UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
Ingeniero de Sistemas

TEMA:

ANÁLISIS Y EVALUACIÓN DEL IMPACTO DE LOS CIBERATAQUES EN ADOLESCENTES DE 12 A 17 AÑOS DE LA CIUDAD DE QUITO UTILIZANDO HERRAMIENTAS OPEN SOURCE EN ESCENARIOS VIRTUALES CONTROLADOS Y PLANTEAR UN PROTOCOLO PARA LA MITIGACIÓN A LOS CIBERATAQUES

AUTOR:
WILLIAM XAVIER TORRES SARANGO

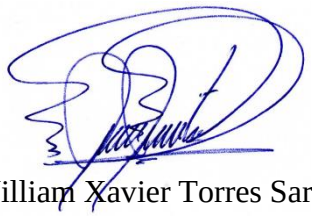
TUTOR:
DANIEL GIOVANNY DÍAZ ORTIZ

Quito, julio de 2021

CESIÓN DE DERECHOS DE AUTOR

Yo William Xavier Torres Sarango con documento de identificación No. 1712733235, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de titulación intitulado: ANÁLISIS Y EVALUACIÓN DEL IMPACTO DE LOS CIBERATAQUES EN ADOLESCENTES DE 12 A 17 AÑOS DE LA CIUDAD DE QUITO UTILIZANDO HERRAMIENTAS OPEN SOURCE EN ESCENARIOS VIRTUALES CONTROLADOS Y PLANTEAR UN PROTOCOLO PARA LA MITIGACIÓN A LOS CIBERATAQUES, mismo que ha sido desarrollado para optar por el título de INGENIERO DE SISTEMAS en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato digital a la Bilbioteca de la Universidad Politécnica Salesiana.



William Xavier Torres Sarango
C.I: 1712733235

Quito, julio de 2021

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR/A

Yo declaro que bajo mi dirección y asesoría fue desarrollado el Artículo Académico, con el tema: ANÁLISIS Y EVALUACIÓN DEL IMPACTO DE LOS CIBERATAQUES EN ADOLESCENTES DE 12 A 17 AÑOS DE LA CIUDAD DE QUITO UTILIZANDO HERRAMIENTAS OPEN SOURCE EN ESCENARIOS VIRTUALES CONTROLADOS Y PLANTEAR UN PROTOCOLO PARA LA MITIGACIÓN A LOS CIBERATAQUES, realizado por William Xavier Torres Sarango, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerado como trabajo final de titulación.

Daniel Giovanny Díaz Ortiz
C.I: 1716975501

Quito, julio de 2021

DEDICATORIA

Este trabajo elaborado después de mucho tiempo, debido a los grandes impedimentos que se me han presentado a nivel personal; por fin llegaron a un final e inicio de nuevas metas por cumplir. Está enfocado a un tema que me apasiona y con el cual espero seguir contribuyendo para ayudar a la sociedad.

Está dedicado para mis padres, que pese a las adversidades y acompañamiento en los momentos más complicados de mi vida personal, laboral y económico, supieron brindarme su apoyo, cariño, cuidados, alimentación y un techo. Les agradezco por sembrar en mi vida valores que me han permitido llegar a muchos logros, inclusive sin contar con tan anhelado título universitario.

A mis hermanos, que pese a encontrarnos distanciados geográficamente, siempre estamos unidos por la fuerza del corazón y de nuestros pensamientos.

A mis sobrinos, que los adoro con mi alma, pese a que ya se encuentran en una etapa de adultez, siempre serán mis niños queridos.

William Xavier Torres Sarango

AGRADECIMIENTO

Agradezco a los docentes de la Universidad Politécnica Salesiana, que a lo largo de mi vida académica muchos supieron brindar su amistad más que una docencia. A mi tutor Daniel Giovanny Díaz Ortiz, que pese a la complicación de nuestros horarios supo brindarme el tiempo adecuado para sacar adelante este proyecto. Un agradecimiento especial para el Ingeniero Franklin Hurtado, quien supo escucharme y me guió de la mejor manera previo a la elaboración de mi trabajo de titulación. A la Ingeniera Patsy Prieto, que con un corazón blando, supo brindarme la oportunidad, para terminar este proceso después de varios años de mi ausencia académica.

William Xavier Torres Sarango

ANÁLISIS Y EVALUACIÓN DEL IMPACTO DE LOS CIBERATAQUES EN ADOLESCENTES DE 12 A 17 AÑOS DE LA CIUDAD DE QUITO UTILIZANDO HERRAMIENTAS OPEN SOURCE EN ESCENARIOS VIRTUALES CONTROLADOS Y PLANTEAR UN PROTOCOLO PARA LA MITIGACIÓN A LOS CIBERATAQUES

ANALISIS AND EVALUATION OF THE IMPACT OF CIBERATTACKS ON ADOLESCENTS BETWEEN 12 AND 17 YEARS OLD IN THE CITY OF QUITO USING OPEN SOURCE TOOLS IN CONTROLED VIRTUAL SCENARIOS AND PROPOSE A PROTOCOL FOR THE CIBERATTACKS MITIGATION

William Torres[1], Daniel Díaz[2]

Resumen

El presente documento, consiste en analizar el impacto de los ciberataques en adolescentes de 12 a 17 años de la ciudad de Quito. Para ello, se utilizará diferentes herramientas de uso libre conocidas como Open Source, dentro de un ambiente controlado. Para el levantamiento de información requerida dentro del estudio, se realiza una encuesta utilizando medios tecnológicos por flexibilidad, rapidez en la obtención de resultados y por la facilidad de uso. Se propone realizar el laboratorio con una cuenta de correo y una cuenta de usuario ficticia creada en una red social, que permita desarrollar cada uno de los pasos que realizan los ciberatacantes para robar datos de posibles víctimas. Basados en los artículos 178, 180 y 212, páginas 29, 30 y 34 del COIP. De esta manera, se evitará fuga de información y no se vulnerarán los derechos de los adolescentes encuestados. Posterior a ello, con los resultados, el análisis y tabulación de la

Abstract

This document consists of analyzing the impact the cyberattacks on adolescents between 12 and 17 years old in the city of Quito. For this, different free-use tools known as Open Source will be used within a controlled environment. To collect the information required within the study, a survey is carried out using technological means due to flexibility, speed in obtaining results and ease of use. It is proposed to carry out the laboratory with an email account and a fictitious user account created in a social network, which allows the development of each of the steps that cyber attackers take to steal data from possible victims. Based on articles 178,180 and 212, pages 29, 30 and 34 of the COIP. In this way, information leakage will be avoided, and the rights of the adolescents surveyed will not be violated. After that, with the results, the analysis, and tabulation of the information collected in the survey of adolescents, it is

[1]Estudiante de Ingeniería de Sistemas, Universidad Politécnica Salesiana, Egresado – UPS - Sede Quito. Autor para Correspondencia: wtorres@est.ups.edu.ec

[2] Magister en Redes de Comunicaciones, Ingeniero de Sistemas, Docente de la Carrera de Ingeniería de Sistemas, Universidad Politécnica Salesiana, UPS - Sede Quito.

Email: ddiaz@ups.edu.ec

información recolectada en la encuesta a los adolescentes, se propone diseñar e implementar un protocolo para la mitigación ante posibles ciberataques. El mismo que será dividido en diferentes guías; dos de estos documentos serán dirigidos para la sociedad en general y personas involucradas en la protección a adolescentes; y los otros dos documentos están dirigidos para el personal de TIC´s de instituciones educativas, para su respectivo análisis e implementación de protocolos.

Palabras Clave: ciberataque, Open Source, COIP, protocolo.

proposed to design and implement a protocol for mitigating possible cyberattacks. The same one that will be divided into different guides; two of these documents will be directed to general society and people involved in the protection of adolescents; and the other two proposed documents are aimed at the ICT staff of educational institutions, for their respective analysis and implementation of protocols.

Keywords: cyberattack, Open Source, COIP, protocol

1. Introducción

Actualmente, existen amenazas dentro de redes sociales, blogs, publicidad en páginas web, video juegos en red, etc.

Uno de los mayores delitos que genera preocupación a nivel mundial y que ha dejado consecuencias devastadoras es el conocido Grooming; esta es una práctica que se lleva a cabo mediante el engaño a niñas, niños y adolescentes, con la finalidad de preparar el terreno para cometer abusos sexuales [1]; constituyéndose en un daño irreversible para la víctima y sus familiares.

En Ecuador el Reglamento a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos (Decreto No. 3496 – Gustavo Noboa Bejarano, Presidente constitucional de la república del Ecuador), expedida en el año 2002, hace referencia a la "protección de datos" en su artículo 9. En el mismo se establece que, "para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros" [2].

"La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución. La obtención de información sobre datos personales sin autorización puede ser sancionada con pena de prisión de dos meses a dos años y multa de USD 2 000" [2].

Pese a existir en la ley una mención a la protección de datos personales dentro de la legislación ecuatoriana, la necesidad de un artículo que reflexione en torno al uso de los datos personales en la Web se hace cada día más evidente. La aprobación de este proyecto de Ley implicaría que Ecuador deje de ser, junto con Bolivia y Venezuela, uno de los países que no cuentan con legislación específica en relación con la ciberseguridad.

De acuerdo a un estudio realizado por ChildFund Ecuador, entre 2017 y 2019 Ecuador registró 169 casos de abuso sexual en medios digitales a niños y niñas, estudios revelan que se denuncian solo 1 de cada 10 agresiones [3].

De acuerdo a Global Cybersecurity Index (GCI 2018), en la Figura 1, se puede notar el ranking en Sudamérica sobre la inseguridad cibernética

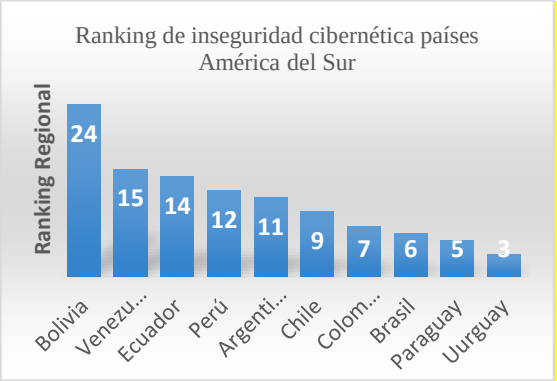


Figura 1. Ranking de ciberseguridad países América del Sur.

Donde, Ecuador ocupa el tercer lugar dentro de los países sudamericanos más inseguros frente a ciberataques [4].

Los ciberataques pueden generar consecuencias como: depresión, aislamiento social, baja autoestima, presión social, y hasta suicidio.

Las y los adolescentes, al ser un grupo de atención prioritaria, requiere de una atención especial y sobre todo de mayor observación y protección [5]; "se deben plantear medidas de prevención, intervención y sanción a los actos que afecten la integridad de las y los menores de edad. Las niñas, niños y adolescentes son susceptibles al engaño de cualquier adulto por no contar con la madurez adecuada, a diferencia de personas mayores de edad; por tanto, el uso indebido del Internet y las redes sociales podrían conllevar al peligro y que se atente contra su vida, libertad, integridad física, psíquica, moral y sexual" [5].

