Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables

Maestría en Telecomunicaciones

Ingeniería social: Análisis de las técnicas más utilizadas en los ataques a redes sociales y la percepción de la población urbana de Loja.

Trabajo de Titulación, previo a la obtención del título de Magister en Telecomunicaciones.

AUTOR:

Ing. Cristian Fabián Guerrero Espinosa

DIRECTOR:

Ing. John Tucker Yépez, Mg. Sc.

Loja-Ecuador

2024

Certificación

Universidad Nacional de Loja

1859

Sistema de Información Académico Administrativo y Financiero - SIAAF

CERTIFICADO DE CULMINACIÓN Y APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Yo, **TUCKER YEPEZ JOHN JOSSIMAR**, director del Trabajo de Integración Curricular denominado **Ingeniería social: Análisis de las técnicas más utilizadas en los ataques a redes sociales y la percepción de la población urbana de Loja**, perteneciente al estudiante **CRISTIAN FABIAN GUERRERO ESPINOSA**, con cédula de identidad N° **1104679079**.

Certifico:

Que luego de haber dirigido el **Trabajo de Integración Curricular**, habiendo realizado una revisión exhaustiva para prevenir y eliminar cualquier forma de plagio, garantizando la debida honestidad académica, se encuentra concluido, aprobado y está en condiciones para ser presentado ante las instancias correspondientes.

Es lo que puedo certificar en honor a la verdad, a fin de que, de así considerarlo pertinente, el/la señor/a docente de la asignatura de **Integración Curricular**, proceda al registro del mismo en el Sistema de Gestión Académico como parte de los requisitos de acreditación de la Unidad de Integración Curricular del mencionado estudiante.

Loja, 26 de Junio de 2024

JOHN JOSSIMAR TUCKER YEPEZ

F) ----------

DIRECTOR DE TRABAJO DE INTEGRACIÓN CURRICULAR

Certificado TIC/TT.: UNL-2024-001275

1/1

Educamos para **Transformar**

Autoría

Yo, **Cristian Fabián Guerrero Espinosa**, declaro ser autor del presente trabajo de titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación del trabajo de titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma: Firmado electrónicamente por: CRISTIAN FABIAN GUERRERO ESPINOSA

Cédula de Identidad: 1104679079

Fecha: 28 de junio de 2024

Correo electrónico: cristian.f.guerrero@unl.edu.ec

Teléfono: 0997244165

Carta de autorización por parte del autor para la consulta de producción parcial o total, y/o publicación electrónica de texto completo del trabajo de titulación.

Yo**, Cristian Fabián Guerrero Espinosa**, declaro ser autor del trabajo de titulación denominado: **Ingeniería social: Análisis de las técnicas más utilizadas en los ataques a redes sociales y la percepción de la población urbana de Loja. ,** como requisito para optar el título de **Magíster Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del trabajo de titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los veintiocho días del mes de junio del dos mil veinticuatro.

Firma: Firmado electrónicamente por: CRISTIAN FABIAN GUERRERO ESPINOSA

Autor: Cristian Fabián Guerrero Espinosa
Cédula: 1104679079
Dirección: Loja
Correo Electrónico: cristian.f.guerrero@unl.edu.ec
Teléfono: 0997244165

DATOS COMPLEMENTARIOS:
Director del trabajo de titulación: Ing. John Jossimar Tucker Yépez Mg. Sc.

Dedicatoria

Al concluir exitosamente esta importante etapa de mi formación académica, deseo expresar mi sincero agradecimiento a quienes han sido parte fundamental de este logro.

En primer lugar, a mis queridos padres y familia, por su amor incondicional, apoyo constante y confianza inquebrantable, impulsándome a alcanzar mis sueños y metas. A mi hermano Sebas, a quien busco inspirar con mi ejemplo. A mis amigos, que con sus palabras de aliento me han acompañado durante este trayecto. A Andrea, por su infinita paciencia y cariño brindado, especialmente en los momentos difíciles.

Y por supuesto, a Dios, por permitirme realizar uno de mis grandes anhelos y bendecirme con la presencia de mis padres en este día tan especial.

