tienen visible fotos y videos, un 20% el lugar donde viven, un 7% el lugar donde estudian y otro 7% el número telefónico, lo que indica que un alto porcentaje de los encuestados están susceptibles ante ataques, actualmente existen muchos riesgos a los que se expone la información al hacer uso de las redes sociales ya que generalmente se comparte información confidencial la cual puede ser utilizada como blanco de ataque, la información puede llegar a manos de desconocidos los cuales pueden aprovechar la ocasión para manipular a la víctima o simplemente robar o modificar los datos con el fin de cometer actos ilícitos, por lo anterior es indispensable validar la información que se comparte tomando ciertas medidas de seguridad que se pueden encontrar en la configuración de privacidad sin embargo es conveniente tener en cuenta que se debe compartir información sensible con un grupo de amigos conocido o solo para el usuario y no para todo público.

4. ¿Qué criterio utiliza para agregar personas a su lista de amigos en redes sociales?

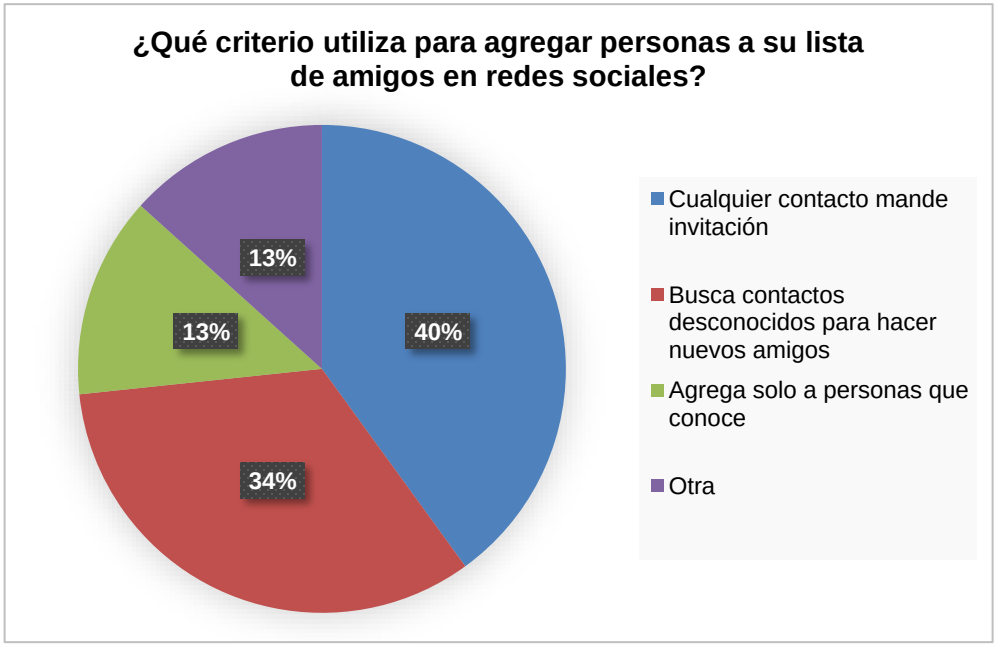
Tabla 4. Uso redes sociales.

RESPUESTAS	Grado 11°	
	f	h(%)
Agrega cualquier contacto que le mande una invitación	60	40%
Busca contactos que no conoce para hacer nuevos amigos	50	34%
Agrega solo personas conocidas.	20	13%
Otra	20	0%
Total	**150**	**100%**

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Qué criterio utiliza para agregar personas a su lista de amigos en redes sociales?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 7. Agregar personas a lista de amigos de redes sociales



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Qué criterio utiliza para agregar personas a su lista de amigos en redes sociales?, de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

El resultado del gráfico indica que el 40% de los estudiantes encuestados acceden a sus cuentas de redes sociales para chatear con sus amigos y/o familiares, mientras que un 34% de los estudiantes usa sus redes sociales para conocer personas, otro 13% utiliza sus redes sociales para compartir pasatiempos con sus amigos y/o familiares y un 13% es de entretenimiento para compartir fotos, videos o juegos en línea.

Analizando estas cifras se puede observar que según los resultados arrojados en la encuesta un alto porcentaje (%) de los encuestados se ven afectados ante el criterio que utilizan para agregar personas a su lista de amigos puesto que la mayoría agregan a personas desconocidas, lo cual puede ser contraproducente ya que es un factor que incrementa el riesgo ante ciberataques o incluso en casos de ciber acoso, hoy en día se ha convertido en una práctica muy peligrosa sobre todo cuando se refiere a menores de edad ya que no se sabe quien se encuentra frente al ordenador generalmente estos ciberdelincuentes utilizan cualquier artimaña para generar confianza en la víctima y atacar para obtener datos confidenciales, siendo así un objetivo claro de estafas, es importante revisar la configuración de privacidad de la red social y validar la información de tal manera que quien envié solicitud de amistad sea solo personas conocidas, el aceptar personas con perfiles falsos podrían contener un sinfín de problemáticas tales como estados de depresión o discriminación, amenazas, burla, intimidación etc. Los atacantes son difíciles de detectar ya que la mayoría son anónimos.

5. ¿Revisa las condiciones o alertas que se muestran acerca de los permisos que se da a la aplicación para poder utilizar su información y fotos?

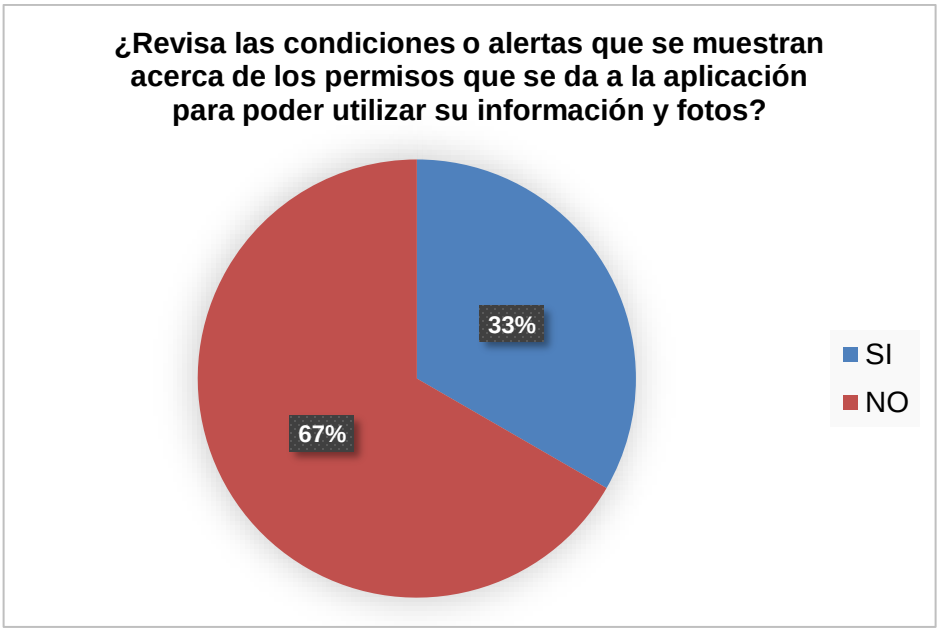
Tabla 5. Alertas de permisos para publicación de fotos.

RESPUESTAS	**Grado 11°**	
	f	h(%)
Si	30	33%
No	120	67%
Total	150	100%

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Revisa las condiciones de alerta que arroja las aplicaciones?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 8. Criterio para agregar personas a redes sociales



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Revisa las condiciones de alerta que arrojan las aplicaciones?, de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

El resultado del gráfico indica que el 67% de los encuestados no revisan las condiciones o alertas que se muestran acerca de los permisos que se da a la aplicación para poder utilizar su información y fotos, mientras que un 33% de los encuestados si revisan las alertas. Después de analizar el resultado de la encuesta se llega a la conclusión que un alto porcentaje (%) de los estudiantes no tienen en cuenta las alertas que se generan en las aplicaciones, sobre todo en las aplicaciones que a redes sociales se refieren por lo cual pueden poner en riesgo la información que a diario comparten como fotos, videos, pasatiempos, ubicación geológica, etc. Por lo anterior, es necesario que se tome medidas de precaución y y comprobar el estado de seguridad de las aplicaciones instaladas en los dispositivos móviles para ello existe Google play protect se utiliza solo en dispositivos Android, es un servicio de protección contra todo tipo de malware para mantener seguros los dispositivos, aplicaciones e información; se encarga de analizar periódicamente el dispositivo con las medidas de seguridad necesarias y si encuentra una aplicación dañina, la elimina automáticamente o informa al usuario que la aplicación contiene riesgos y que se debe desinstalar para no perder información importante, además cuenta con una búsqueda rigurosa en la que cada aplicación debe cumplir con las políticas de privacidad y seguridad quienes la infrinjan serán suspendidos, cabe destacar que hay que estar muy alerta ante este tipo de notificaciones para prevenir ataques futuros, también contiene una opción

en caso de hurto o perdida del dispositivo con la función encontrar mi dispositivo, la cual permite acceder desde una cuenta de Google mediante la cual se podrá bloquearlo remotamente o eliminar todos los datos si es necesario.

6. ¿Conoce usted que es la ingeniería social?

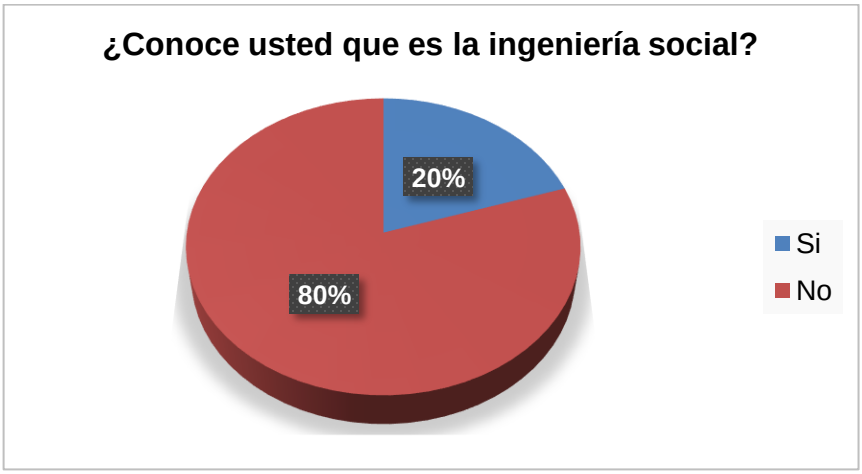
Tabla 6. Ataque de ingeniería social.

RESPUESTAS	Grado 11°	
	f	h(%)
Si	20	20%
No	130	80%
Total	150	100%

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Conoce usted que es la ingeniería social?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 9. Ataque de ingeniería social.



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Conoce usted que es la ingeniería social?, de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

El resultado del gráfico indica que el 80% de los estudiantes encuestados dijeron no tener conocimiento ante los ataques de la ingeniería social, mientras que solo un 20% de los estudiantes encuestados afirmaron que sí tienen conocimientos de ataques de la ingeniería social, lo cual indica que un gran porcentaje de los

encuestados pueden ser víctimas de ataques de ingeniería social por no tener el conocimiento necesario, hoy en día este tipo de técnicas son muy conocidas en el mundo cibernético, generalmente se basa en la manipulación psicológica a través del phishing (manipulación de la víctima y suplantación personal), vishing (manipulación victima a través de llamadas telefónicas identificándose como una organización de buen nombre), utiliza las redes sociales para acceder a la información y obtener información confidencial, es común encontrar que muchos de los ciberdelincuentes que utilizan este tipo de ataques suplantan la identidad de sus víctimas además de robar credenciales, con el fin de robar dinero e información dado lo anterior es indispensable la capacitación continua que permita identificar los tipos de ataque de ingeniería social, las claves para detectar, evitar, prevenir y combatir ataques futuros con el fin de mantener seguridad a la hora de navegar y compartir información en redes sociales.