De acuerdo al Acuerdo Ministerial No. 029 del Ministerio de Inclusión Económica y Social del 03 de agosto de 2018; la Carta Magna, en su artículo 44, establece que: "El Estado, la sociedad y la familia promoverán de forma prioritaria el desarrollo integral de las

niñas, niños y adolescentes, y asegurarán el ejercicio pleno de sus derechos; se atenderá al principio de su interés superior y sus derechos prevalecerán sobre los de las demás personas. Las niñas, niños y adolescentes tendrán derecho a su desarrollo integral, entendido como proceso de crecimiento, maduración y despliegue de su intelecto y de sus capacidades, potencialidades y aspiraciones, en un entorno familiar, escolar, social y comunitario de afectividad y seguridad. Este entorno permitirá la satisfacción de sus necesidades sociales, afectivo-emocionales y culturales, con el apoyo de políticas intersectoriales nacionales y locales" [6].

Gran parte de los estudios estadísticos, no dan cuenta de mediciones para grupos menores de 15 años, lo cual provoca cierta incertidumbre frente al uso de las tecnologías digitales en adolescentes.

Según UNICEF (2015), un tercio de adolescentes en el mundo usa Internet durante dos o tres horas al día, un 14% lo utiliza más de 8 horas diarias.

De acuerdo a la ONU y la Fundación Telefónica, el 55% de los adolescentes latinoamericanos han sido víctimas de ciberacoso.

Ante esta problemática, el 06 de marzo de 2020, en Ecuador se firma un compromiso entre: el Consejo Nacional para la Igualdad Intergeneracional (CNII), la Dirección Nacional de Registro de Datos Públicos (Dinardap), el Ministerio de Educación, ChildFund, la Asociación Ecuatoriana de Ciberseguridad. Además, forma parte de este compromiso el Instituto Interamericano del Niño, la Niña y Adolescentes (IIN), y la Organización de Estados Americanos (OEA) para trabajar conjuntamente en diferentes mecanismos, que permitan al Ecuador contar con una Internet segura para niñas, niños y adolescentes.

El acuerdo contempla la creación de una red intergeneracional para desarrollar protocolos, mapas de riesgos y un manual de uso seguro de la Internet.

La red de trabajo actuará sobre aspectos que permitan abordar el ámbito familiar, sistema educativo y comunidad, para apoyar a los menores en el aprendizaje de mecanismos de autocuidado y acompañamiento de un adulto responsable.

Posteriormente, Ecuador generó un primer documento de Política Pública de Internet Segura, desarrollado y difundido el 24 de septiembre del 2020.

Pero, a la fecha del inicio de este estudio no existe seguimiento al documento de Política Pública de Internet Segura [7], la misma que no cuenta con análisis técnicos tecnológicos y tampoco cuenta con protocolos definidos para mitigar problemas que generan los ciberataques a niñas, niños y adolescentes.

En el Ecuador, según el INEC, "1 de cada 2 niños, niñas y adolescentes usan computadora; por eso, es indispensable mantenerse informado y contar con mecanismos para anticiparse y prevenir los riesgos que representa la red y su mal uso".

Actualmente, se puede evidenciar que las nuevas generaciones, llamados "nativos digitales", pasan gran parte de su día en las redes sociales y usando tecnología; y no son conscientes de los riesgos que conlleva compartir y publicar información (fotos, videos, datos) en línea, ya sea utilizando herramientas sociales o utilizando redes Wifi gratuitas.

De acuerdo al sitio Web Internet Segura del Gobierno Nacional del Ecuador, el porcentaje de personas que usan Internet para el año 2019 fue de 59,2%, personas que utilizan un teléfono inteligente 76,8% y el analfabetismo digital es del 11,4% [8].

La UNESCO también advierte sobre los potenciales efectos negativos sobre el bienestar y la salud que produce el ciberacoso en los estudiantes. Según los datos de 7 países europeos, la proporción de niños entre 11 y 16 años que fueron víctimas de ciberacoso aumentó del 7% al 12% entre 2010 al 2014 [9].

Entre los principales usos de Internet en la región destacan las redes sociales que alcanzan

el 96% de los usuarios, frente al 81% a nivel internacional [10]. Así se muestra en la Figura 2.

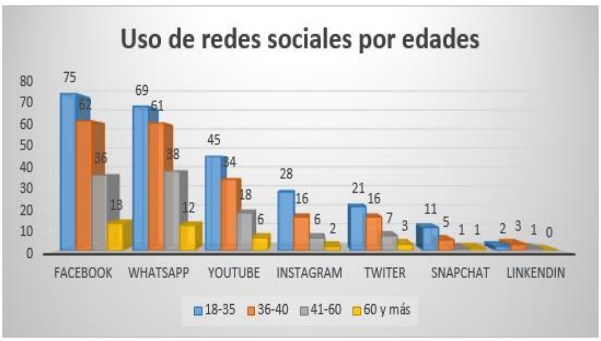


Figura 2. Latinobarómetro 2016 (en OEA –IIN. 2018).
Re-elaboración: CNII. 2020

Debido a que la ciberseguridad es un tema nuevo dentro del Ecuador, y especialmente en el campo de políticas públicas, se ha optado en tomar como herramienta de estudio y de impulso al documento "Política pública por una internet segura para niños, niñas y adolescentes". Basados en estos análisis y resultados, se cumplirá dos de los objetivos planteados para este estudio, los cuales son: **Analizar el nivel de exposición de los adolescentes de 12 a 17 años de la ciudad de Quito ante posibles ciberataques** y **Diseñar e implementar un protocolo para la mitigación ante posibles ciberataques.**

2. Métodos y materiales

Se debe mencionar que existen diferentes enfoques dentro de este proyecto, así se tiene: social, académico, técnico, investigativo y cuantitativo; para lo cual se utilizará diferentes metodologías según corresponda.

2.1. Metodología descriptiva

Se utilizará la técnica cuantitativa o de encuestas, con el fin de conocer ¿cuántos adolescentes entre 12 y 17 años de la ciudad de Quito se conectan actualmente a Internet?, ¿cuántos adolescentes cuentan con redes sociales?, ¿cuántos adolescentes han sido víctimas de algún tipo de ciberataque?, ¿cuántas horas del día dedican a la navegación por Internet?, ¿qué tipo de redes sociales visitan?, ¿qué buscan en Internet?

La información recolectada en la encuesta, es de manera general, para entender ciertos riesgos y vulnerabilidades a los que se encuentran expuestos las y los adolescentes de la ciudad de Quito.

Las preguntas están divididas en cuatro partes para no mezclar términos. La que se encuentra estructurada de la siguiente manera: Datos del encuestado, Internet, redes sociales, ciberataque.

La intención de esta encuesta es recolectar la mayor cantidad de información posible, sin invadir la privacidad de los adolescentes; que permita analizar la problemática actual de los ciberataques y, asimismo, que permita desarrollar un laboratorio controlado para la comprobación del mismo.

Las preguntas son cerradas y con opciones de SI o NO, salvo alguna excepción que puede ser más amplia; lo que se pretende es contar con un rápido procesamiento de datos.

2.2. Recolección de datos y análisis de la información.

Se identificará el grado de conocimiento, los riesgos e impactos a adolescentes indistintamente de alguna institución educativa y se procederá a identificar a aquellos que han sufrido de algún ciberataque, con la finalidad de elaborar un documento con los protocolos más adecuados para su respectiva mitigación.

Basados en los artículos 178, 180 y 212 del Código Orgánico Integral Penal, Registro Oficial No. 180 del 10 de febrero del año 2014, páginas 31 y 35; al tratarse el estudio sobre el impacto de los ciberataques en adolescentes de 12 a 17 años de edad de la ciudad de Quito, no se utilizará ninguna información personal que pueda afectar la integridad de los adolescentes encuestados; para solucionar este inconveniente técnicamente hablando, se procederá a crear una cuenta de correo y un perfil de usuario dentro de una red social, con el fin de demostrar posteriormente la forma de actuar por parte de los ciberatacantes.

2.3. Estimación de población futura [11]

Actualmente gracias al INEC (Instituto Nacional de Estadística y Censos), se ha logrado obtener los datos de los censos de los años 1990, 2001 y 2010 de la ciudad de Quito por edades y sexo; por lo tanto, se procederá a obtener el número de adolescentes dentro del rango de edad requerido y con ello la proyección de adolescentes entre 12 y 17 años para el año 2021.

Existen diferentes métodos de cálculo; por lo que, se procederá a realizar el cálculo con 3 metodologías diferentes como son:

- Método aritmético

$$Pf = Po + Ka * (tf - to) \quad (1)$$

- Método geométrico

$$Pf = Po * (1 + r)^{\Delta t} \quad (2)$$

- Método parabólico

$$Pf = A + B\Delta t + C\Delta t^2 \quad (3)$$

Con los resultados obtenidos, se calculará el promedio entre los que sean similares. En caso de no ser similar un valor, se procederá a descartar el resultado y no se tomará en cuenta para el cálculo del promedio. De esta manera se intenta minimizar posibles errores.

Tabla 1. Número de estudiantes entre 12 y 17 años de la ciudad de Quito

Ubicación geográfica	Año de censo	Número de habitantes (adolescentes)
Quito	1990	138914
	2001	164567
	2010	171284
	2021	189645

Debido a que el objeto de estudio son los adolescentes de la ciudad de Quito, no se toma en cuenta a adolescentes que en realidad no residen en la ciudad o que se encuentran de visita; es decir, a turistas.

2.4. Cálculo de la muestra poblacional [12]

Una vez que se ha realizado el cálculo de población futura de los adolescentes de 12 a 17 años de la ciudad de Quito, se procede a utilizar la fórmula de la muestra:

$$n = \frac{k^2 * p * q * N}{(e^2 * (N - 1)) + k^2 * p * q} \quad (4)$$

Donde las variables representan lo siguiente:

- N = Población
- k = 1,96 constante que representa el nivel de confianza.
- p = 0,5 valor estimado de la proporción de la muestra (probabilidad de éxitos).
- q = 0,5 probabilidad de fracaso
- e = 5% error de estimación.

2.3 Materiales utilizados

Herramientas de software para generar ciberataques:

- Sistema Operativo Kali Linux 2020
- Herramienta de Análisis de aplicaciones Web OWASP ZAP
- Herramientas de ingeniería social (Setoolkit – Social Engineering Toolkit), "es un framework de código abierto para realizar pentesting enfocado en ataques de Ingeniería Social" [13].
- Webmail, como servidor de correo electrónico, desde donde se realizará el envío del phishing. Este mismo servidor servirá para configurar un dominio para suplantar identidad.
- Servicio de correo Gmail, donde se encuentra la cuenta de la víctima
- Hydra de Kali Linux, es una herramienta de auditoría open source. El ataque que realiza es más conocido como ataque de fuerza bruta.
- The Hardvester, es una herramienta open source que permite obtener información en fuentes abiertas [14].
- Herramienta TinyURL, permite enmascarar un dominio o dirección IP.

3. Resultados y discusión

Se procede a realizar el cálculo de proyección futura utilizando los siguientes métodos: Aritmético, geométrico y parabólico; después

de los cálculos respectivos se logra obtener el siguiente resultado:

Pf = 189 645 habitantes (adolescentes de 12 a 17 años) proyectado para el año 2021.

Donde, Pf = Población futura.

Utilizando la fórmula de la muestra, se procede a realizar el respectivo cálculo, obteniendo así el valor o número de habitantes (estudiantes) que deben ser encuestados, para cumplir el objetivo; siendo n = 383 habitantes (estudiantes).

Paralelamente se desarrolla con la herramienta de formularios de Google un formato tipo encuesta. La misma que se encuentra ubicada en el siguiente link: https://docs.google.com/forms/d/1axiJ3OFD7H8BhvzOtSurKxOYINXC9p16DzipbZgvDec/edit .

La encuesta se llegó a realizar a 902 estudiantes de secundaria, así se puede observar en la Figura 3.

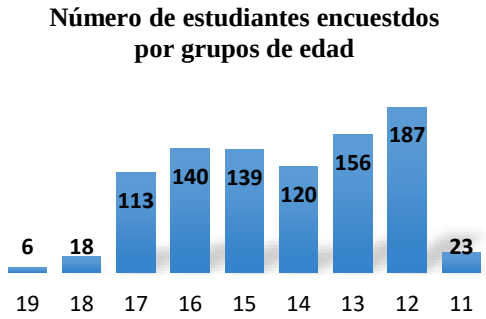


Figura 3. Número de estudiantes encuestados por grupos de edad

De la información recolectada, se puede observar que existen alumnos mayores de edad; por ejemplo: se tiene 6 alumnos cuya edad es de 19 años, 18 alumnos con 18 años de edad y 113 alumnos nacidos en el año 2003 con 18 años de edad. De igual manera, se observa que existe un grupo de 23 estudiantes que tienen 11 años de edad. Estos grupos no serán tomados en cuenta, porque el análisis de ciberataques está enfocado a adolescentes de 12 a 17 años. Por tanto, el total de la muestra de adolescentes que van a servir como objeto de estudio suman 855, distribuidos como se muestra en la Tabla 2.

Tabla 2. Número de adolescentes agrupado por año de nacimiento

Número de alumnos	Año de nacimiento	Edad (años)
113	2003	17
140	2004	16
139	2005	15
120	2006	14
156	2007	13
187	2008	12

Con base a los datos obtenidos en el registro de la encuesta, se puede observar que se supera el tamaño de la muestra requerido en un 223%; logrando así, que el margen de error disminuya.

De acuerdo a los resultados obtenidos, se obtiene que el 48% son de sexo femenino y el 52% son de sexo masculino; así se puede observar en la Figura 4.

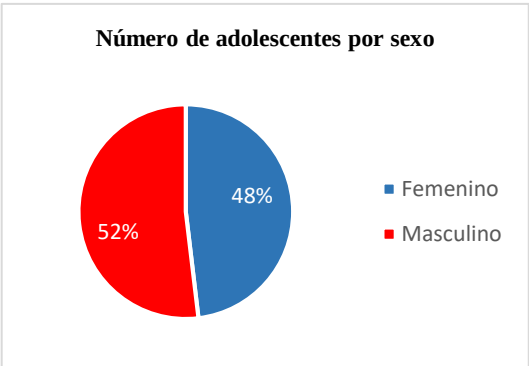


Figura 4. Número de adolescentes por sexo

De la muestra de 902 estudiantes, se puede observar que el 97% de estudiantes si tienen servicio de Internet en casa, mientras que el 3% no cuenta con servicio mencionado en casa. Es decir, existe la posibilidad de que el 97% sea más vulnerable a recibir algún tipo de ciberataques al estar conectado desde el hogar; como se muestra en la Figura 5.

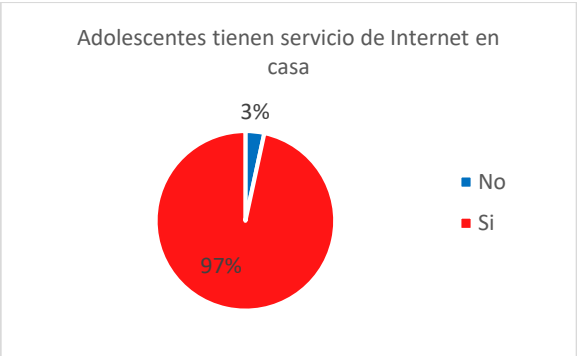


Figura 5. Porcentaje de adolescentes que tienen servicio de Internet

Asimismo, los adolescentes indican que se conectan a Internet a través de distintos equipos tecnológicos, como se muestra en la Tabla 3.

Tabla 3. Tipos de equipos informáticos utilizados por adolescentes

Número de estudiantes	Porcentaje	Equipo utilizado
601	66,6%	Smartphone
378	41,9 %	Computadora de escritorio
330	36,6%	Laptop
37	4,1%	Tablet
12	1,3%	Cabina de Internet
2	0,2%	Equipo desde la biblioteca

Con base a los resultados de la encuesta realizada a 855 adolescentes, se puede analizar que un gran grupo de adolescentes tiene un equipo informático en el dormitorio, la mayoría son aquellos que se encuentran entre 15 a 17 años. Así se lo puede mostrar en la Tabla 4.

Tabla 4. Tipo de equipo informático utilizado para conectarse a Internet desde el dormitorio

Ubicación de equipo tecnológico	Porcentaje de encuestados	Total de encuestados
En el cuarto de estudio	20,6%	176
Está en la sala	39,9%	341
Está en mi dormitorio	31,3%	268
No tengo computadora en casa	8,2%	70
Total respuestas		**855**

Tabla 5. Adolescentes por grupo de edad que tienen el equipo informático en el dormitorio

Edad	Porcentaje	Total
17	15%	39
16	19%	51
15	18%	47
14	12%	33
13	17%	46
12	19%	52
Total		**268**

El 39,4% de estudiantes que tienen correo electrónico y/o redes sociales no son supervisados por los padres de familia. El 23,1% indica que son supervisados menos de 3 veces al mes y el 37,6% si es controlado por los padres de familia. Por tanto, existe una mayor probabilidad de que los estudiantes sufran algún tipo de ciberataque, al no tener supervisión de parte de padres/madres de familia.

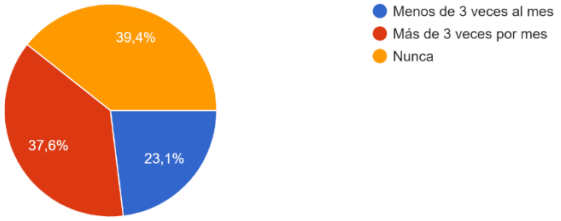


Figura 6. Número de adolescentes sin supervisión sobre redes sociales y cuentas de correo electrónico

Analizando los datos de aquellos adolescentes que no cuentan con una supervisión de parte de padres de familia o de algún adulto, estos llegan a cubrir el 23% de los adolescentes; es decir, el mayor porcentaje corresponde al grupo entre 15 y 17 años de edad. Como se muestra en la Figura 7.

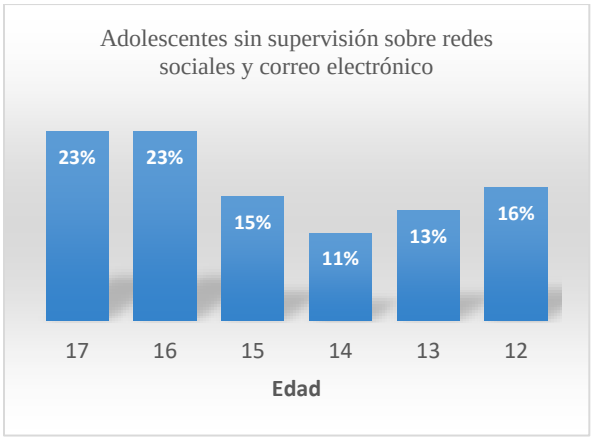


Figura 7. Adolescentes por grupos de edad sin supervisión de redes sociales y correos electrónicos

En la Figura 8, se puede observar que los adolescentes tampoco cuentan con una supervisión adecuada de los equipos informáticos como computadoras, laptops, Smartphone, Tablet que utilizan, ya sea para clases a distancia o virtuales o actividades diarias. El 44% de los estudiantes, no son supervisados por ningún padre/madre de familia por la confianza sobre sus hijos. El 33% indica que sus equipos si son supervisados más de 3 veces al mes. El 17% indica que son supervisados menos de 3 veces por mes. El 4% de estudiantes indica que nunca han supervisado sus equipos informáticos por desinterés de los padres y el 2% de estudiantes indica que sus padres nunca han supervisado sus equipos informáticos por desconocimiento del uso de los mismos. Por tanto, se tiene que, el 50,13% de estudiantes puede sufrir de algún tipo de ataque informático.

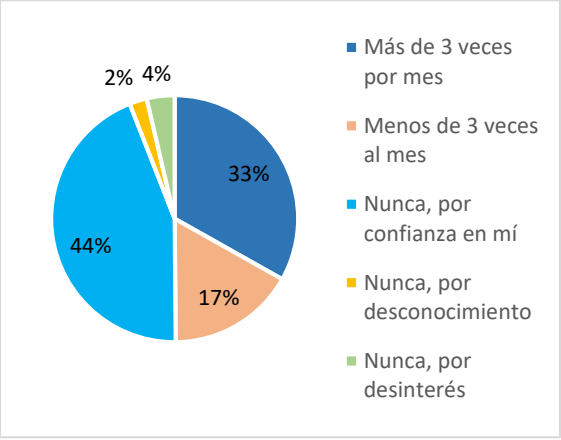


Figura 8. Supervisión de equipos informáticos

Los adolescentes que cuentan con menor supervisión de sus equipos tecnológicos, son aquellos de edad más avanzada; es decir, entre 15 y 17 años de edad. Así se muestra en la Figura 9.

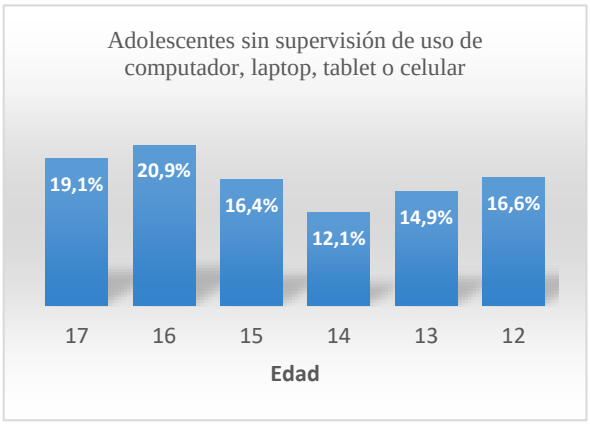


Figura 9. Adolescentes por grupo de edad sin supervisión de equipos informáticos

Con base a la información recolectada, se procede a analizar el tiempo que pasan los adolescentes conectados a Internet. Donde, el 45% pasa conectado a Internet siempre por las clases virtuales. El 29% indica que pasa conectado más de 3 horas al día. El 19% de adolescentes pasa conectado a Internet entre 1 a 3 horas al día. El 5% de adolescentes indica que pasa conectado menos de 1 hora al día y el 2% de los adolescentes sólo se conecta los fines de semana. Así se puede observar en la Figura 10.

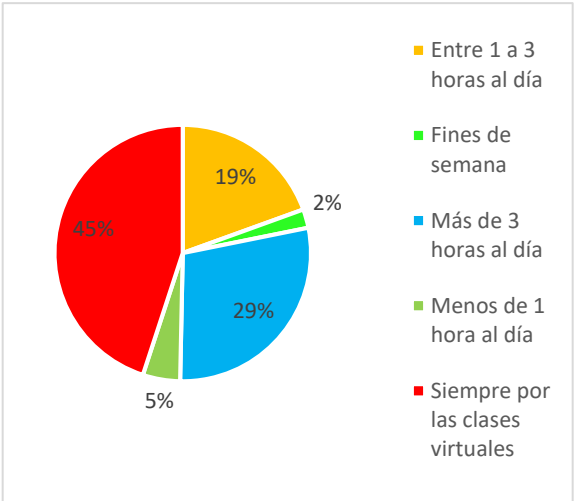


Figura 10. Frecuencia con la cual los adolescentes están conectados a Internet

Los adolescentes que indican que siempre pasan conectados a Internet por las clases virtuales, en su mayor número pertenece al grupo de 12 años con el 19,9%. Posteriormente se tiene al grupo de 15 años con el 17,9% y por último al grupo de 16 años con el 17,2%; como se muestra en la Figura 11.