7. ¿Ha recibido usted llamadas, mensajes de texto, e-mails, chats mediante los cuales le soliciten datos personales o confidenciales?

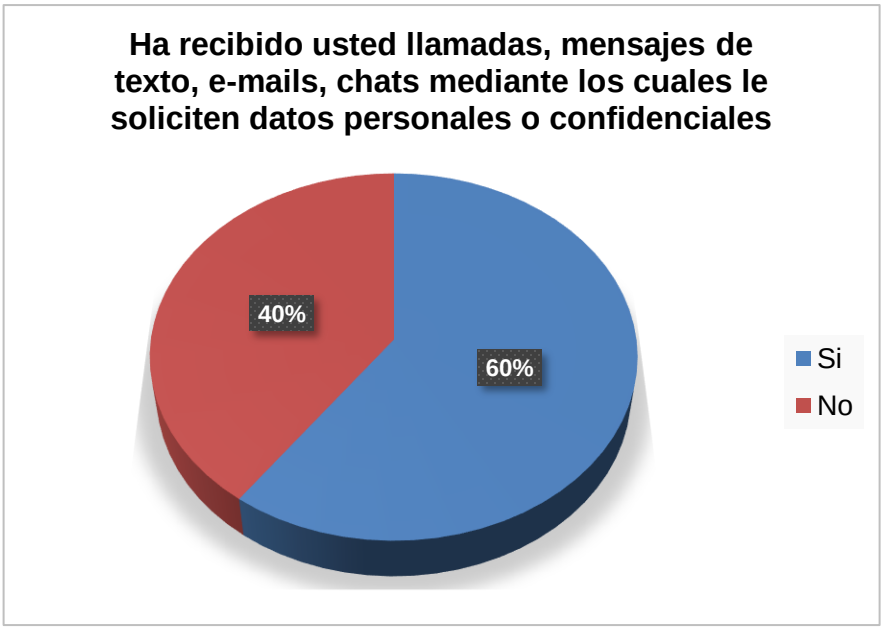
Tabla 7. Solicitud de datos personales o confidenciales.

RESPUESTAS	**Grado 11°**	
	f	h (%)
Si	90	60%
No	60	40%
Total	150	100%

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Ha recibido usted llamadas, mensajes de texto, e-mails, chats mediante los cuales le soliciten datos personales o confidenciales?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 10. Solicitud de información confidencial.



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Ha recibido usted llamadas, mensajes de texto, e-mails, chats mediante los cuales le soliciten datos personales o confidenciales?, de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

El 60% encuestados, respondieron afirmativamente frente al recibir llamadas, mensajes de texto, e-mails, chats que les solicitaban información personal, mientras que un 40% de los encuestados respondieron negativamente.

Se pudo deducir que existe una amenaza permanente sobre los estudiantes ya que existen personas inescrupulosas con fines delictivos que buscan obtener información confidencial de manera fraudulenta, generalmente se realizan a través de la recepción de emails personales, mensajes de texto con publicidad engañosa o recepción de llamadas en las cuales el atacante se encarga de persuadir a la víctima mediante la manipulación o engaño generando confianza en su víctima de tal manera que esta entregue información sin percatarse de ello; es así como se ha llegado a casos extremos como por ejemplo acoso sexual, trata de blancas, extorción y una infinidad de actos delictivos que han generado gran impacto en la sociedad actual, para prevenir este ataque es necesario realizar un análisis de mejora y control a nivel de seguridad informática en las instituciones educativas de tal manera se pueda actuar de forma inmediata en el momento en el que este tipo de ataques sucedan.

8. ¿Ha recibido capacitación acerca de seguridad de la información o cómo protegerse ante ataques informáticos?

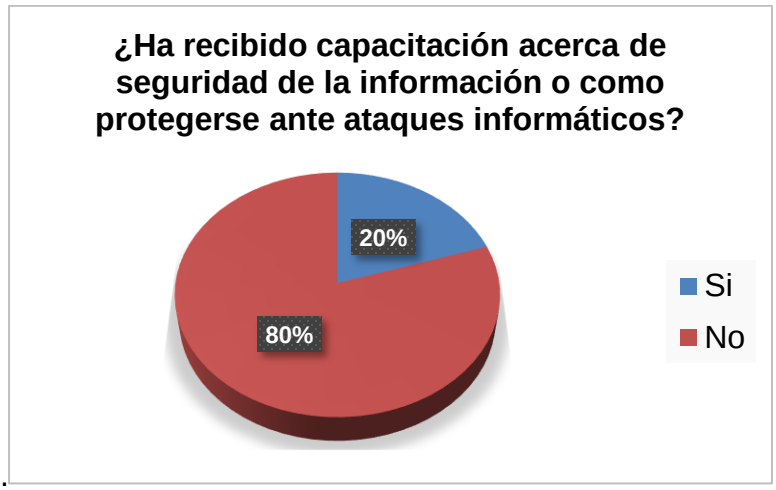
Tabla 8. Capacitación de seguridad de la información.

RESPUESTAS	Grado 11°	
	f	h(%)
Si	30	20%
No	120	80%
Total	150	100%

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Ha recibido capacitación acerca de seguridad de la información?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 11.Como protegerse ante ataques informáticos



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Ha recibido capacitación acerca de seguridad de la información?, de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

El 80% de los estudiantes encuestados, respondieron negativamente a que no han recibido capacitación acerca de la seguridad de la información o cómo protegerse ante ataques, mientras que un 20% de los estudiantes encuestados respondieron afirmativamente.

Los resultados obtenidos a través de la encuesta demuestran que un alto porcentaje (%) de los encuestados no cuentan con ninguna capacitación referente a la seguridad informática, en la actualidad la causa principal de robo de información se debe a errores propios ya que son causadas por el mal accionar de los usuarios por desconocimiento en cuanto a políticas y medidas de seguridad informática, lo anterior implica que se estaría en riesgo eminente por desconocer los métodos de ataque y las formas de protección, mediante la capacitación continua se podrá reducir el riesgo de ataques como phishing, sexting, ramsonware entre otros.

Dado lo anterior, es importante sensibilizar a los estudiantes en cuanto a cómo actuar y evaluar el correcto uso de la seguridad de la información para tomar medidas inmediatas de protección de información; para mejorar los aspectos de seguridad y garantizar el cumplimiento de los 3 pilares: disponibilidad, integridad y confidencialidad de tal manera que se aproveche las herramientas, políticas y controles de seguridad con el fin de generar interés en la necesidad de adquirir conocimientos cuando de seguridad informática se trata, la manera más adecuada de reducir un ataque informático es la formación ya que detecta, previene y evita ser víctimas de ciberataques.

9. ¿Qué factores cree usted que ponen en peligro la información que comparte en internet?

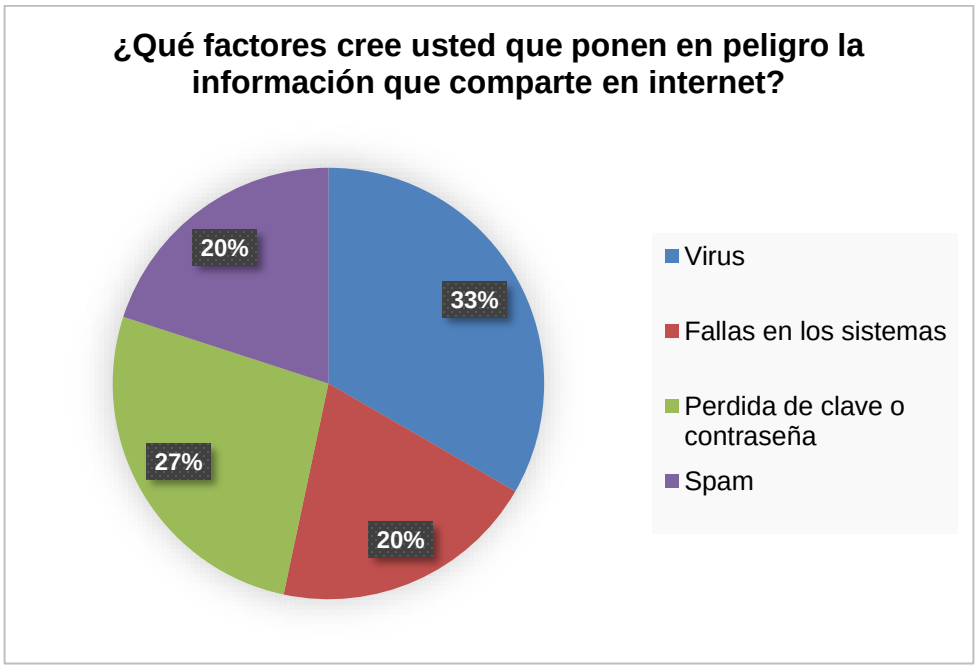
Tabla 9. Causas que afectan la seguridad de la información.

RESPUESTAS	**Grado 11°**	
	f	h(%)
Virus	50	33%
Fallas en los sistemas	30	20%
Perdida de clave o contraseña	40	27%
Spam	30	20%
Total	**150**	**100%**

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Qué factores cree usted que ponen en peligro la información que comparte en internet?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 12. ¿Qué factores cree usted que ponen en peligro la información que comparte en internet?



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Qué factores cree usted que ponen en peligro la información que comparte a través de internet?, de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

El 33% de los encuestados, afirman que los factores que ponen en peligro la información son los virus, otro 20% afirman que se debe a fallas en los sistemas, un 27% afirman que se debe a la pérdida de la clave o contraseña mientras que un 20% afirman que se puede ver afectada por Spam (generalmente se encuentra en e-mails).

Es así como se puede concluir que los factores que ponen en peligro la información que se comparte a través de internet según la población encuestada son los virus, ya que no se cuenta con las condiciones para dar un buen uso a las herramientas de protección de información por lo cual hay que permanecer alerta, no abrir e-mails sospechosos y eliminarlos inmediatamente de la bandeja de entrada y de la papelera de reciclaje, no descargar archivos sospechosos, tener instaladas las mejores herramientas para detección de virus confiable, mantener activo el Windows defender, actualizar con frecuencia los sistemas de protección, analizar mediante el antivirus cada uno de los dispositivos extraíbles que se inserten en el ordenador, no ejecutar programas desconocidos, instalar periódicamente parches de seguridad, realizar mediante el antivirus un escaneo en tiempo real de todos los archivos almacenados en el ordenador, mantener actualizado el sistema operativo, mantener activa la seguridad en el navegador de tal forma que se tenga desactivado los plug-ins, cookies ya que son potencialmente vulnerables ante ataques

cibernéticos, cerrar inmediatamente el sitio web si el navegador indica que no es un sitio seguro.

10. ¿Usted ha sido víctima de ataques informáticos en los que tenga que ver robo de su información personal o divulgación de información que comprometa su integridad?