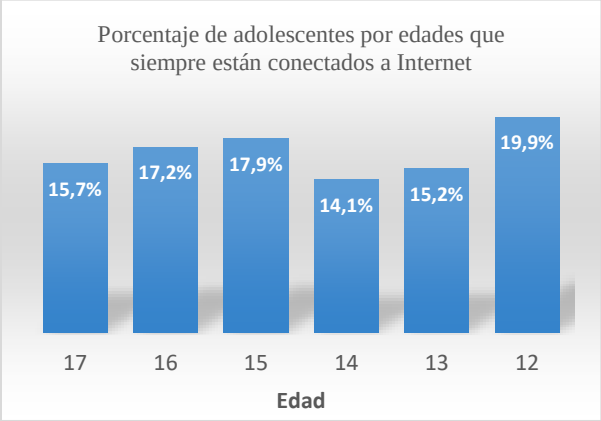


Figura 11. Adolescentes por grupos de edad que siempre están conectados a Internet

Se consultó sobre las actividades que los adolescentes realizan con mayor frecuencia frente a los dispositivos electrónicos e informáticos, y se tiene que el 57,4% de adolescentes utiliza los equipos informáticos para acceder a redes sociales; además, el 50,8% lo utiliza para el uso de streaming (observar y/o escuchar videos y música). El 44,9% lo utiliza para revisar su correo electrónico. El 44,3% también lo utiliza para acceder a juegos en línea. El 38,9% lo utiliza para descargar archivos y sólo el 2,70% para comercio electrónico. Por tanto, los adolescentes pueden ser más propensos a recibir un ciberataque a través de las redes sociales, streaming, correo electrónico, juegos en línea y por descarga de archivos.

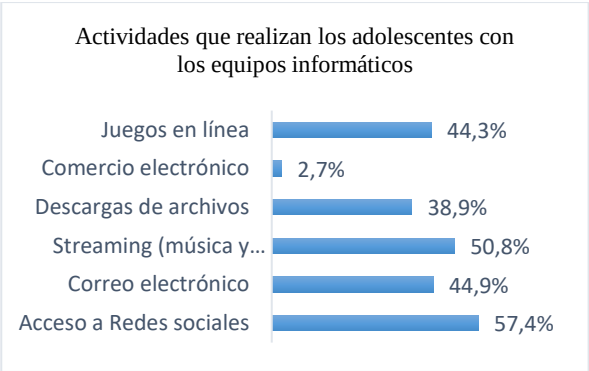
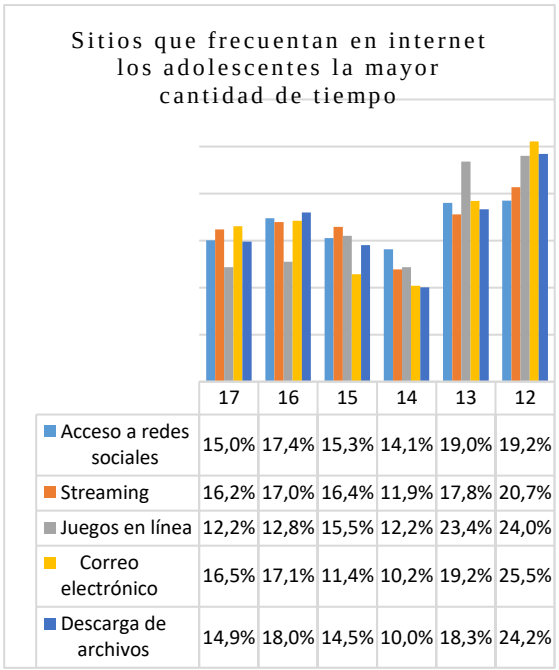


Figura 12. Actividades que realizan los adolescentes en los equipos informáticos

Se realizará mayor énfasis en las opciones mencionadas que superan el 40% de la muestra. Además, a través de estas aplicaciones se puede abrir la brecha para aplicar directamente un ataque de ingeniería social, como se observa en la Figura 13.



	17	16	15	14	13	12
Acceso a redes sociales	15,0%	17,4%	15,3%	14,1%	19,0%	19,2%
Streaming	16,2%	17,0%	16,4%	11,9%	17,8%	20,7%
Juegos en línea	12,2%	12,8%	15,5%	12,2%	23,4%	24,0%
Correo electrónico	16,5%	17,1%	11,4%	10,2%	19,2%	25,5%
Descarga de archivos	14,9%	18,0%	14,5%	10,0%	18,3%	24,2%

Figura 13. Sitios que frecuentan en Internet los adolescentes con mayor frecuencia

Dentro de la encuesta se procede a consultar quién controla en mayor manera el uso de Internet; donde, se puede evidenciar que son las madres de familia quienes mayormente controlan a los adolescentes el acceso a Internet con un 51% de los encuestados. El 21% responde que nadie controla el acceso a Internet, lo cual indica que

se desconoce el tipo de navegación y los lugares a los cuales acceden. El 17% indica que son los padres quienes controlan el acceso a Internet. El 8% contesta que son las hermanas/os mayores quienes controlan el acceso a Internet. El 3% contesta que tienen algún otro familiar adulto quien controla el acceso a Internet.

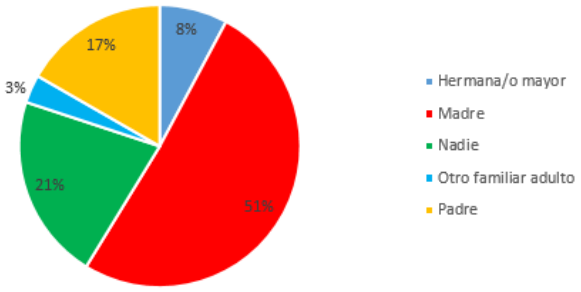


Figura 14. ¿Quién controla el acceso a Internet a los adolescentes en casa?

Debido a que existe un grupo de adolescentes que indica que nadie le controla el acceso a Internet, y siendo este el segundo valor más alto de la gráfica anterior, se procederá a realizar un análisis del mismo.

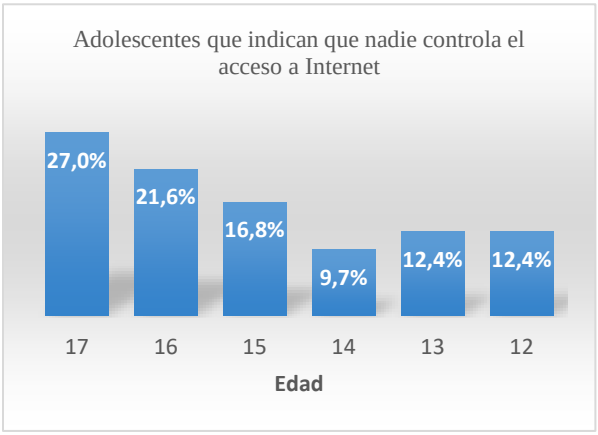


Figura 15. Adolescentes por grupo de edad sin supervisión de acceso a Internet

Se logra observar que los adolescentes que menor control tienen sobre el acceso a Internet son aquellos que se encuentran en el grupo de 15 a 17 años de edad.

Con base al resultado anterior, se requiere medir el nivel de seguridad con la cual cuentan los adolescentes al por el tiempo y exposición a la que se encuentran dentro de Internet. Por tanto, se requiere conocer la frecuencia con la cual cambian o modifican la contraseña en redes sociales y correo electrónico. Esta pregunta tiene dos finalidades, la primera es conocer si los adolescentes están conscientes de la importancia de actualizar y modificar las contraseñas de los correos electrónicos y las redes sociales por lo menos más de dos veces al año. Y la segunda es, analizar el grupo de adolescentes que pueden ser más vulnerables a un ciberataque por la falta de actualización y/o modificación de contraseñas.

Se logra identificar que el 63,7% de adolescentes no actualizan o modifican la contraseña de sus correos electrónicos y/o redes sociales. Mientras que el 36,3% de adolescentes aparentemente está consciente de la importancia de modificar las contraseñas.

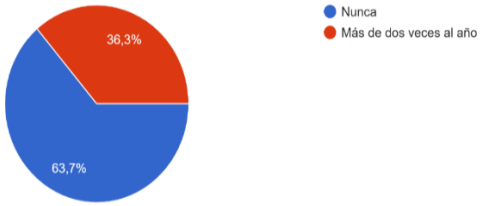


Figura 16. ¿Con qué frecuencia modifican la contraseña de correo electrónico y de redes sociales?

Con base a los resultados obtenidos y del análisis anterior, se puede observar que los adolescentes de 12 años de edad con un 29,0% son la mayor parte de usuarios que no cambian nunca la contraseña de su correo electrónico y de redes sociales, siendo más vulnerables a posibles ataques de ingeniería social. Así se muestra en la Figura 17.

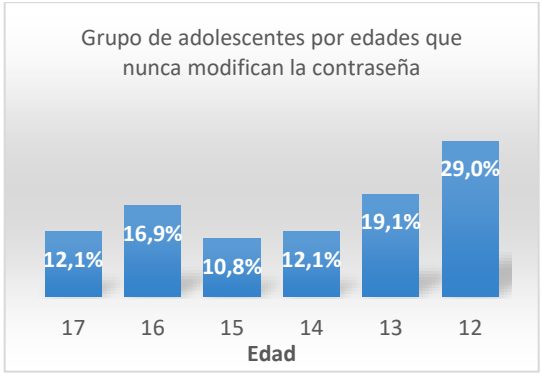


Figura 17. Grupo de adolescentes por edades que nunca modifican la contraseña

Se conoce que, al día de hoy, las contraseñas de fácil reconocimiento y de menor longitud en cuanto a caracteres son las más vulnerables, permitiendo así que un ciber delincuente pueda acceder y generar algún tipo de daño.

Para ello, se procede a consultar cómo tienen creada la contraseña en redes sociales y correos electrónicos con las diferentes opciones: letras (mayúsculas/minúsculas), números, caracteres especiales, combinación de las anteriores. Así se muestra en la Figura 18.

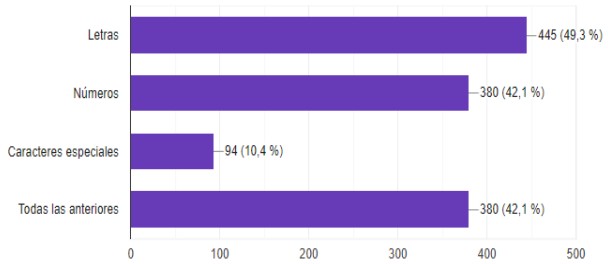


Figura 18. Configuración de contraseña de los adolescentes

Se puede observar los resultados de aquellos adolescentes que escogieron tanto una de las opciones o más, entre sus diferentes combinaciones. El resultado de ello se puede apreciar de la siguiente manera: el uso de letras (mayúsculas y minúsculas) es la forma más utilizada en crear contraseñas ya que un 49,3% de adolescentes la utiliza. El uso de números dentro de las contraseñas la realiza un 42,1% de adolescentes, una combinación con caracteres especiales lo realiza el 10,4%. Una combinación con caracteres como letras, números y caracteres especiales lo realiza un 42,1%.