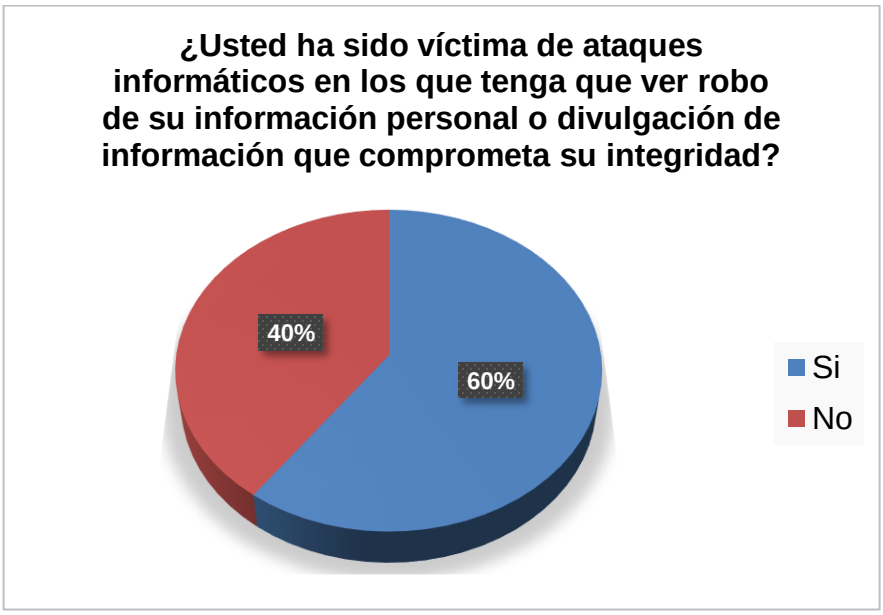
Tabla 10. ¿Ha sido víctima de ataques informáticos?

RESPUESTAS	**Grado 11°**	
	f	h(%)
Si	90	60%
No	60	40%
Total	150	100%

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Ha sido víctima de ataques informáticos?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 13. ¿Ha sido víctima de ataques informáticos?



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Ha sido víctima de ataques informáticos?, de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

El 40% de los encuestados, respondieron negativamente que no han sido víctimas de ataques informáticos, en los que tenga que ver con robo de la información personal o divulgación de información que compromete su integridad, mientras que un 60% de los estudiantes encuestados respondieron afirmativamente.

Se deduce que un gran porcentaje de la población encuestada han sido víctimas ante el robo o manipulación de información personal en los cuales ha tenido mucho que ver el engaño y divulgación de información de personas desconocidas; hoy en día la infiltración de información se ha convertido en la principal amenaza ante ciberataques, los delincuentes aprovechan la falta de información de ciertos usuarios para cometer actos delictivos como robo de información, suplantación de identidad, etc. Trayendo consigo efectos negativos sobre las víctimas como por ejemplo: aspecto personal y dificultades psicológicas que han afectado notablemente la conducta, conduciendo a innumerables problemas en el ambiente social y familiar; por lo anterior es necesario tener en cuenta las prácticas de protección y las tácticas utilizadas por los atacantes para ello es indispensable mantener un plan de acción de prevención y detección por parte de la institución educativa y los estudiantes de tal manera que se tenga en cuenta medidas preventivas tales como: Definición de políticas de privacidad y seguridad en la información confidencial, desarrollo o ejecución de planes de ciberseguridad en los cuales se debe tener en cuenta la formación y sensibilización de los datos que se comparten vía internet, definir políticas de seguridad en cuanto al uso de medios tecnológicos que determine el alcance de uso de ordenadores o conexión de dispositivos a la red de la institución educativa.

11. ¿Qué medios de comunicación piensa usted que pueden influir en la seguridad de su información?

Tabla 11. Medios de comunicación que influyen en la seguridad de la información.

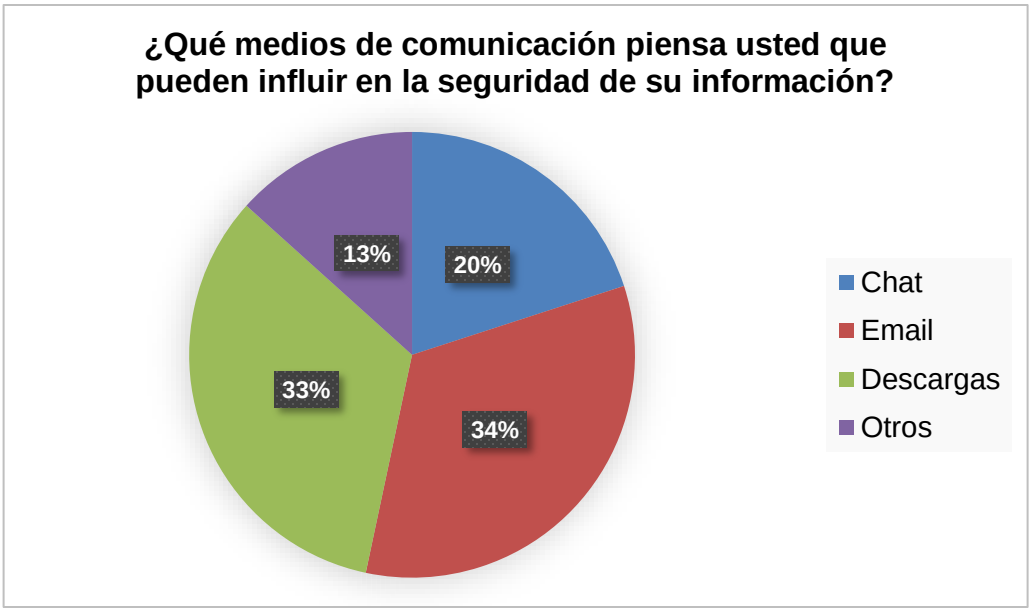
RESPUESTAS	**Grado 11°**	
	f	h (%)
Chat	30	20%
Email	50	34%
Descargas	50	33%
Otros	20	13%
Total	**150**	**100%**

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Qué medios de comunicación piensa usted que pueden influir en

la seguridad de su información?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 14. Medios de comunicación que influyen en la seguridad de la información.



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Qué medios de comunicación piensa usted que pueden influir en la seguridad de su información?, de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

El 33% de los encuestados, afirman que las causas influyen en la seguridad de la información son las descargas de ciertos archivos que se almacenan en el ordenador, mientras que un 34% piensan que los emails que se reciben como los que se envían pueden ser rastreados afectando la seguridad de la información, un 20% piensan que los chats con personas, ya sean contactos propios o personas diferentes pueden afectar la seguridad de la información mediante el envió de links, spams u otros métodos para captar información confidencial mientras que un 13% piensa que las causas que afectan la seguridad de la información es sniffer.

Por los resultados obtenidos se concluye que los medios de comunicación que más influyen en cuanto a seguridad de información son la recepción y envió de e-mails, en la actualidad existen infinidad de ataques informáticos uno de los mas conocidos y utilizados vía correo electrónico es el phishing como se ha explicado en capítulos anteriores se encarga de la suplantación de identidad mediante el robo de contraseñas; es importante que tanto el plantel educativo, padres de familia y estudiantes tomen precauciones como por ejemplo no acceder a enlaces o links provenientes de desconocidos, nunca entregar datos personales sino se conoce la

procedencia de la persona que lo solicita o si es un sitio web seguro, cambiar las contraseñas de acceso periódicamente además de utilizar diferentes contraseñas para cada cuenta, no abrir ni responder correos de spam, utilizar herramientas de seguridad : antivirus, antispyware, actualizaciones de seguridad entre otros.

12. ¿Los equipos a los que se conecta cuentan con protección como antivirus o antispyware actualizados?

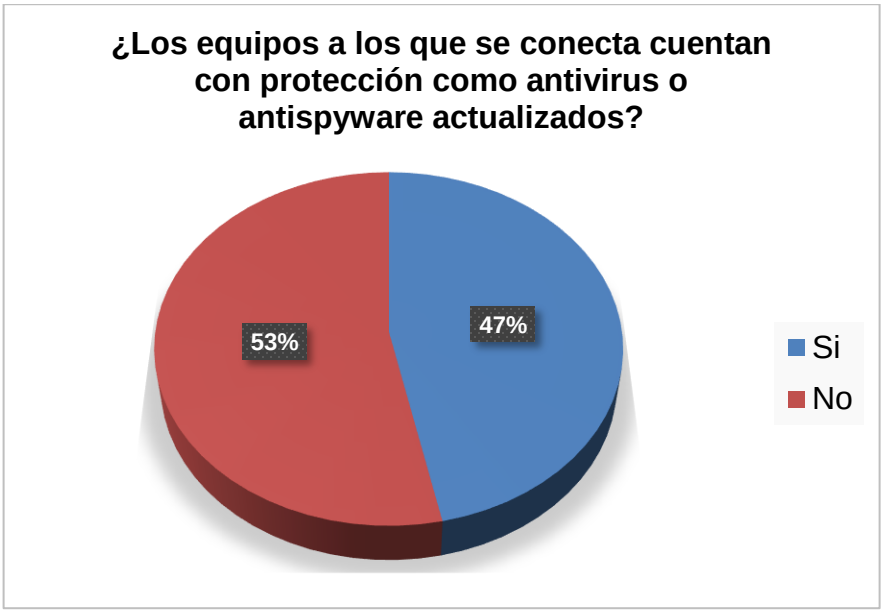
Tabla 12. Equipos contienen medidas de protección de información.

RESPUESTAS	**Grado 11°**	
	f	h(%)
Si	70	47%
No	80	53%
Total	150	100%

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Los equipos a los que se conecta cuentan con protección como antivirus?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 15. Cuenta con protección de antivirus.



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Los equipos a los que se conecta cuentan con protección como antivirus?, de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

El 47% de los encuestados, respondieron negativamente a que los equipos a los que se conectan cuentan con protección antivirus o antispyware debidamente actualizado, mientras que un 53% de los encuestados respondieron afirmativamente.

Dado lo anterior, se puede deducir que gran cantidad de los equipos de cómputo a los que se conectan los estudiantes no cuentan con antivirus y antispyware actualizado, lo que implica que la información que se almacena en los equipos sea alterada o eliminada, generalmente los virus ingresan a través de unidades de almacenamiento como USB, Discos duros externos, al recibir correos electrónicos de procedencia sospechosa, ingreso a sitios web inseguros; estos a su vez logran afectar el buen funcionamiento del ordenador enviando continuamente mensajes o abriendo ventanas emergentes, ocultar archivos, abrir o reproducir videos, imágenes o audios, ralentizan la memoria RAM ya que impiden que se ejecuten archivos o procesos del sistema operativo, se crean almacenan archivos maliciosos sobre el disco del ordenador, en fin existen un sin número de ataques que se generan a través de virus y spyware; Para lo cual es importante que en cada equipo de cómputo se mantenga actualizada la protección de antivirus y antispyware, si se hace uso del sistema operativo Windows es recomendable mantener activo Windows defender es un software gratuito que permite la identificación de cualquier tipo de malware que afecte el buen funcionamiento del ordenador este a su vez se actualiza cada vez que se actualice las funciones del sistema operativo; en el mercado existen varios proveedores de seguridad que contienen buenos sistemas para detección de virus y pueden ser utilizados en los diferentes sistemas operativos como: Windows, Mac y Android, además poseen paquetes de seguridad de acuerdo a las necesidades de cada usuario para la detección temprana de virus y antispyware.

13. ¿La contraseña de acceso a sus redes sociales, correo electrónico, etc., es segura? es decir, ¿cuenta con caracteres especiales, combinación de mayúsculas, minúsculas y números?

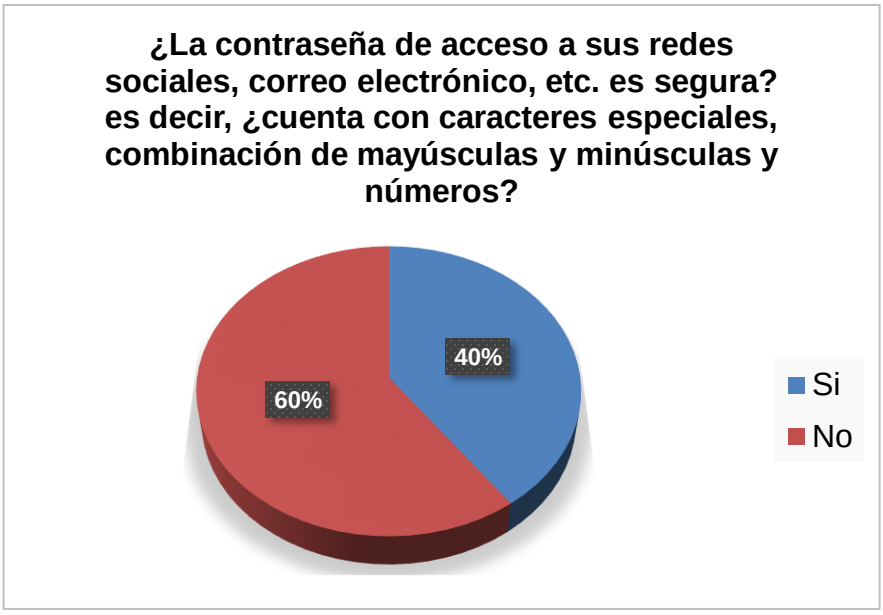
Tabla 13. Contraseña segura de acceso.

RESPUESTAS	**Grado 11°**	
	f	h(%)
Si	60	40%
No	90	60%
Total	150	100%

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿La contraseña de acceso a sus redes sociales, correo electrónico, etc. es segura?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 16. Contraseña segura.



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿La contraseña de acceso a sus redes sociales, correo electrónico, etc. es segura? es decir, ¿cuenta con caracteres especiales, combinación de mayúsculas y minúsculas y números? de los estudiantes que fueron encuestados, representados en porcentaje en gráfica pastel.

Como se puede observar en la gráfica de pastel el 60% de los encuestados respondió negativamente, mientras que un 40% de los encuestados respondieron afirmativamente. Lo cual significa que la mayoría de los encuestados no poseen medidas de seguridad necesarias como la utilización de caracteres especiales, combinación de mayúsculas y minúsculas y números para el acceso a las diferentes cuentas como: redes sociales, correos electrónicos, páginas web, sistemas de información, entre otros los cuales contienen información privada o confidencial a la que no puede acceder cualquier persona, es común encontrar este tipo de problemas ya que generalmente las personas prefieren utilizar contraseñas cortas, palabras lexicalizadas como por ejemplo nombre propio, números del 1 al 5, número de identidad, etc. De tal modo que sean fáciles de recordar para no generar inconvenientes a la hora ingresar a cada cuenta sin tener que recuperar la contraseña cada vez que ingresa; por desgracia este método incumple con las requisitos mínimos de seguridad; hoy por hoy esta práctica se ha convertido un método peligroso ya que facilita a los atacantes el ingreso y robo a cuentas con datos personales o confidenciales, por ello es importante tomar medidas de protección de seguridad para el acceso a cuentas en las que se explique las formas de creación de contraseñas robustas y seguras lo ideal es combinar caracteres especiales con mayúsculas, minúsculas y números, con el fin de disminuir la

probabilidad de ataques, además se debe cambiar periódicamente las contraseñas y memorizarlas, no compartir el método de creación de contraseñas con nadie ya que si el ciberdelincuente realiza una investigación exhaustiva sobre el perfil de la víctima podría descubrir fácilmente la contraseña y acceder a los datos personales.

14. ¿Usted utiliza la misma contraseña de acceso a sus redes sociales, correo electrónico, etc.?

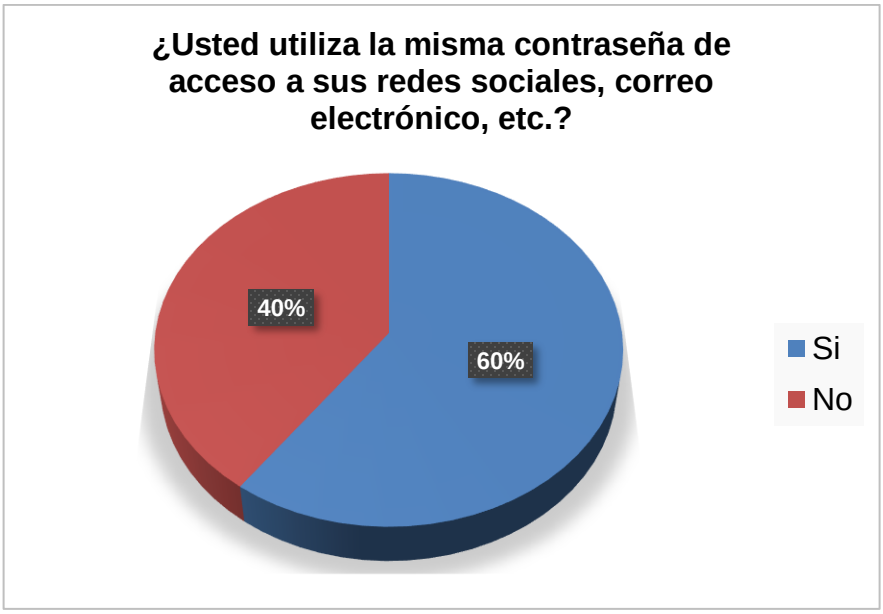
Tabla 14. Utiliza la misma contraseña de acceso.

RESPUESTAS	Grado 11°	
	f	h(%)
Si	90	60%
No	60	40%
Total	150	100%

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Usted utiliza la misma contraseña de acceso a sus redes sociales, correo electrónico, etc.?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 17. Utiliza la misma contraseña de acceso.



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Usted utiliza la misma contraseña de acceso a sus redes sociales, correo electrónico, etc?, de los

estudiantes que fueron encuestados, representados en porcentaje en gráfica de pastel.

El 40% de los encuestados respondió negativamente, mientras que un 60% de los encuestados respondieron afirmativamente. Lo cual significa que el (60%) de los encuestados utilizan la misma contraseña de acceso en sus diferentes redes sociales, correos electrónicos, etc. Esto es común ya que generalmente las personas prefieren utilizar las mismas contraseñas de acceso con el fin de no olvidarlas y posterior a ello perder el acceso a sus redes, emails etc. Es recomendable no reutilizar las contraseñas de acceso ya que son la llave de protección y privacidad a cada una de las cuentas, sin embargo en la era actual se ha recurrido a utilizar una contraseña fácil de recordar , utilizarla en varios procesos poniendo en riesgo toda la información; será más fácil para el ciber-delincuente acceder a una cuenta y tomar poder sobre las demás cuentas vinculadas suplantando la identidad de la víctima, tomando números telefónicos que pueden ser utilizados para extorción o saber hábitos y hobbies para manipular y obtener información confidencial, para ello es importante que se debe hacer uso de buenas prácticas como utilizar diferentes contraseñas de acceso para cada cuenta, modificar las claves periódicamente, no entregar las contraseñas de acceso a nadie, no acceder a redes W-Fi abiertas ya que son un canal de comunicación de fácil acceso en la que terceros podrán interceptar contraseñas a través de un keylogger ,si se olvidan con facilidad es recomendable utilizar gestores de contraseñas los cuales se encargan de generar una nueva contraseña y almacenarla, se debe permanecer alerta con las preguntas de seguridad que se generan al crear una nueva contraseña, no almacenar en papel o en medio digital ninguna contraseña, evitar crear contraseñas con datos personales como fechas de nacimiento propio o de núcleo familiar , números de identidad, el hacer uso de buenas prácticas permitirá mantener segura la información sin mayor implicación a que terceros hagan de las suyas con los datos confidenciales. .

15. ¿Cambia constantemente sus contraseñas de acceso?

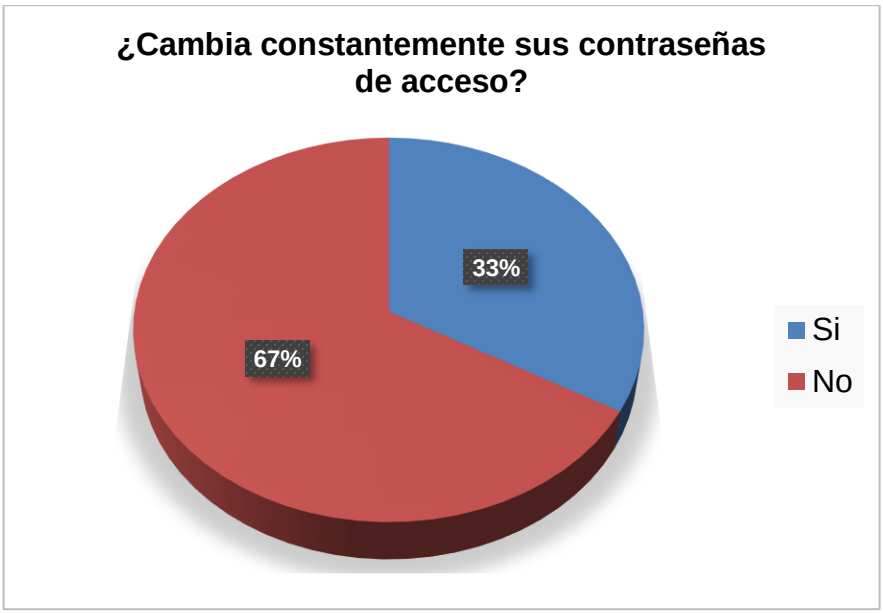
Tabla 15. Cambio de contraseña.

RESPUESTAS	**Grado 11°**	
	f	h(%)
Si	50	33%
No	100	67%
Total	150	100%

Fuente: Elaboración propia.

La tabla anterior indica los resultados que obtuvieron los estudiantes encuestados con la pregunta: ¿Cambia constantemente sus contraseñas de acceso?, donde f es igual a frecuencia y h es el promedio en porcentaje.

Figura 18. Cambia constantemente las contraseñas.



Fuente: Elaboración propia.

Esta figura contiene las respuestas de la pregunta: ¿Cambia constantemente sus contraseñas de acceso?, de los estudiantes que fueron encuestados, representados en porcentaje en la gráfica de pastel.

El 67% de los encuestados respondió negativamente y un 33% de los encuestados respondieron afirmativamente que realizan cambios constantemente de las contraseñas de acceso. Mediante el resultado de la encuesta se pudo deducir que un gran porcentaje (67%) de la población encuestada no cambia la contraseña de acceso a las diferentes cuentas por temor a perderlas, olvidarlas o simplemente por desconocimiento en seguridad de información ; dado lo anterior es posible afirmar que no se realiza cambio de las credenciales de acceso por los casos expuestos con anterioridad. Actualmente gran parte de ataques cibernéticos ocurren por vulnerabilidad o debilidad durante la creación de contraseñas de acceso, los dispositivos móviles y ordenadores almacenan gran cantidad de información confidencial por lo cual es aconsejable cambiar la contraseña periódicamente por una nueva; es importante no reutilizar contraseñas pasadas o utilizar contraseñas cortas ya que será un blanco de ataque por ciberdelincuentes, hoy por hoy es fundamental hacer uso de contraseñas seguras ya que son una puerta de acceso a todo tipo de información,se debe tener en cuenta que existen métodos de protección de privacidad y seguridad, en este contexto y con el objetivo de que se gestione de forma segura las contraseñas se debe tomar medidas de seguridad como: capacitaciones y buenas prácticas de tal forma que se permita gestionar de modo

eficiente la información en cuanto a la correcta gestión y creación de contraseñas de autenticación y así impedir que los atacantes aprovechen este tipo de riesgos y logren suplantar la identidad de las personas.