Realizando un mayor análisis a los resultados anteriores, se procede a analizar a aquellos adolescentes que solamente escogieron la opción Letras (mayúsculas y minúsculas) sin ninguna de las otras posibles combinaciones; obteniendo que un 12% utiliza como contraseña el uso de letras, lo cual los hace más vulnerables ante un ataque de fuerza bruta.

Asimismo, las contraseñas para ser menos vulnerables deben contar con un número superior a 8 caracteres, de lo cual se observa que el 18,5% de adolescentes usa contraseñas de menos de 8 caracteres, lo cual indica que tanto sus cuentas de correo como de redes sociales pueden ser vulneradas con mayor facilidad. Así se puede confirmar en la Figura 19.

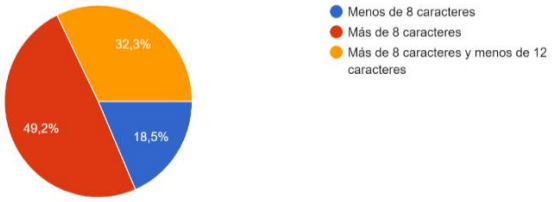


Figura 19. Número de caracteres utilizado para crear contraseñas

Profundizando en el mismo tema, se analiza aquellos adolescentes que utilizan solamente letras, para la creación de contraseñas. Obteniendo que, de 82 adolescentes, 42 de ellos que representan al 51,2% pertenecen al grupo de 12 a 13 años de edad, volviéndolos más vulnerables; como se muestra en la Figura 20.

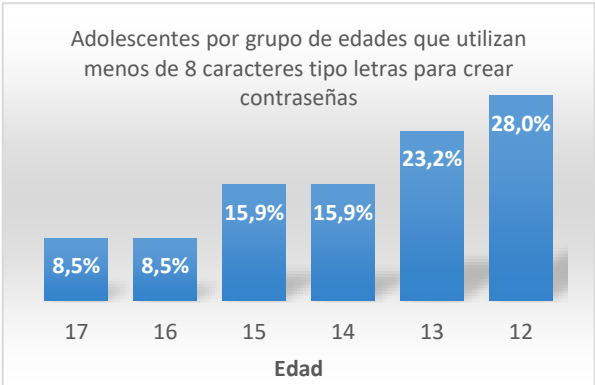


Figura 20. Adolescentes por grupo de edades que utilizan menos de 8 caracteres tipo letras para crear contraseñas

Con todos estos resultados obtenidos, se desea conocer cuáles son las aplicaciones más utilizadas por los adolescentes. De lo cual se obtiene los siguientes resultados:

Como se puede observar en la Figura 21, el 91,2% de los adolescentes acceden a la herramienta de YouTube, esto se debe a que la mayoría navega en Internet para ver videos, escuchar música e interactuar con youtubers.

El 89,4% de adolescentes utiliza WhatsApp. El 72,4% utiliza Facebook.

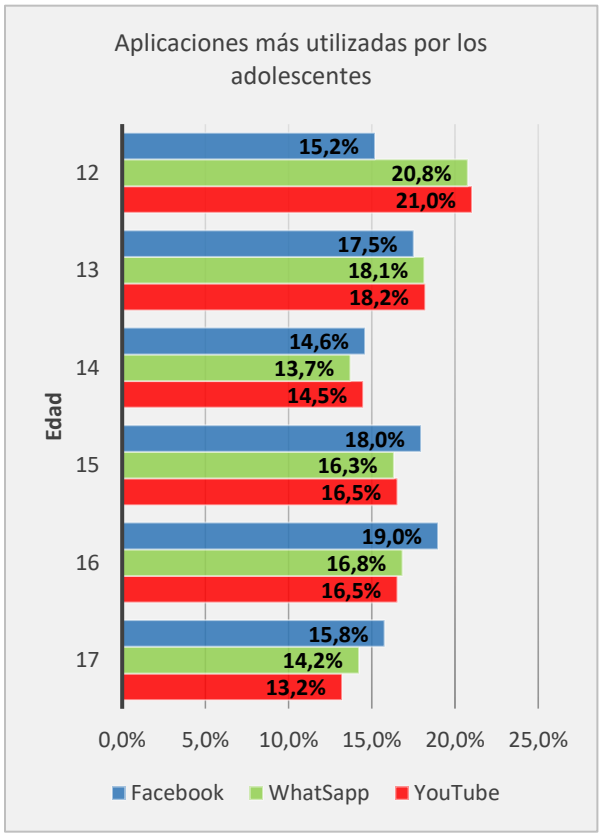


Figura 21. Aplicaciones más utilizadas por los adolescentes

De similar manera, se procedió a consultar si los adolescentes tienen cuentas de redes sociales que los padres no conozcan. Donde, se puede observar en la Figura 22, el 21,8% de adolescentes indican que si tienen cuentas de redes sociales que sus padres no conocen. Este grupo en su mayoría son aquellos que se encuentran entre 15 y 17 años de edad.

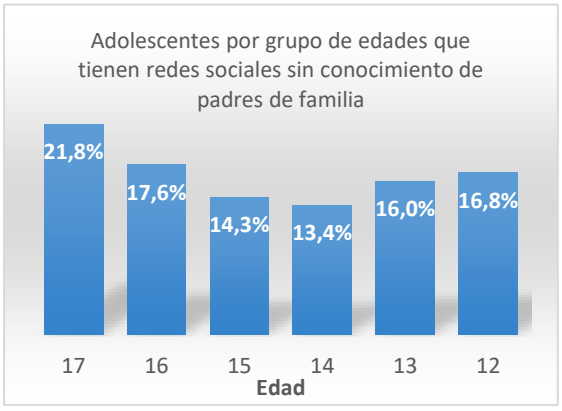


Figura 22. Adolescentes por grupos de edades que tienen redes sociales sin conocimiento de padres de familia

Asimismo, de la encuesta realizada a los adolescentes, se puede observar en la Figura 23, que el 15,1% de ellos crean la cuenta de usuario y/o el perfil con su nombre real.

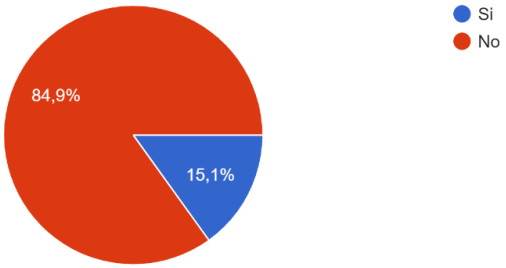


Figura 23. Uso de nombre real en redes sociales y correo electrónico

Pero lo que más llama la atención es que, la mayor parte de adolescentes que realizan esta actividad son los de menor edad, volviéndolos más vulnerables ante posibles ciberataques. Así se muestra en la Figura 24.

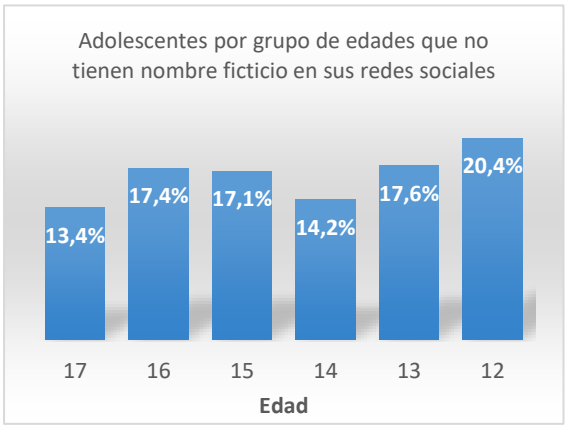


Figura 24. Uso de nombre real en redes sociales y correo electrónico

Los adolescentes al no ser supervisados, pasan un mayor número de horas expuestos ante posibles vulnerabilidades, y con ello a posibles a ataques de ingeniería social.

El 17,4% de adolescentes no tiene idea del número de veces que reacciona a los mensajes llegados en el día; es decir, algunos pierden la noción del tiempo o simplemente se ha generado algún tipo de adicción al estar pendiente de las redes sociales. Estos datos se pueden observar en la Figura 25.

Figura 25. Frecuencia con la cual se conectan los adolescentes a los dispositivos móviles.

Los adolescentes que mayormente pasan pendientes de las redes sociales y por tanto del celular o Tablet, se encuentran entre 15 y 17 años; pero, lo más preocupante es que una gran mayoría de adolescentes del grupo de 12 años conforman el 18,4% de la muestra.

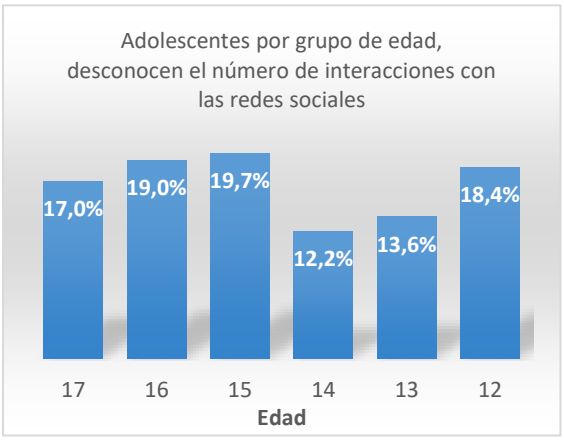


Figura 26. Adolescentes por grupos de edad que desconocen el número de interacciones con las redes sociales

Con todos estos datos recolectados, existe la posibilidad de que los adolescentes logren a acceder a sitios desconocidos o que les lleguen invitaciones de dudosa procedencia. Se puede observar en la Figura 27, que el 24,1% de adolescentes si llegan a aceptar invitaciones de perfiles desconocidos dentro de las redes sociales, probablemente porque le gusta la imagen de perfil o porque le llama la atención; lo cual los hace vulnerables a ataques de ingeniería social.

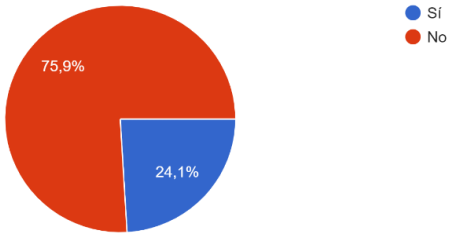
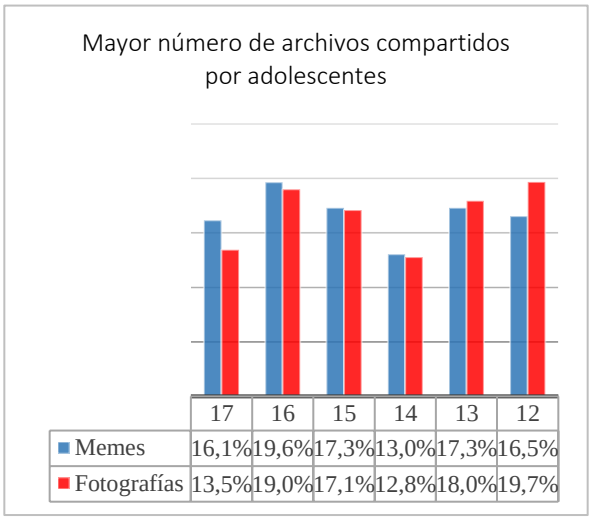


Figura 27. Adolescentes que aceptan la invitación de perfiles desconocidos en redes sociales

La información que más comparten los adolescentes a través de redes sociales, de acuerdo a grupos de edades son memes y fotografías. Así se puede observar en la Figura 28.