6. MÉTODOS DE PREVENCIÓN PARA REDUCIR ATAQUES DE INGENIERÍA SOCIAL

Después de realizar la encuesta y determinar posibles problemas ante ataques de ingeniería social, es posible mejorar las técnicas de seguridad de la información de la siguiente manera.

6.1 CAPACITACIONES

Es importante implementar métodos de capacitación a los jóvenes, ya que después de los hallazgos encontrados mediante la aplicación de la encuesta existe un porcentaje alto de estudiantes que poseen desconocimiento ante los ataques de ingeniería social, entonces no sabrían cómo evitarlos. Una de las recomendaciones es no entregar información confidencial o personal sin antes contar con la debida autorización de los padres o tomar precauciones ante cualquier ciberataque, es recomendable realizar capacitaciones con el fin de demostrar de qué manera los atacantes puede ocultar y manipular a su víctima mediante su información personal.

6.2 POLÍTICAS DE SEGURIDAD

Se debe incluir políticas básicas de seguridad en cada una de las instituciones educativas, como por ejemplo hacer uso de la política de prohibición de uso de redes sociales y acceso a páginas para adultos, es necesario concientizar a los estudiantes que deben establecer seguridad en las redes sociales, correos electrónicos entre otros, para que personas inescrupulosas no puedan acceder a la información personal.[38]

6.3 ACTUALIZACIÓN

Para poder llevar a cabo medidas preventivas es importante que tanto estudiantes como el personal de las instituciones educativas se encuentren en constante capacitación para generar alertas ante posibles amenazas y dar solución lo más pronto posible. Es recomendable mejorar las estrategias de seguridad, actualizando constantemente los antivirus de cada equipo, mejorando los servidores (firewall, encriptación SSL/TLS, entre otros) e implementar herramientas para el control en la red (switches, puntos de acceso inalámbricos, firewalls, clientes).

[38] Clavijo, Ciro Antonio Dussan. "Políticas de seguridad informática." *Entramado* 2.1 (2006): 86-92.

6.4 SOFTWARE DE SEGURIDAD

Es necesario hacer uso de software de seguridad como: Antivirus, antispyware Cortafuegos, bloqueador de ventanas emergentes(pop-ups), redes privadas virtuales (VPN) de acceso remoto seguro, sistemas de prevención y detección de instrucciones (IPS/IDS), que permita proteger la información ante nuevos ataques y amenazas en la red de datos. Es recomendable realizar antes una evaluación de los componentes que la institución posee y de acuerdo a ello implementar un paquete de seguridad que ofrezca total control y protección ante posibles ataques de ingeniería social.

6.5 COPIAS DE SEGURIDAD

Es importante realizar copias de seguridad constantemente las cuales permiten evitar la pérdida de información confidencial, es recomendable revisar que los sistemas de respaldo funcionen correctamente, además es necesario que el almacenamiento de las debidas copias de seguridad se realice en otros dispositivos, debido a que existen diversos ataques de ingeniería social que pueden cifrar las copias de seguridad.

6.6 CONTRASEÑAS

Es necesario hacer uso de la política de seguridad para el correcto uso de contraseñas, deben ser seguras, contar con 8 a 10 caracteres como mínimo combinando mayúsculas, minúsculas, utilizando caracteres especiales o símbolos, realizar cambios de forma periódica como mínimo a 5 meses y no hacer uso de las mismas claves en todas las redes sociales, correos electrónicos o medios electrónicos a los que se tenga acceso.[39]

[39] Política de contraseñas y seguridad de la información. INTECO. [En línea] [con acceso el 30 de noviembre de 2019]. Disponible en: https://www.unirioja.es/servicios/si/seguridad/difusion/politica_contrasenas.pdf

7. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

Dentro del marco de la investigación del presente proyecto se plasma y se describe el proceso de técnicas de ingeniería social aplicada a estudiantes de grado 11° de la ciudad de San Juan de Pasto, para después determinar las conclusiones y recomendaciones del caso.

Por ende y en este contexto, se dio posibles soluciones del problema de investigación planteado. Ahora ya concluida la validación de la propuesta presentada y con los resultados obtenidos que permiten comprobar si el desarrollo de la propuesta, obedece o se relaciona a alguna de las hipótesis planteadas al principio del proceso investigativo. Así, finalmente concluir aspectos específicos con la información recolectada.

8. CONCLUSIONES

- Mediante la presente investigación, se logró identificar que el nivel de vulnerabilidad es bastante alto, dado que la información compartida es fácil de capturar por los escasos conocimientos que presentan los estudiantes en cuanto a seguridad de información, esto se evidencio durante la aplicación de la encuesta.

- Se descubrieron bastantes vulnerabilidades a través de los resultados de la encuesta, dado que no existe un método de capacitación que permita a los estudiantes obtener los conocimientos necesarios en seguridad informática, dado lo anterior se debe tener en cuenta que tanto padres de familia como docentes se comprometan en sensibilizar a los jóvenes en la aplicación de buenas prácticas y políticas de seguridad que permitan gozar de beneficios sin comprometer información personal o confidencial.

- La ingeniería social es un método de ataque cibernético que afecta a las personas más vulnerables, para evitar esta situación, es necesario gestionar la información a través de los diferentes métodos de comunicación y redes sociales para procesar adecuadamente la información para evitar y prevenir futuros ataques.

- Según el análisis realizado a los estudios y antecedentes encontrados durante esta investigación, se identificó que los adolescentes son los más vulnerables ante ataques de ingeniería social, teniendo en cuenta que a través del tiempo se han venido empleando nuevas técnicas de ataques, los cuales podrían ser evitadas si existe un acompañamiento de los padres o docentes.

- Con los resultados obtenidos en las encuestas se deduce que los estudiantes no protegen su información, exponiendo sus datos para que puedan ser robados por ciberdelincuentes, debido a que, un 73% acepta cualquier tipo de invitación y busca personas no conocidas en las redes, un 67% de los estudiantes no revisa las condiciones y alertas de las aplicaciones, un 53% no posee antivirus en sus equipos, un 60% no posee contraseñas seguras, un 60% utilizan las mismas credenciales de acceso para todos los sitios y un 67% no cambia sus claves de ingreso.

9. RECOMENDACIONES

- Para un mejor manejo de la información personal es recomendable realizar capacitaciones continuas en cuanto a seguridad de la información y cómo protegerse ante ataques de ingeniería social.

- Concientización de los peligros del internet, generando diferentes alertas en las instituciones educativas de las técnicas que los ciber-atacantes utilizan actualmente, de tal manera que genere el conocimiento necesario para evitar ser víctimas de estos ataques.

- Realizar diferentes campañas sobre el uso de las herramientas tecnológicas apropiadas, que permitan identificar los riesgos ante los ataques cibernéticos que se presentan frente a las técnicas de ingeniería social.

- Protección de los equipos móviles y de cómputo en la red, utilizando diversas herramientas como antispyreware y antivirus totalmente actualizados.

- Denunciar cualquier tipo de comportamiento sospechoso o extraño y alertar a familiares, docentes y autoridades competentes para tomar las medidas correspondientes frente a los ataques cibernéticos.

- Se debe actualizar los contenidos y plan de estudios expuestos en la materia de informática, de tal manera que se incluya temáticas tendientes a la seguridad de la información.

10. DIVULGACIÓN

La divulgación de este proyecto se ejecutó a estudiantes de grado 11° de las diferentes instituciones educativas de la ciudad de San Juan de Pasto, no posee restricción alguna ya que la información desarrollada es pública.

De igual manera se espera compartir este proyecto en el repositorio o espacio que tenga asignado la Universidad Nacional Abierta y a Distancia UNAD en la nube de tal manera que se dé a conocer la monografía tanto a estudiantes como a los usuarios que ingresen al repositorio.

REFERENCIAS BIBLIOGRÁFICAS

Tesis: MONTES. Carolina, VARGAS. Viviana. Problemas de ingeniería social y su impacto en la adolescencia colombiana. Bogotá, Dc, 2018, 57p. Trabajo de grado (Problemas de ingeniería social y su impacto en la adolescencia colombiana). Universidad Nacional abierta y a distancia. Facultad ciencias básicas tecnología e ingeniería. Especialización en seguridad informática. [En línea]. Fecha. [Abril 2019]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/22583/1/41946700.pdf

GARCÍA GUILABERT, Natalia. Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio. Murcia, España. 2014, 502p. Trabajo de grado (Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio). Universidad de Murcia [En línea]. Fecha. [Abril 2019]. Disponible en: https://digitum.um.es/digitum/bitstream/10201/40868/1/Tesis%20Natalia_Garcia_Guilabert_Victimización%20de%20menores%20por%20ciberacoso%20continuado.pdf

Articulo Web: HERRERA, María F. Ciberataques un mal creciente en Colombia. [En línea]. Fecha. [Abril 2019]. Disponible en: https://www.lafm.com.co/economia/ciberataques-un-mal-creciente-en-colombia.

HYPPONEN, Mikko. Ciberataques [En línea]. Fecha. [Abril 2019]. Disponible en:https://www.bbvaopenmind.com/articulos/ciberataques/

RINCON, Alberto. ÁVILA, William. Simbiosis vital para describir el ciberbullying en Colombia Ciberataques estamos preparados [En línea]. Fecha. [abril 2019]. Disponible en: http://www.scielo.org.co/pdf/recig/v12n14/v12n14a09.pdf.

BALLESTEROS, Benjamín, MATA, Leticia. Jóvenes Bullying y Ciberbullying. [En línea]. Fecha. [abril 2019]. Disponible en: http://www.injuve.es/sites/default/files/2017/42/publicaciones/revista_completa_injuve_115.pdf.

CENTRO DE ESTUDIOS ANDALUCES, Bullying, cyberbullying y dating violence [En línea]. Fecha. [abril 2019]. Disponible en: https://www.centrodeestudiosandaluces.es/datos/publicaciones/Actualidad75.pdf.

Tesis: MORALES.Rojas. Danyorsa.Mabel. Ciberacoso de niños, niñas y adolescentes en las redes sociales: Un estudio sobre los sistemas de protección y prevención judicial. Bogotá, Dc.2015 Trabajo de grado (Ciberacoso de niños, niñas y adolescentes en las redes sociales: Un estudio sobre los sistemas de protección y prevención judicial.) Universidad Católica de Colombia. Facultad de derecho. Disponible en: https://repository.ucatolica.edu.co/browse?type=author&value=Rojas+Morales%2C+Danyorsa+Mabel.

Stopbullyng.gov, Que es el ciberacoso. [En línea]. Julio 2018. [28 Abril de 2019]. Disponible en: https://espanol.stopbullying.gov/acoso-por-internet/qué-es/ur6/índice.html.

Internet Segura for Kids (IS4K). Ciberacoso escolar. [En línea] [28 abril de 2019]. Disponible en: https://www.is4k.es/necesitas-saber/ciberacoso-escolar.

Pantallas Amigas 2014. ¿Cómo actuar ante el ciberacoso? Ignora, bloquea, pide ayuda y denuncia [En línea]. Mayo 21 2014 [28 abril de 2019]. Disponible en: https://www.youtube.com/watch?v=tVAjiyNzYq0

Ciberacoso (Cyberbullying): Lo que necesita saber Por Common Sense Media, Understood Founding Partner [En línea] [28 abril de 2019]. Disponible en:https://www.understood.org/es-mx/friends-feelings/child-social-situations/online-activities-social-media/cyberbullying-what-you-need-to-know

BELTRÁN, Mónica, En: El País Compartir No Siempre es bueno en. mayo 2019 Disponible en: https://elpais.com/elpais/2019/03/27/planeta_futuro/1553676865_249212.html.

MORENO, Megan.Acoso cibernético: información importante para los padres. Julio 2018 https://www.healthychildren.org/Spanish/family-life/Media/Paginas/cyberbullying.aspx.

We live security 5 cosas que debes saber sobre la Ingeniería Social [En línea]. Enero 2016 [28 abril de 2019]. Disponible en: https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/

Tesis Ramírez Claudia, Collo Harold. Estudio de ingeniería social en el uso de redes sociales. Bogotá 2017 trabajo de grado (Estudio de ingeniería social en el uso de redes sociales). Universidad Nacional abierta y a distancia. Facultad ciencias básicas tecnología e ingeniería. Especialización en seguridad informática. Disponible en:

https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14505/1/17659358.pdf

En: Revista Enter. La Ingeniería Social: El Ataque Informático Más Peligroso. Julio 2016 Disponible en: https://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

B secure pasión por la seguridad Técnicas y ataques de ingeniería social. Disponible en: https://www.b-secure.co/recursos/infografias/tecnicas-y-ataques-de-ingenieria-social

Noticias de seguridad informática. DIVERSAS METODOLOGÍAS Y TIPOS DE ATAQUES DE INGENIERÍA SOCIAL. [En línea]. Agosto 2016 [28 abril de 2019]. Disponible en: https://noticiasseguridad.com/importantes/diversas-metodologias-y-tipos-de-ataques-de-ingenieria-social/.

ALZATE CASTAÑEDA, Cristian Camilo y GALEANO VILLA, Jorge Luis. Protocolo de Políticas de Seguridad Para las Universidades de Risaralda. Trabajo de grado Profesional en Ingeniero de Sistemas y Telecomunicaciones. Risaralda.: Universidad Católica de Risaralda. Facultad de ciencias básicas e ingeniería, 2013. 100 p. Disponible en: https://docplayer.es/5605322-Protocolo-de-politicas-de-seguridad-informatica-para-las-universidades-de-risaralda-jorge-luis-galeano-villa-cristian-camilo-alzate-castaneda.html

UNIR. “La Ingeniería Social, acercándonos a los molestos Spam, Phishing y Hoax”. TEMPERINE, Marcelo. Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. Buenos Aires, 2013, 12p. Trabajo de investigación (Doctorando en Derecho). Universidad Nacional del Litoral. Facultad de Ciencias Jurídicas y Sociales. Argentina.

MIFSUD, Elvira. “Introducción a la seguridad informática”. [En línea]. Marzo 2012. [abril 28 de 2019]. Disponible en: http://recursostic.educacion.es/observatorio/web/ca/software/softwaregeneral/1040-introduccion-a-la-seguridad-informatica?start=1.

SANCHEZ ARTEAGA, Juan Miguel. Estudio y análisis del uso de las redes sociales en la ciudad de Cuenca y elaboración de un manual de buenas prácticas de usuario. Cuenca, 2011, 140p. Trabajo de investigación (Ingeniero en sistemas). Universidad Politécnica Salesiana. Facultad de educación. Cuenca.

Caviativa Patricia, Jaramillo, Valentino. “Prevención de acoso en aulas y ciberacoso en la educación superior a través de recursos educativos digitales abiertos”. Trabajo

de grado España 2018.Universidad de Alicante Disponible en: http://hdl.handle.net/10045/84896

Rodríguez Carmen, Martínez Pecino, Roberto Segura.” Journalistic treatment of adolescent cyberbullying in the Spanish press; Tratamiento periodístico del ciberacoso adolescente en la prensa española”. España.2018. [En línea]. 2018. [abril 28 de 2019]. Disponible en: http://revistas.ucm.es/index.php/ESMP/article/view/62239

GARCIA ROMERO, JOAN ENRIC. Estudio de metodologías de ingeniería social. Trabajo de grado España 2019. Universitat Oberta de Catalunya http://hdl.handle.net/10609/89045

ACOSTA PINEDA, SANTIAGO, BOHADA, JOHN A, PINEDA, MAGDA LORENA. Ingeniería Social En Instituciones De Educación Superior. Pamplona 2018.Universidad pamplona Disponible en: http://revistas.unipamplona.edu.co/ojs_viceinves/index.php/RCTA/article/view/3026 Universidad de pamplona.

LÓPEZ, CARLOS, Ingeniería social: el ataque silencioso. El salvador 2015. editor: El Salvador, North América: ITCA, Editores, 2015. Escuela Especializada en Ingeniería. Disponible en http://hdl.handle.net/10972/2910

MENDEZ, ALEJANDRO, Estudio de metodologías de ingeniería social España 2018.Universitat Oberta de Catalunya. Disponible en: http://hdl.handle.net/10609/90305

ICONTEC INTERNATIONAL. NORMA TÉCNICA COLOMBIANA - NTC 1486. [En línea]. [Consultado abril 2019]. Disponible en: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

FREIRE, Teresa. CORTEZ, María. Las vulnerabilidades humanas en relación a la Seguridad Informática para evitar la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica. Ambato, 2013. Universidad Técnica de Ambato. Ecuador.

GARCÍA, Alonso y ALEGRE RAMOS. María del Pilar. SEGURIDAD INFORMÁTICA ED.11 Paraninfo. Madrid: Paraninfo, 2011. 163p. ISBN 8497328124, 9788497328128

GONZÁLEZ AGUDELO, Daniel. El riesgo y la faculta de políticas de seguridad informática una amenaza en las empresas certificadas. Bogotá, 2014, 22p. Trabajo de investigación (administración de la seguridad y salud ocupacional). Universidad Militar Nueva Granada. Facultad de relaciones internacionales, estrategia y seguridad. Cundinamarca.

GUERRERO, David. MONCAYO, Laura. PARRA, Juanita. Tesis de Grado [En línea]. [Consultado mayo 2019]. Disponible en: 2015. http://www.institutomerani.edu.co/publicaciones/tesis/2015/cyberbullying%20_acoso_escolar_era%20virtual.pdf.

ORTEGA, Jessica. BUELGA, Sofía. CAVA, María. Influencia del clima escolar y familiar en adolescentes, víctimas de ciberacoso. En: Comunicar. Vol.; 24. No.(Feb.2016); p. 57-65.

TICSCONSULTING. “Ingeniería Social: explotar por medio de la manipulación y el engaño el eslabón más débil de la cadena de seguridad: factor humano”. [En línea]. 18 enero 2011. [11 mayo de 2019]. Disponible en: http://www.ticsconsulting.es/blog/generar-claves-seguras-3.

URRUTIA, José. HERNÁNDEZ, Geovanna. Ingeniería social a través de medios informáticos, análisis de las posibles amenazas existentes en la facultad de ciencias administrativas de la universidad de Guayaquil. Guayaquil, 2015. Universidad de Guayaquil. Ecuador.

HADNAGY, Christopher. Ingeniería social. El arte del hacking personal. Anaya Multimedia-Anaya Interactiva, 2011. 400p LEY 1620 - MINISTERIO DE EDUCACIÓN NACIONAL [En línea]. [Consultado mayo 2019]. Disponible en: http://www.mineducacion.gov.co/1759/articles327397_archivo_pdf_proyecto_decreto.pdf

CRECE EL ACOSO VÍA INTERNET ENTRE ESCOLARES EN COLOMBIA [En línea]. [Consultado abril 2019]. Disponible en: http://www.mineducacion.gov.co/observatorio/1722/article-300085.html

FORMATO - NTC 1486. [En línea]. [Consultado abril 2019]. Disponible en: https://sig.unad.edu.co/

RINCÓN, Alberto. ÁVILA, William. Simbiosis vital para describir el Ciberbullying en Colombia, en este caso tomaremos una de las preguntas la cual es “Ha sufrido algún ataque cibernético” [En línea]. [Consultado mayo 2019]. Disponible en: 2014. http://www.scielo.org.co/pdf/recig/v12n14/v12n14a09.pdf

LEGUIZAMON, Mayra. EL PHISHING. España, 2014, 47p. TRABAJO FINAL DE GRADO (GRADO EN CRIMINOLOGÍA Y SEGURIDAD). Universidad Jaime I. España CASTRO, FRANCISCO. MIRÓ, FERNANDO. ¿Nos parecen más inseguros los ciberlugares después de un ciberataque? España, 2018 Ministerio de Economía y Competitividad, Gobierno de España. [En línea] mayo 2019 [Consultado abril 2019]. Disponible en: http://www.ehu.eus/ojs/index.php/inecs/article/view/19689.

GRUPO BANCOLOMBIA. Ingeniería social [En línea] mayo 2019 [Consultado abril 2019]. Disponible en:https://www.grupobancolombia.com/wps/portal/personas/aprender-es-facil/seguridad/internet/ingenieria-social

TUDELA DE MARCOS, SERGIO, BARRÓN LÓPEZ DE RODA, ANA Redes sociales: del ciberacoso a los grupos de apoyo online con víctimas de acoso escolar / Social net Works: from cyberbullying to online support groups with bullying victims. Málaga 2017.Trabajo de investigación (Psicología). Universidad de Málaga, Facultad de Psicología.

CSO.España edición digital 36 Redes sociales, el vehículo perfecto para un ciberataque masivo. España 2018. [En línea]. [Consultado mayo 2019]. Disponible en:https://cso.computerworld.es/cibercrimen/redes-sociales-el-vehiculo-perfecto-para-un-ciberataque-masivo.

AMARO, JOSÉ, RODRÍGUEZ, CITLALLI, MACÍAS, MARÍA, ANDRADE, MARÍA. Ciberataques A Un Paso De La Ciberguerra.Mexico.2018. [En línea]. [Consultado mayo 2019]. Disponible en: http://revistas.ujat.mx/index.php/ecosoc/article/view/2250

PISCITELLI, Emiliano. Ingeniería Social: Cuáles son los tipos de ataque. [En línea]. RedUSERS. 2015., 5 p. Disponible en: http://www.redusers.com/noticias/ingenieriasocial-cuales-son-los-tipos-de-ataque/.

El Uso Educativo De Las Redes Sociales [En línea]. [Consultado abril 2019]. Disponible en: http://propuestastic.elarequi.com/propuestas-didacticas/eltrabajo-en-red-y-las-redes-sociales/el-uso-educativo-de-las-redes-sociales/

MERCHÁN, MARÍA. CyberbullyingObserver: Herramienta para la detección del ciberacoso en redes sociales utilizando técnicas Big Data.

España 2017.Disponible en: http://hdl.handle.net/10578/15445 Trabajo de investigación. Universidad de Castilla-La Mancha, 2017

BIBLIOGRAFÍA COMPLEMENTARIA

SGSI Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad [En línea]. [Consultado Julio 2019]. Disponible en: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

AVAST, Que es la ingeniería social [En línea]. [Consultado Julio 2019]. Disponible en: https://www.avast.com/es-es/c-social-engineering

Palabra de Hacker. (2017, marzo 24). Que es ingeniería social [Archivo de video]. Recuperado de: https://www.youtube.com/watch?v=PkuBzgW9sBw

La ingeniería social al servicio del cibercrimen [En línea]. [Consultado julio 2019]. Disponible en: https://computerworld.co/la-ingenieria-social-al-servicio-del-cibercrimen/

Clavijo, Ciro Antonio Dussan. "Políticas de seguridad informática." Entramado 2.1 (2006): 86-92.