	17	16	15	14	13	12
Memes	16,1%	19,6%	17,3%	13,0%	17,3%	16,5%
Fotografías	13,5%	19,0%	17,1%	12,8%	18,0%	19,7%

Figura 28. Mayor número de archivos compartidos por adolescentes a través de redes sociales

Se debe tomar en cuenta que muchos adolescentes han llegado a utilizar las redes sociales incluso como una manera de desahogo, lo cual es peligroso, debido a que un ciberdelincuente puede aprovechar estas debilidades y proceder a realizar algún acto ilícito.

Así se puede observar en la Figura 29, que el 39,1% de adolescentes que han llegado a conocer a través de redes sociales a otras personas, finalizaron conociéndolas físicamente. De lo cual, el mayor grupo se concentra entre edades de 15 a 17 años.

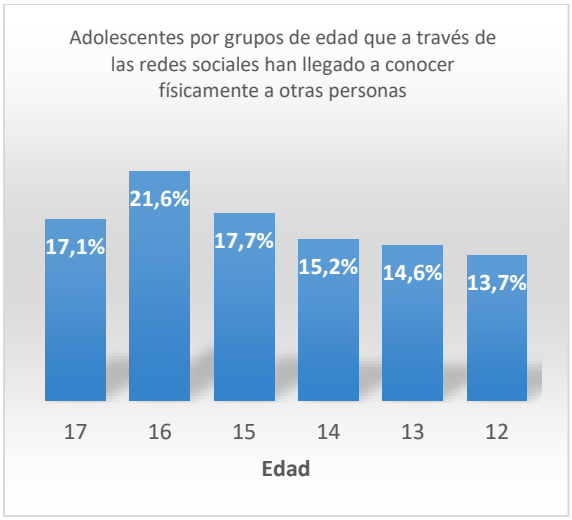


Figura 29. Adolescentes por grupos de edades que han llegado a conocer físicamente a otras personas

Los adolescentes de hoy en día se han hecho muy dependientes de la conexión a Internet y redes sociales. Actualmente la mayoría de adolescentes no conciben un mundo sin estas herramientas.

Así se muestra en la Figura 30 los resultados de la encuesta, donde un gran porcentaje de ellos llegan a tener síntomas de tristeza, aburrimiento y nerviosismo cuando no cuentan con servicio de Internet y por tanto del acceso a redes sociales; lo cual los lleva a tener síntomas de ansiedad, desesperación y depresión que puede recaer en un mayor problema a nivel social.

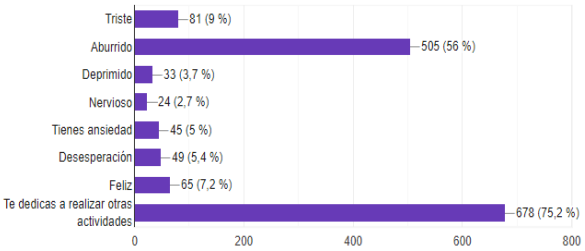


Figura 30. Estado de ánimo de adolescentes al no estar conectado a Internet y/o redes sociales

Al analizar los resultados del estado de ánimo negativo del cual sufren muchos adolescentes, se puede observar en la Figura 31, que recaen sobre los más pequeños del grupo de adolescentes; es decir, de 12 a 13 años de edad.

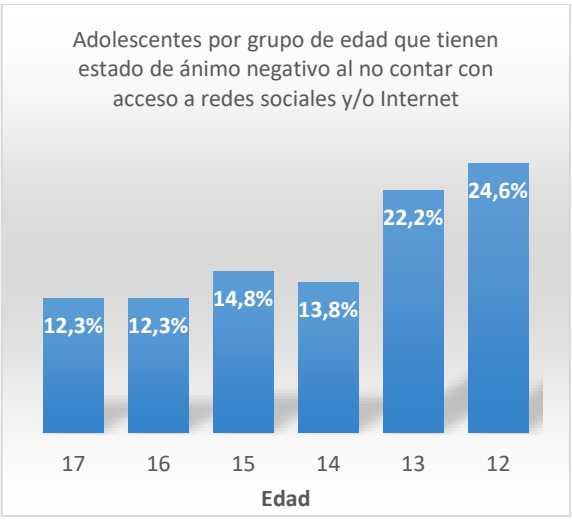


Figura 31. Adolescentes por grupo de edad con estado de ánimo negativo al no estar conectados a Internet y/o redes sociales

El 42% de adolescentes no conoce sobre el término ciberataque, así se puede observar en los resultados de la Figura 32. Lo cual es un indicador de la falta de educación tecnológica, haciéndolos más vulnerables a sufrir de algún tipo de ciberataque sin darse cuenta.

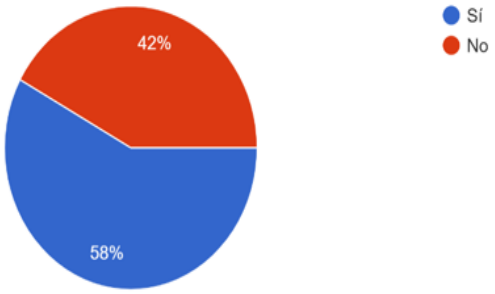


Figura 32. Adolescentes que han escuchado el término ciberataque

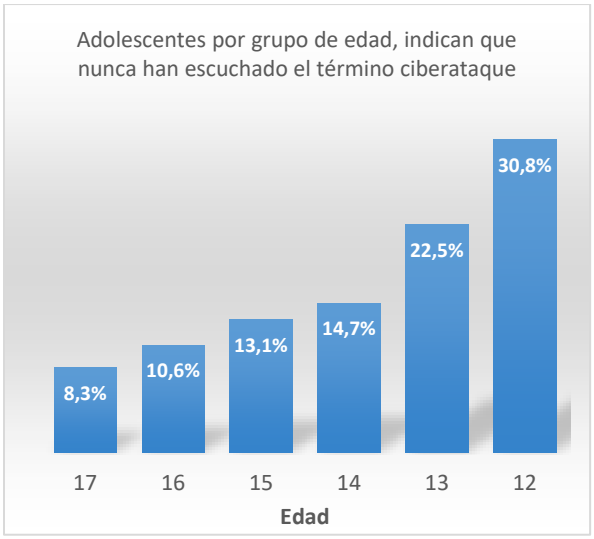


Figura 33. Adolescentes por grupo de edad que no han escuchado el término ciberataque

De este grupo de adolescentes que desconoce sobre el término ciberataque, y, por tanto, de los peligros del mismo; son más propensos a acceder a sitios o links que les puede llegar a través de correo electrónico y/o redes sociales. Así se puede mostrar en la Figura 34.

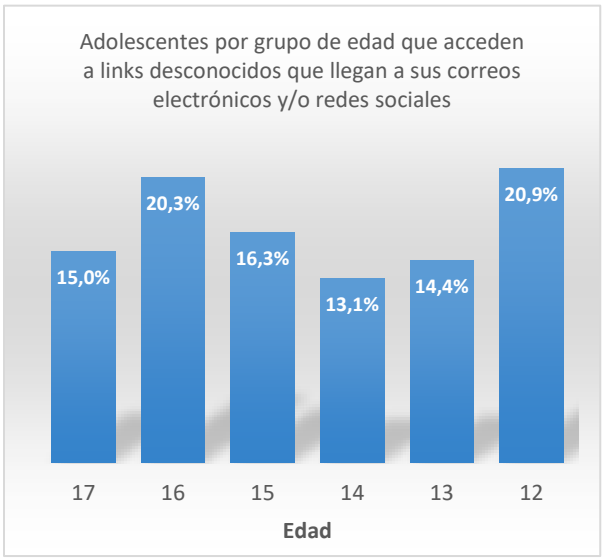


Figura 34. Adolescentes por grupos de edad que acceden a links desconocidos

El 90,9% de los adolescentes encuestados indican que nunca han sufrido de un ciberataque. Mientras tanto, el 9,1% indica que si ha sufrido de algún tipo de ciberataque. Tal como se muestra los resultados en la Figura 35.

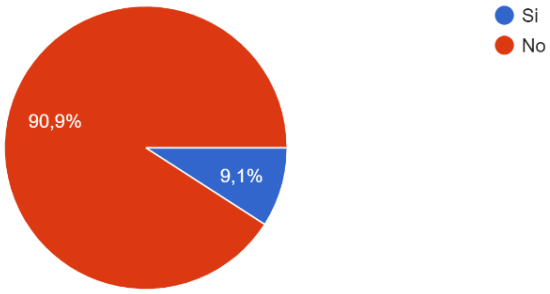


Figura 35. ¿Alguna vez ha sido víctima de un ciberataque?

Con base a los resultados de la encuesta, se procede a analizar a mayor detalle a aquellos adolescentes que si han sufrido algún tipo de ciberataque.

Las y los adolescentes entre 15 y 17 años de edad indican que si han sido víctimas de algún tipo de ciberataque. Se debe aclarar que, las y los adolescentes de menor edad desconocen en su mayoría lo que es un ciberataque, de acuerdo a los resultados obtenidos y analizados anteriormente. Por tanto, los adolescentes de menor edad pueden desconocer si en verdad han sido víctimas de un ciberataque. Para ello se muestra la Figura 36, para un mejor análisis.

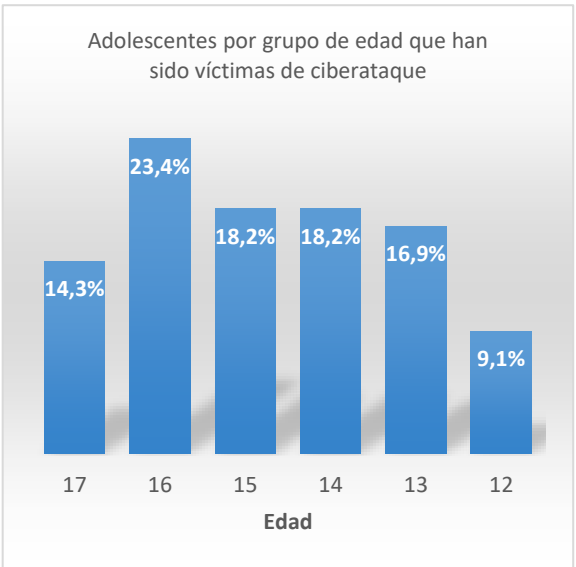


Figura 36. Adolescentes por grupos de edad que han sido víctimas de ciberataque

Con los ciberataques viene de la mano el acoso estudiantil o bullying que es ejecutado a través de las mismas herramientas tecnológicas utilizadas hoy en día. Los adolescentes encuestados indican que han sufrido bullying a través de diferentes tipos de tecnologías, como se muestra en la Figura 37 y Figura 38.