Política de contraseñas y seguridad de la información. INTECO. [En línea] [Consultado 30 de noviembre de 2019]. Disponible en: https://www.unirioja.es/servicios/si/seguridad/difusion/politica_contrasenas.pdf

ANEXOS

Anexo A. Resumen analítico especializado R.A.E

Fecha de Realización: 12 de diciembre de 2019
Título: Técnicas de Ingeniería Social aplicada en los estudiantes de grado 11° de la ciudad de San Juan de Pasto
Autor: TAMAYO ARGOTI, Leydi Dayana
Palabras Claves: Ingeniería Social, seguridad informática, ciber-atacante, vulnerabilidad, phishing, delito informático, ataque, confidencialidad, integridad, disponibilidad.
Descripción: La Ingeniería Social, es un ataque cibernético en el cual se obtiene información confidencial o personal a través de la manipulación a la víctima mediante técnicas de persuasión y engaño, es una de las herramientas más utilizadas por los cyber delincuentes, ya que a través del tiempo debido a la evolución tecnológica se ha ido mejorando e incrementando el robo de información, es por ello que en este proyecto se presenta la problemática y el impacto de la ingeniería social en los estudiantes de grado 11° de la ciudad de San Juan de Pasto, mediante la identificación de vulnerabilidades de la seguridad de la información, realizando un estudio de las metodologías usadas de tal manera que se logre determinar los tipos de técnicas aplicables a través de Ingeniería social. Mediante el presente proyecto de grado se comprenden temáticas importantes como referencias históricas y relevantes de ataques informáticos, teniendo en cuenta conceptos de seguridad informática, técnicas de ataque, tipos de ataque, ciber atacantes o ciber-delincuentes, finalmente se realizarán recomendaciones de cómo evitar ser víctimas de este tipo de ataque y proteger la información adecuadamente.
Fuentes Destacadas: Tesis: MONTES. Carolina, VARGAS. Viviana. Problemas de ingeniería social y su impacto en la adolescencia colombiana. Bogotá, Dc, 2018, 57p. Trabajo de grado (Problemas de ingeniería social y su impacto en la adolescencia colombiana). Universidad Nacional abierta y a distancia. Facultad ciencias básicas tecnología e ingeniería. Especialización en seguridad informática. [En línea]. Fecha. [abril 2019]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/22583/1/41946700.pdf GARCÍA GUILABERT, Natalia. Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio. Murcia, España. 2014, 502p. Trabajo de grado (Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio). Universidad de Murcia [En línea]. Fecha. [abril 2019]. Disponible en: https://digitum.um.es/digitum/bitstream/10201/40868/1/Tesis%20Natalia_Garci

a_Guilabert_Victimización%20de%20menores%20por%20ciberacoso%20continuado.pdf

Tesis: MORALES.Rojas. Danyorsa.Mabel. Ciberacoso de niños, niñas y adolescentes en las redes sociales: Un estudio sobre los sistemas de protección y prevención judicial. Bogotá, Dc.2015 Trabajo de grado (Ciberacoso de niños, niñas y adolescentes en las redes sociales: Un estudio sobre los sistemas de protección y prevención judicial.) Universidad Católica de Colombia. Facultad de derecho. Disponible en: https://repository.ucatolica.edu.co/browse?type=author&value=Rojas+Morales%2C+Danyorsa+Mabel.

Tesis Ramírez Claudia, Collo Harold. Estudio de ingeniería social en el uso de redes sociales. Bogotá 2017 trabajo de grado (Estudio de ingeniería social en el uso de redes sociales). Universidad Nacional abierta y a distancia. Facultad ciencias básicas tecnología e ingeniería. Especialización en seguridad informática. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14505/1/17659358.pdf

ÁLZATE CASTAÑEDA, Cristian Camilo y GALEANO VILLA, Jorge Luis. Protocolo de Políticas de Seguridad Para las Universidades de Risaralda. Trabajo de grado Profesional en Ingeniero de Sistemas y Telecomunicaciones. Risaralda.: Universidad Católica de Risaralda. Facultad de ciencias básicas e ingeniería, 2013. 100 p. Disponible en: https://docplayer.es/5605322-Protocolo-de-politicas-de-seguridad-informatica-para-las-universidades-de-risaralda-jorge-luis-galeano-villa-cristian-camilo-alzate-castaneda.html

UNIR. “La Ingeniería Social, acercándonos a los molestos Spam, Phishing y Hoax”. TEMPERINE, Marcelo. Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. Buenos Aires, 2013, 12p. Trabajo de investigación (Doctorando en Derecho). Universidad Nacional del Litoral. Facultad de Ciencias Jurídicas y Sociales. Argentina.

SÁNCHEZ ARTEAGA, Juan Miguel. Estudio y análisis del uso de las redes sociales en la ciudad de Cuenca y elaboración de un manual de buenas prácticas de usuario. Cuenca, 2011, 140p. Trabajo de investigación (Ingeniero en sistemas). Universidad Politécnica Salesiana. Facultad de educación. Cuenca.

Caviativa Patricia, Jaramillo, Valentino. “Prevención de acoso en aulas y ciberacoso en la educación superior a través de recursos educativos digitales abiertos”. Trabajo de grado España 2018.Universidad de Alicante Disponible en: http://hdl.handle.net/10045/84896

GARCIA ROMERO, JOAN ENRIC. Estudio de metodologías de ingeniería social. Trabajo de grado España 2019. Universitat Oberta de Catalunya http://hdl.handle.net/10609/89045

LÓPEZ, CARLOS, Ingeniería social: el ataque silencioso. El salvador 2015. editor: El Salvador, North América: ITCA, Editores, 2015. Escuela Especializada en Ingeniería. Disponible en http://hdl.handle.net/10972/2910

MÉNDEZ, ALEJANDRO, Estudio de metodologías de ingeniería social España 2018.Universitat Oberta de Catalunya. Disponible en: http://hdl.handle.net/10609/90305

ICONTEC INTERNATIONAL. NORMA TÉCNICA COLOMBIANA - NTC 1486. [En línea]. [Consultado abril 2019]. Disponible en: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_g ene ral/09062014/n_icontec.pdf

GONZÁLEZ AGUDELO, Daniel. El riesgo y la faculta de políticas de seguridad informática una amenaza en las empresas certificadas. Bogotá, 2014, 22p. Trabajo de investigación (administración de la seguridad y salud ocupacional). Universidad Militar Nueva Granada. Facultad de relaciones internacionales, estrategia y seguridad. Cundinamarca.

GUERRERO, David. MONCAYO, Laura. PARRA, Juanita. Tesis de Grado [En línea]. [Consultado mayo 2019]. Disponible en: 2015. http://www.institutomerani.edu.co/publicaciones/tesis/2015/cyberbullying%20_ acos o_escolar_era%20virtual.pdf.

URRUTIA, José. HERNÁNDEZ, Geovanna. Ingeniería social a través de medios informáticos, análisis de las posibles amenazas existentes en la facultad de ciencias administrativas de la universidad de Guayaquil. Guayaquil, 2015. Universidad de Guayaquil. Ecuador.

FORMATO - NTC 1486. [En línea]. [Consultado abril 2019]. Disponible en: https://sig.unad.edu.co/LEGUIZAMON, Mayra. EL PHISHING. España, 2014, 47p. TRABAJO FINAL DE GRADO (GRADO EN CRIMINOLOGIA Y SEGURIDAD). Universidad Jaime I. España CASTRO, FRANCISCO. MIRÓ, FERNANDO. ¿Nos parecen más inseguros los ciberlugares después de un ciberataque? España, 2018 Ministerio de Economía y Competitividad, Gobierno de España. [En línea] mayo 2019 [Consultado abril 2019]. Disponible en: http://www.ehu.eus/ojs/index.php/inecs/article/view/19689.

Contenido del documento: El desarrollo del presente trabajo de grado consta de:

FORMULACIÓN DEL PROBLEMA.

¿Qué hábitos de seguridad de la información se deben tener en cuenta para minimizar las vulnerabilidades ante ataques mediante ingeniería social a los estudiantes de grado 11° de la ciudad de San Juan de Pasto?

Objetivo General.

Investigar sobre los métodos aplicados a la ingeniería social utilizados en la red que permitan mitigar el riesgo de vulnerabilidades y fallas de la seguridad de la información mediante el uso de internet en los estudiantes de grado 11° de la ciudad de San Juan de Pasto.

Objetivos Específicos

- Indagar sobre las técnicas de ingeniería social y como se aplican, para identificar los riesgos ante el uso de la red por parte de los estudiantes de grado 11° de la ciudad de San Juan de Pasto.
- Determinar metodologías de ingeniería social para aplicar a los estudiantes de grado 11° en algunos colegios de la ciudad de San Juan de Pasto.
- Analizar los resultados obtenidos ante los ataques informáticos presentados por el uso inadecuado de datos personales por parte de los estudiantes de grado 11° de la ciudad de San Juan de Pasto.

Marco Referencial: El cual se divide en: Marco de Contexto, Marco teórico, Marco conceptual y Marco histórico.

Diseño Metodológico: Fase que permite recopilar la información necesaria para el desarrollo del proyecto, en esta etapa se encuentra el tipo y la línea de investigación, el instrumento de recolección de información, población, muestra y metodología de desarrollo.

Desarrollo del proyecto: Fase que permite realizar el desarrollo del proyecto según los objetivos planteados, se divide en: Análisis de la situación actual, Activos de información, Declaración de aplicabilidad, Políticas de Seguridad.

Resultados: Fase que permite obtener los resultados de acuerdo al desarrollo del proyecto.

Divulgación: Manera en que se realizará la divulgación del proyecto de grado.

Conclusiones.

Bibliografía e infografía, Anexos

Metodología: Monografía

Conceptos nuevos: Grooming, Phishing, Sexting.

Conclusiones:

- Mediante la presente investigación, se logró identificar que el nivel de vulnerabilidad es bastante alto, dado que la información compartida es fácil de capturar por los escasos conocimientos que presentan los estudiantes en cuanto a seguridad de información, esto se evidencio durante la aplicación de la encuesta.
- Se descubrieron bastantes vulnerabilidades a través de los resultados de la encuesta, dado que no existe un método de capacitación que permita a los estudiantes obtener los conocimientos necesarios en seguridad informática, dado lo anterior se debe tener en cuenta que tanto padres de familia como docentes se comprometan en sensibilizar a los jóvenes en la aplicación de buenas prácticas y políticas de seguridad que permitan gozar de beneficios sin comprometer información personal o confidencial.
- La ingeniería social es un método de ataque cibernético que afecta a las personas más vulnerables, para evitar esta situación, es necesario gestionar la información a través de los diferentes métodos de comunicación y redes