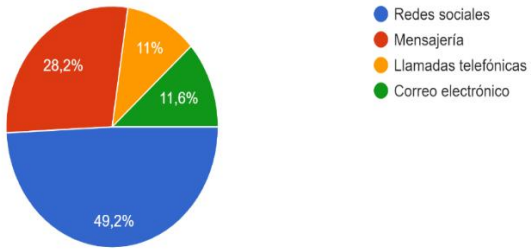


Figura 37. Adolescentes que han sufrido bullying a través de diferentes tipos de tecnologías

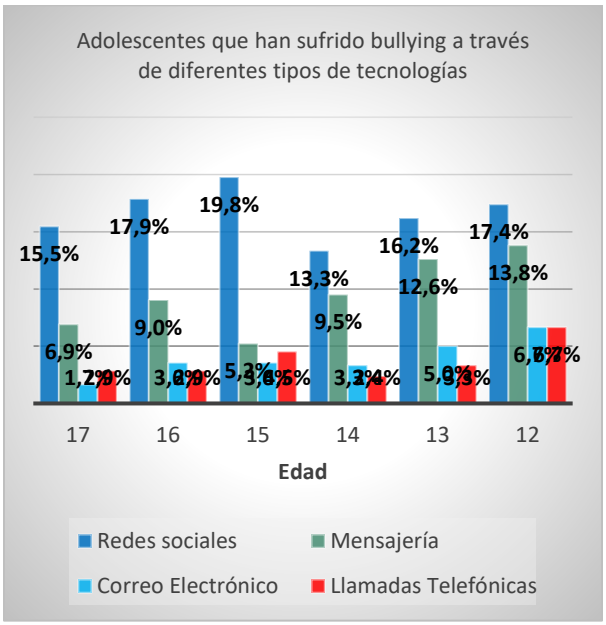


Figura 38. Adolescentes por grupos de edad que han sufrido bullying a través de diferentes tipos de tecnologías

Actualmente, los adolescentes cuentan con mayores conocimientos en cuanto al uso de tecnologías; lo cual puede facilitar a inculcar una buena base de conocimientos sobre peligros y seguridades informáticas, y tratar temas de seguridad en la publicación de información. Así se puede observar en la Figura 39; donde, el mayor porcentaje está entre 12 a 13 años de edad.

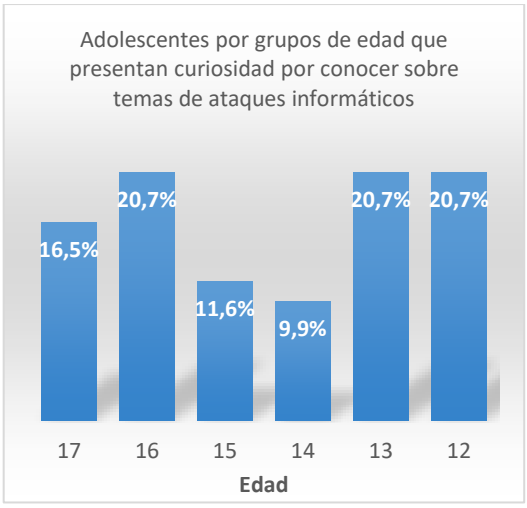


Figura 39. Adolescentes por grupos de edad que presentan curiosidad por temas de ataques informáticos

En la Figura 40, se puede observar que, un gran número de adolescentes no acude a personas adultas para dialogar sobre algún tipo de problema o peligros encontrados en Internet. Así lo demuestra el 14% de adolescentes encuestados, y como dato llamativo, se puede observar que existe un 0% de confianza en acudir a los docentes, con quienes actualmente interactúan la mayor parte del tiempo.

Figura 40. Nivel de confianza de parte de los adolescentes frente a problemas encontrados en Internet

Como dato relevante de la Figura 40, se logra obtener como resultado que, las madres de familia son quienes han dialogado o intervenido de mayor manera ante algún tipo de problema producido en Internet y/o a través de redes sociales de los adolescentes. Pero, asimismo, las madres de familia pueden llegar a ser víctimas de algún tipo de ciberataque y a través de ellas el delincuente puede llegar hasta las víctimas más vulnerables.

3.1 Desarrollo de laboratorio

Basados en los artículos 178, 180 y 212 del Código Orgánico Integral Penal, R.O. No. 180 del 10 de febrero del año 2014, páginas 31 y 35. Por ese motivo, como parte de la ejecución del ataque, no se utilizará ninguna de las cuentas de los adolescentes; para ello, se procede a crear una cuenta de correo y un perfil de usuario dentro de una red social, para el respectivo laboratorio.

Con base al análisis de datos, se puede encontrar un gran número de adolescentes vulnerables ante posibles ataques de ingeniería social. Para ello, los adolescentes con mayores problemas (82 adolescentes) que cuentan con poco control parental son los más vulnerables, sin dejar de lado a toda la muestra.

Al tratarse de usuarios que se encuentran entre edades de 12 a 17 años, por razones legales no se obtendrá más información sobre el mismo. Este es un laboratorio demostrativo, el cual no tendrá ninguna afectación y será totalmente transparente.

En la Figura 41, se ejemplifica el tipo y esquema de ataque a realizar.

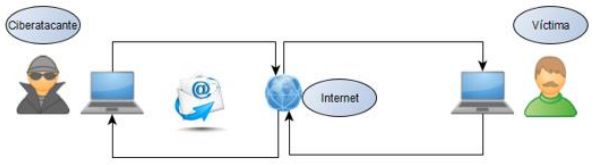


Figura 41. Esquema de ataque de ingeniería social a través de phishing

Para el laboratorio se procederá a simular un ataque de ingeniería social; cada ataque suele ser diferente, pero existen características que hacen que el ciclo de vida sea similar en todos.

Para ello se seguirá los pasos de la Figura 42.

Figura 42. Fases de Ingeniería Social [13]

Previo al ataque de ingeniería social, se procede a crear una cuenta de correo electrónico y un perfil de usuario (víctima) en la red social Facebook; con la finalidad de no involucrar posibles datos de adolescentes. Así se muestra en la Figura 43.

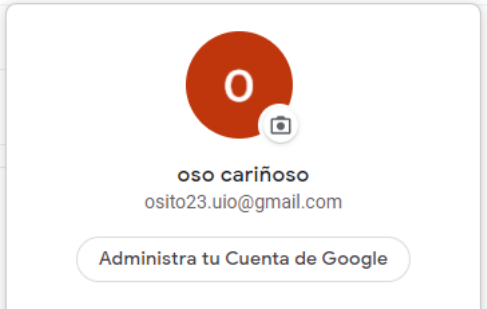


Figura 43. Cuenta de correo electrónico creada como víctima

Como parte del proceso para el envío de correo suplantado, se realiza la instalación y configuración de un servidor de correos (Linux, Postfix, Squirrelmail, Dovecot). La instalación y configuración no es parte de este estudio; por lo que se sugiere, investigar en cualquier navegador de Internet o en YouTube.

Para enmascarar la dirección IP, se procede a utilizar una herramienta de uso gratis en línea llamada **tinyurl.com**, tal como se muestra en la Figura 44.

Figura 44. Enmascaramiento de dirección IP o Dominio

De similar manera, dentro del servidor de correos, se configura una cuenta de correo electrónico como soporte.facebook para crear el ataque.

La manera en cómo atacan los ciberdelincuentes procede de la siguiente manera:

- Los ciberatacantes intentan aprovecharse de la curiosidad de la persona, estableciendo contactos no solicitados a nombre de personas que quizás conozca la víctima o que pueden ser de especial interés cuando se refiere a redes sociales. Una manera simple es suplantar el soporte técnico de algún servicio; en este caso soporte técnico de Facebook, como se muestra en la Figura 45.

Figura 45. Envío de correo, ataque de ingeniería social a través de phishing

- También pueden clonar sitios confiables con el afán de que el usuario registre los datos y de esta manera obtener datos privados. Con ello ya pueden llegar a robar información.
- Los ciberdelincuentes proceden a generar algún tipo de vínculo, con el fin de llegar a la confianza.
- Una vez que ya cuentan con la atención de la víctima, continuarán engañando hasta que la víctima caiga en la persuasión. En este caso, se solicita a la víctima que ingrese al link enviado al correo electrónico para que pueda acceder a la actualización emergente de Facebook.
- Logrado el objetivo de la confianza, se tomará un tiempo adecuado, para conocer a la víctima. En este caso de laboratorio, simplemente el ciberatacante debe esperar a que la víctima acceda al link enviado por correo electrónico, como se muestra en la Figura 46.

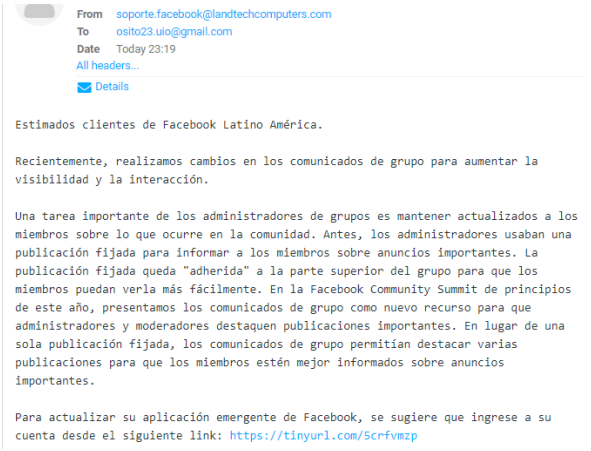


Figura 46. Correo de la víctima

Mientras tanto el ciberatacante, ya cuenta con un sitio clonado de la red social Facebook, para lo cual, se utilizó Kali Linux (Figura 47) y la herramienta **social engineering toolkit** [15]

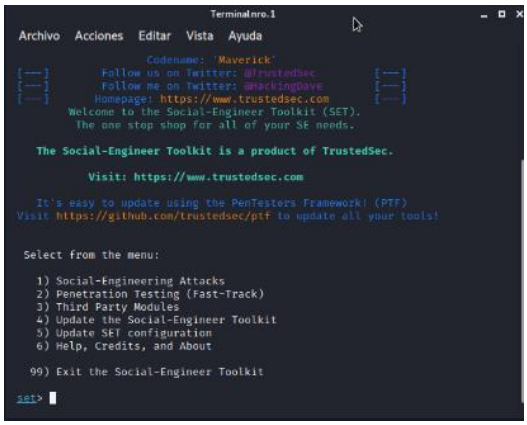


Figura 47. Herramienta de ingeniería social Setoolkit

En este laboratorio, la víctima accede al link enviado por correo electrónico, donde se puede observar la página principal de Facebook, la diferencia es que se encuentra clonado y la víctima al no observar la dirección URL procede a registrar los datos de usuario y contraseña para acceder a la misma. Así se muestra en la Figura 48.

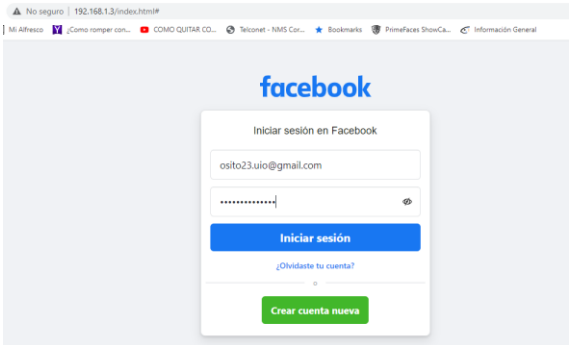


Figura 48. Ingreso de datos de la víctima

- Una vez que registra los datos, automáticamente es re-direccionado nuevamente a la pantalla principal de acceso de Facebook; pero en este caso, es el sitio oficial. En este sitio debe volver a registrar los datos, pero a diferencia del caso anterior, ya podrá acceder a su perfil oficial. Véase la Figura 49 y Figura 50.

Figura 49. Ingreso de datos de la víctima al sitio oficial

Figura 50. Acceso al perfil de usuario por parte de la posible víctima

- Mientras tanto, el ciberdelincuente al notar movimiento dentro de la consola del servidor de ataque, puede revisar que ya existe información digitada por parte de la víctima, como se muestra en la Figura 51.