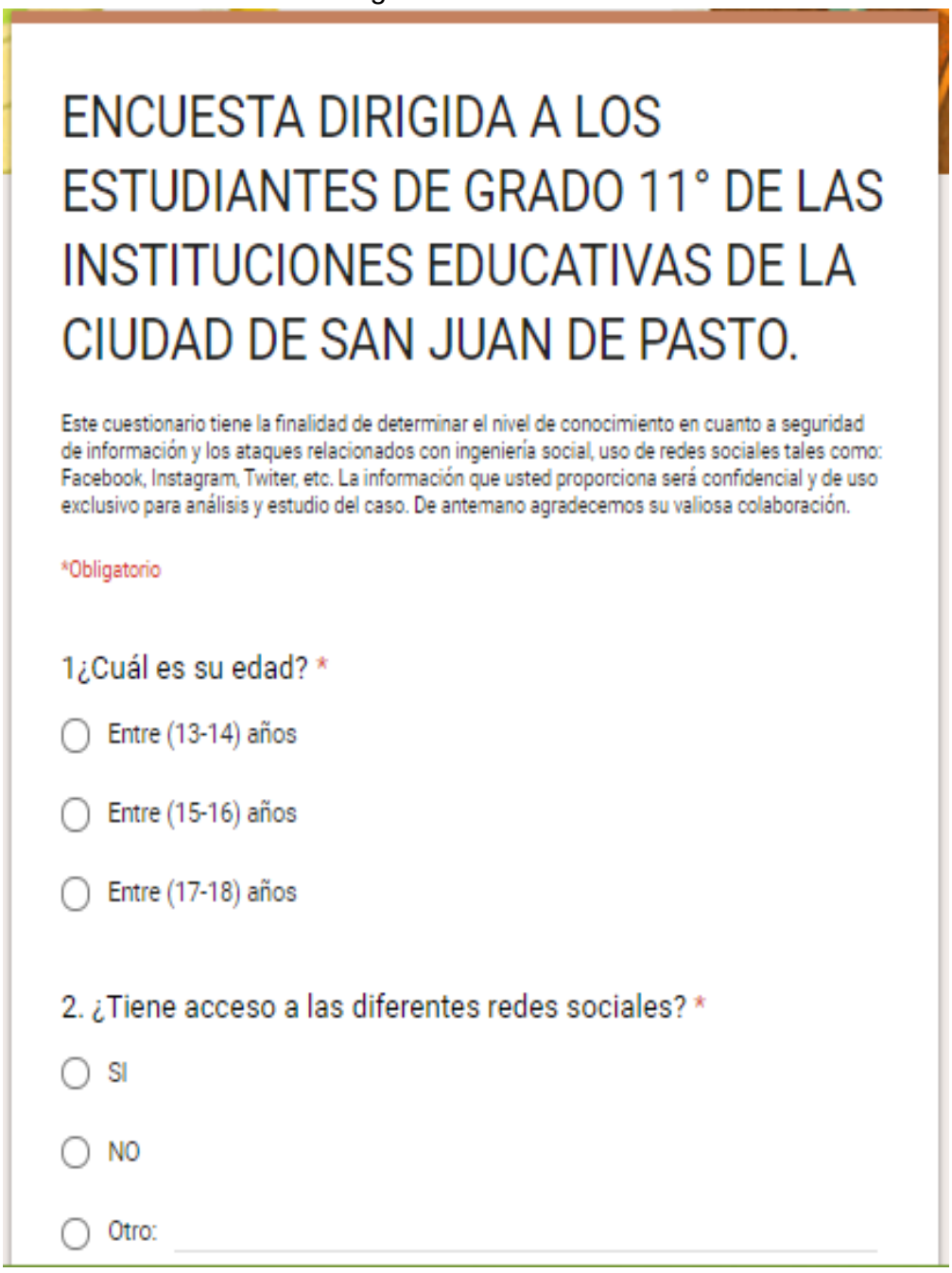
sociales para procesar adecuadamente la información para evitar y prevenir futuros ataques.

- Según el análisis realizado a los estudios y antecedentes encontrados durante esta investigación, se identificó que los adolescentes son los más vulnerables ante ataques de ingeniería social, teniendo en cuenta que a través del tiempo se han venido empleando nuevas técnicas de ataques, los cuales podrían ser evitadas si existe un acompañamiento de los padres o docentes.
- Con los resultados obtenidos en las encuestas se deduce que los estudiantes no protegen su información, exponiendo sus datos para que puedan ser robados por ciberdelincuentes, debido a que, un 73% acepta cualquier tipo de invitación y busca personas no conocidas en las redes, un 67% de los estudiantes no revisa las condiciones y alertas de las aplicaciones, un 53% no posee antivirus en sus equipos, un 60% no posee contraseñas seguras, un 60% utilizan las mismas credenciales de acceso para todos los sitios y un 67% no cambia sus claves de ingreso.

AUTOR: LEYDI DAYANA TAMAYO ARGOTI

Anexo B. Encuesta dirigida a los estudiantes de grado 11° de las instituciones educativas de la ciudad de San Juan de Pasto.

Figura 19.Encuesta



ENCUESTA DIRIGIDA A LOS ESTUDIANTES DE GRADO 11° DE LAS INSTITUCIONES EDUCATIVAS DE LA CIUDAD DE SAN JUAN DE PASTO.

Este cuestionario tiene la finalidad de determinar el nivel de conocimiento en cuanto a seguridad de información y los ataques relacionados con ingeniería social, uso de redes sociales tales como: Facebook, Instagram, Twiter, etc. La información que usted proporciona será confidencial y de uso exclusivo para análisis y estudio del caso. De antemano agradecemos su valiosa colaboración.

*Obligatorio

1¿Cuál es su edad? *

- Entre (13-14) años
- Entre (15-16) años
- Entre (17-18) años

2. ¿Tiene acceso a las diferentes redes sociales? *

- SI
- NO
- Otro:

3.¿Qué información tiene visible en su perfil de redes sociales? *

- [ ] Fotos
- [ ] Videos
- [ ] Lugar donde vive
- [ ] Lugar donde estudia
- [ ] Número telefónico
- [ ] Otro
- [ ] Otro: _____

4.¿Qué criterio utiliza para agregar personas a su lista de amigos en redes sociales? *

- [ ] Agrega cualquier contacto que le mande una invitación
- [ ] Busca contactos que no conoce para hacer nuevos amigos
- [ ] Agrega solo personas conocidas
- [ ] Otra
- [ ] Otro:

5.¿Revisa las condiciones o alertas que se muestran acerca de los permisos que se da a la aplicación para poder utilizar su información y fotos?

- ( ) SI
- ( ) NO

6. ¿Conoce usted que es la ingeniería social? *

- ◯ SI
- ◯ NO

7.¿Ha recibido usted llamadas, mensajes de texto, e-mails, chats mediante los cuales le soliciten datos personales o confidenciales? *

- ◯ SI
- ◯ NO

8. ¿Ha recibido capacitación acerca de seguridad de la información o como protegerse ante ataques informáticos? *

- ◯ SI
- ◯ NO

9. ¿Qué factores cree usted que ponen en peligro la información que comparte en internet? *

- ☐ Virus
- ☐ Fallas en los sistemas
- ☐ Perdida de clave o contraseña
- ☐ Spam

10.¿Usted ha sido víctima de ataques informáticos en los que tenga que ver robo de su información personal o divulgación de información que comprometa su integridad?

- ◯ SI
- ◯ NO

11.¿Qué medios de comunicación piensa usted que pueden influir en la seguridad de su información? *

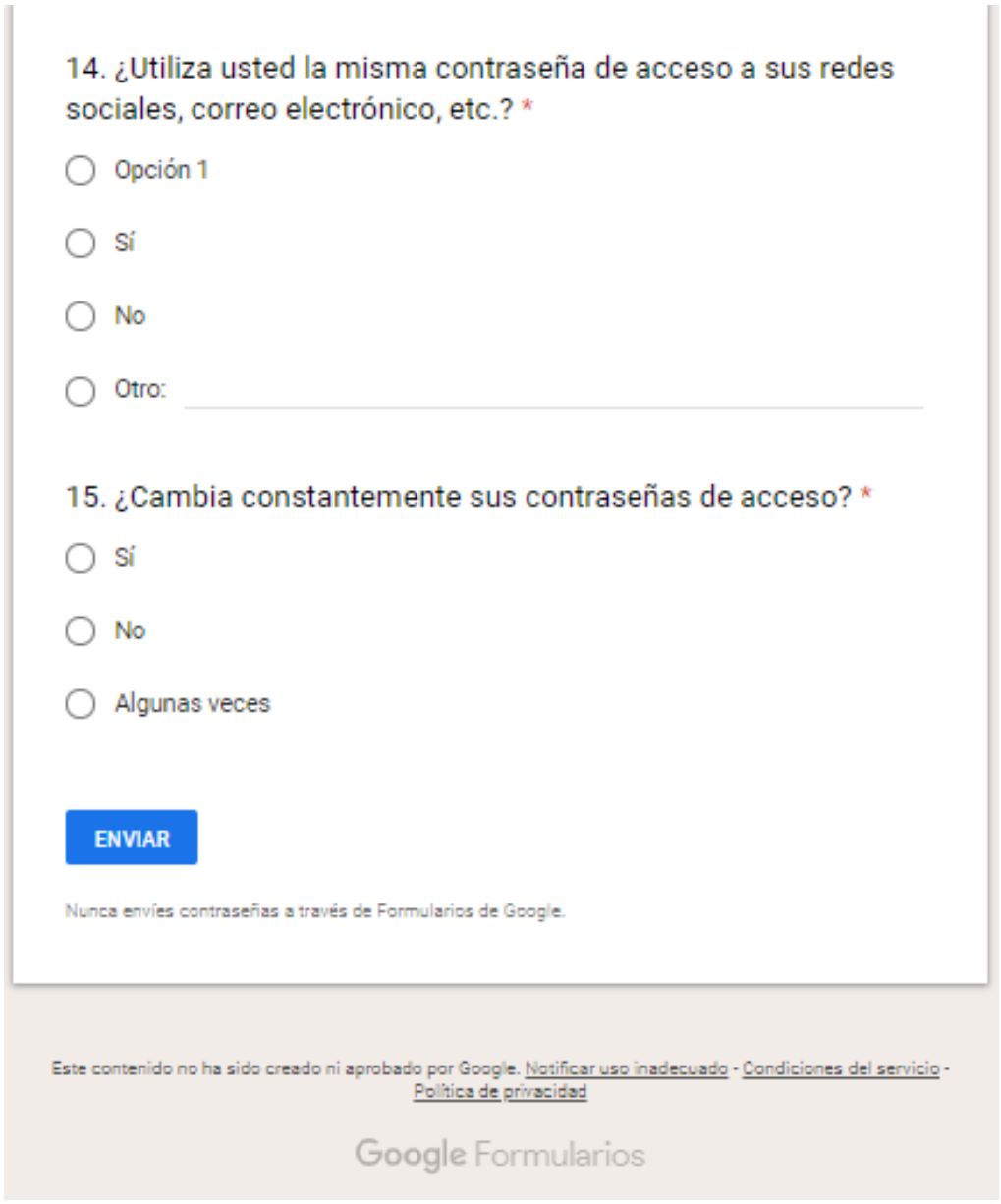
- ☐ Chat
- ☐ Email
- ☐ Descargas
- ☐ Enlaces web de sitios desconocidos

12. ¿Los equipos a los que se conecta cuentan con protección como antivirus o antispyware actualizados? *

- ◯ SI
- ◯ NO

13. ¿La contraseña de acceso a sus redes sociales, correo electrónico, etc. es segura?, es decir cuenta con caracteres especiales, combinación de mayúsculas y minúsculas y números? *

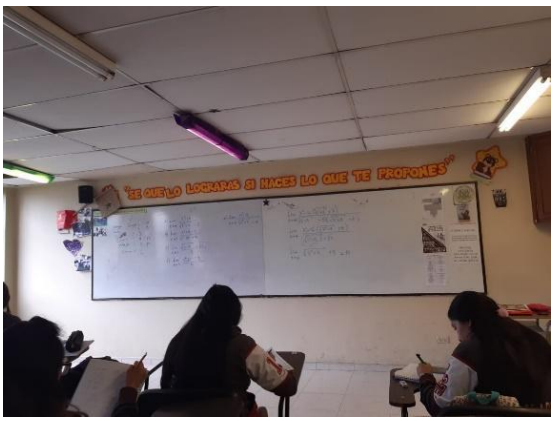
- ◯ SI
- ◯ NO



Fuente: Elaboración propia.

Anexo C. Evidencias Fotográficas diligenciamiento de encuesta.

Figura 20.Registro fotográfico diligenciamiento de encuesta



Fuente: Elaboración propia.