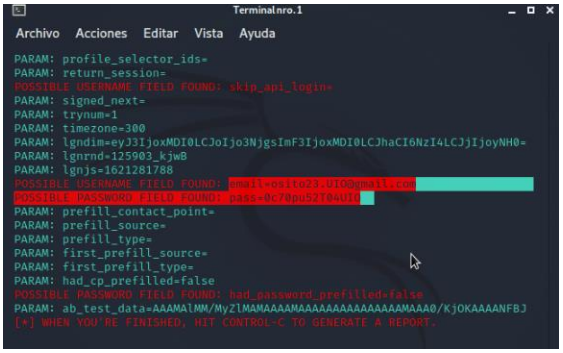


Figura 51. Captura de datos de la víctima

Posteriormente, con los datos obtenidos, el ciberatacante procede a ingresar a la red social de la víctima con los datos obtenidos como se muestra en la Figura 52 y Figura 51.

Figura 52. Acceso a cuenta de usuario de la víctima

Figura 53. Perfil de la víctima vista desde el cibercriminal

- El ciberdelincuente puede navegar por todos los ajustes de configuración de la cuenta robada. Así se puede mostrar en la Figura 54.

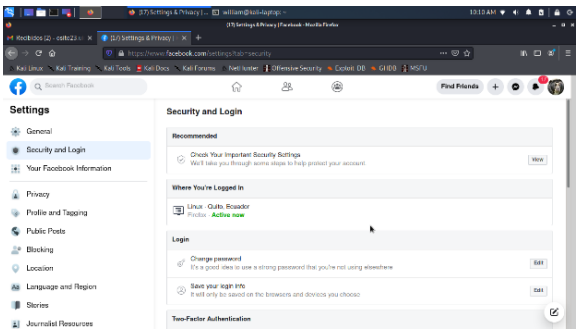


Figura 54. Ventana de administración de la víctima

4. Conclusiones

Actualmente no existen estrategias a nivel gubernamental correctamente definidas y difundidas respecto a los ciberdelitos.

Los ciberataques se producen por la falta de un correcto control y supervisión, de parte de padres de familias y adultos que se encuentran a cargo dentro del círculo familiar de los adolescentes.

Las instituciones educativas actualmente no generan y tampoco promueven una cultura en educación tecnológica, con la finalidad de motivar y educar sobre el tipo de información que debe ser publicado, replicado o enviado a través de las diferentes herramientas tecnológicas.

Actualmente, el Ecuador ya cuenta con una ley creada para tratar temas de ciberdelitos. Así se encuentra tipificado en el COIP en los artículos 178, 180 y 212.

Existe un 42% de adolescentes que desconocen sobre temas respecto a ciberataques y los problemas que se pueden presentar.

De acuerdo a la encuesta realizada, el 58% si tienen algún tipo de conocimiento, pero con deficiencias.

Bajo estas conclusiones; el estado, a través de cada una de las instituciones educativas debe:

- Educar a padres de familia, adolescentes, docentes y personal administrativo en cuanto a hábitos y uso correcto de las tecnologías de información, así se tiene: correo electrónico, redes sociales, navegación segura, video conferencias, peligros encontrados a través de Internet, equipos informáticos.

Los padres de familia deben:

- Ubicar los equipos tecnológicos en un espacio común del hogar, donde puedan mantener un control continuo sobre los adolescentes y el uso de los equipos tecnológicos.
- Dialogar con los adolescentes, indicando que los adultos son los responsables de las actividades, protección y correcto crecimiento de los adolescentes; por tanto, requieren revisar y supervisar las comunicaciones y actividades que tienen con otras personas.
- Motivar a los hijos y en especial a los adolescentes, a realizar actividades lúdicas que permitan mejorar su salud, potenciar su mente y optimizar de mejor manera su tiempo.
- Hablar libremente sobre los peligros que pueden encontrar con el mal uso de Internet.
- Supervisar el correcto uso de los equipos tecnológicos ocupados por los adolescentes.
- Solicitar ayuda profesional en caso de desconocer sobre temas tecnológicos; para ello, puede buscar temas específicos a través de los navegadores de Internet, video tutoriales o consultar con un especialista en seguridades y tecnologías de la información.
- Acudir a los entes de justicia respectivos como Fiscalía, UPC más cercano o llamando al 911, para poner la denuncia respectiva en caso de conocer de un delito informático producido hacia los adolescentes e inclusive hacia el mismo adulto.

Recomendaciones para el uso correcto de computadoras, laptop y dispositivos móviles.

Los docentes de las instituciones educativas y padres de familia deben:

- Fomentar el uso correcto de las TIC´s.
- Fijar horarios y lugares permitidos de uso.
- Instalar software antivirus en los equipos informáticos y tecnológicos con su respectiva licencia.
- Evitar la instalación de software pirata o descargadas de páginas de dudosa procedencia.
- Crear contraseñas robustas mínimo 8 caracteres combinando letras mayúsculas y minúsculas, números y símbolos. Mientras más larga más complicado vulnerarla.

- No ceder contraseñas de los sistemas informáticos de la institución educativa.
- Realizar copias de seguridad de la información de los equipos informáticos y de los dispositivos móviles.

Recomendaciones para el uso correcto de cuentas de correo electrónico y redes sociales.

Las cuentas de correo electrónico y de redes sociales de los adolescentes deben:

- Ser supervisadas constantemente por los padres de familia o por algún adulto que se encuentre sobre la tutela del adolescente.
- Ser modificadas por lo menos dos veces al año.

Dentro de la información del perfil de usuario y del contenido de correos electrónicos:

- Evitar compartir información sensible dentro de las redes sociales; por ejemplo: lugar de estudio, lugar de trabajo, fechas de nacimiento, número de teléfonos, nombre de cuentas de otras redes sociales, fotografías de familiares expuestas al público en general.
- No entregar datos de acceso de otras plataformas tecnológicas.
- En caso de recibir un correo electrónico de dudosa procedencia, debe rechazarlo inmediatamente.
- Ser precavido ante la llegada de correos electrónicos desconocidos e identificar su procedencia.
- Evitar el registro de datos personales a través de links de páginas web de dudosa procedencia.
- No contestar a correos electrónicos de dudosa procedencia.
- Analizar los archivos previamente a la apertura o a la descarga de los mismos utilizando un antivirus actualizado.
- No utilizar la misma contraseña para todas las herramientas (correo electrónico, redes sociales, sistemas bancarios, etc.) que utilizan a nivel personal.
- Eliminar el historial de navegación de manera continua.

Recomendaciones en caso de ser víctima de un ciberataque.

En el caso de notar u observar un atentado de ciberataque a un adolescente, se debe:

- Mantener la calma.
- Actuar inmediatamente.
- Escuchar a los adolescentes sin exagerar y sin minimizar el problema.
- No culpar a las tecnologías.
- Respaldar la información del ciberataque ejecutado; la misma será utilizada como prueba ante los entes de justicia respectivos.
- Bloquear al ciberatacante.
- Acudir a los entes de justicia respectivos como Fiscalía, UPC más cercano o llamando al 911, para poner la denuncia respectiva.
- Dialogar con los adolescentes y demostrar el apoyo para mejorar su autoestima.
- El gobierno tiene la obligación de educar a la sociedad sobre los problemas y formas de mitigar los ciberataques.
- Realizar un seguimiento profesional al estado anímico y posible daño psicológico producido en los adolescentes que hayan sufrido un ciberataque.
- Localizar a un especialista en seguridad de la información, que ayude a identificar el tipo de ataque realizado y brinde la capacitación respectiva para aprender a mitigar temas de ciberataque.
- Depurar la lista de contactos dentro de las redes sociales y bloquear a cuentas desconocidas de los adolescentes afectados.

Referencias

[1] S. Ayala, «Asociación Mexicana de Psicoterapia y Educación,» 01 Noviembre 2018. [En línea]. Available: https://www.psicoedu.org/el-peligro-de-las-redes-sociales-sexting-y-grooming/?v=55f82ff37b55.

[2] MINTEL, «Ministerio de Telecomunicaciones,» 17 abril 2002. [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf.

[3] ChildFound, «NaveguemosSeguros,» 2020. [En línea]. Available: https://www.childfund.ec/boletin-de-prensa-pedofilos-acechan-a-ninos-y-ninas-en-internet/.

[4] CriteriosDigital, «Ecuador es el tercer país más ciberinseguro de la región,» 05 12 2019. [En línea]. Available: https://criteriosdigital.com/noticias/ecuador-chequea/ciberseguridad-ecuador/.

[5] A. Luis Vásquez, «ESPACIO VIRTUAL RIESGOSO PARA LA NIÑEZ Y ADOLESCENCIA,» 22 enero 2019. [En línea]. Available: https://www.derechoecuador.com/espacio-virtual-riesgoso-para-la-ninez-y-adolescencia.

[6] Ministerio_Inclusión_Económica_y_Social, «www.inclusion.gob.ec,» 03 agosto 2018. [En línea]. Available: https://www.inclusion.gob.ec/wp-content/uploads/2019/01/acuerdo_ministerial_029..pdf. [Último acceso: 03 junio 2021].

[7] ChildFund-Ecuador, «NaveguemosSeguros,» 2020. [En línea]. Available: https://www.childfund.ec/boletin-de-prensa-pedofilos-acechan-a-ninos-y-ninas-en-internet/.

[8] InternetSegura, «Internet Segura,» octubre 2020. [En línea]. Available: https://internetsegura.gob.ec/#.

[9] InternetSegura, «Internet Segura,» 30 noviembre 2020. [En línea]. Available: https://internetsegura.gob.ec/?p=895.

[10] CEPAL, «Economía digital para el cambio estructural y la igualdad,» de Publicación de las Naciones Unidas, Santiago de Chile, 2013.

[11] Elmer_Linares_Vigo, «uDocz,» 2021. [En línea]. Available: https://www.udocz.com/read/8994/m-todos-para-calcular-la-poblacion-futura--1-.

[12] P. López, «SCIELO,» 2004. [En línea]. Available: http://www.scielo.org.bo/scielo.php?pid=s1815-02762004000100012&script=sci_arttext.

[13] Cuadernos_de_seguridad, «Cuadernos de seguridad,» 10 02 2020. [En línea]. Available: https://cuadernosdeseguridad.com/2020/02/ingenieria-social-seguridad-incibe/.

[14] «The Harvester,» Osintux, 2021. [En línea]. Available: https://www.osintux.org/documentacion/the-harvester. [Último acceso: 25 06 2021].

[15] FTAMEZ, «https://www.nubetia.com,» 25 marzo 2020. [En línea]. Available: https://www.nubetia.com/que-es-setoolkit/.

[16] L. Vásquez, «ESPACIO VIRTUAL RIESGOSO PARA LA NIÑEZ Y ADOLESCENCIA,» 22 enero 2019. [En línea]. Available: https://www.derechoecuador.com/espacio-virtual-riesgoso-para-la-ninez-y-adolescencia.

[17] ECUADORTV, «ecuadortv,» 06 03 2020. [En línea]. Available: https://www.ecuadortv.ec/categoria/fanatico/noticias/actualidad/internet-ciberseguridad-ecuador-proteccion-derechos.

[18] Ignitech, «AdvPhishing: Herramienta avanzada OTP Phishing!,» ESGEEKS, [En línea]. Available: https://esgeeks.com/advphishing-herramienta-avanzada-otp-phishing/.