Cristian Fabián Guerrero Espinosa

Agradecimiento

A mi familia y amigos, quienes han sido parte esencial de mi crecimiento personal y profesional. Gracias por su constante apoyo y motivación para seguir adelante en todos los momentos de mi vida. Su compañía y aliento han sido fundamentales para alcanzar mis metas.

Al Ingeniero John Tucker, le expreso mi sincera gratitud por su valiosa contribución a través de su amplia experiencia, sólidos conocimientos y acertada dirección. Su guía fue clave para el logro del presente trabajo de titulación.

A todos ustedes, mi más profundo agradecimiento por creer en mí y caminar a mi lado.

Cristian Fabián Guerrero Espinosa

Índice de Contenidos

Índice de Tablas:

Índice de Figuras:

Índice de Anexos:

1. Título

Ingeniería social: Análisis de las técnicas más utilizadas en los ataques a redes sociales y la percepción de la población urbana de Loja.

2. Resumen

En un entorno digital cada vez más interconectado y en constante evolución, el ciberespacio ha experimentado un crecimiento exponencial en el uso de redes sociales, propiciando un terreno fértil para la propagación de ataques cibernéticos basados en ingeniería social, entendiéndose como técnicas sofisticadas de manipulación psicológica que aprovechan la confianza y falta de conocimiento de los usuarios. La falta de comprensión de estas técnicas representa una amenaza significativa para la seguridad y privacidad de los usuarios en línea, dejando tanto a individuos como a organizaciones expuestos a graves riesgos, desde la filtración de datos o información confidencial hasta la vulneración de sistemas y cortes de servicios.

Esta investigación tiene como objetivo principal analizar a fondo los mecanismos de la ingeniería social, evaluar su impacto y proponer estrategias de prevención y mitigación. Para ello, se realizó un estudio exhaustivo que combinó el análisis de casos de estudio, encuestas a usuarios, así como la revisión de la literatura académica relacionado al tema.

Los resultados del presente trabajo de investigación buscan contribuir al conocimiento científico y práctico sobre la ingeniería social, sentando las bases para el desarrollo de programas de capacitación y herramientas tecnológicas que permitan a individuos y organizaciones blindarse de manera efectiva contra este tipo de amenazas. Al generar conciencia sobre los peligros y estrategias de prevención, este trabajo aspira a empoderar a los usuarios y mejorar sustancialmente la seguridad en el entorno digital en constante evolución.

Palabras Clave: *Ciberseguridad, ciberataques, ciberdelitos, redes sociales, ciberespacio, ingeniería social.*

Abstract

In an increasingly interconnected and constantly evolving digital environment, cyberspace has experienced exponential growth in the use of social networks, providing fertile ground for the propagation of cyber-attacks based on social engineering, understood as sophisticated psychological manipulation techniques that exploit users' trust and lack of knowledge. The lack of understanding of these techniques represents a significant threat to the security and privacy of online users, leaving both individuals and organizations exposed to serious risks, ranging from data leaks or sensitive information breaches to system intrusions and service outages, thus generating devastating and far-reaching consequences.

The primary objective of this research is to thoroughly analyze the mechanisms of social engineering, evaluate its impact, and propose prevention and mitigation strategies. To this end, an exhaustive study was conducted that combined the analysis of case studies, user surveys, and a review of academic literature related to the topic, encompassing a multidisciplinary approach. This comprehensive investigation aims to bridge the gap between theoretical knowledge and practical application in the field of cybersecurity.

The results of this research endeavor seek to contribute to scientific and practical knowledge about social engineering, laying the foundations for the development of training programs and technological tools that enable individuals and organizations to effectively protect themselves against such threats. By raising awareness of the dangers and prevention strategies, this work aspires to empower users and substantially enhance security in the ever-evolving digital environment, thereby promoting safer and more responsible use of information technologies. The findings also highlight the importance of continuous education and adaptive measures to keep pace with the rapidly changing landscape of cyber threats

Keywords: *Cybersecurity, cyberattacks, cybercrime, social networks, social media, cyberspace, social engineering.*

3. Introducción

En la era digital actual, la creciente interconexión y dependencia de las tecnologías de la información y la comunicación han transformado drásticamente la forma en que nos relacionamos, trabajamos y accedemos a la información.

El ciberespacio, ese entorno virtual donde convergen estas actividades digitales, se ha convertido en un campo fértil para nuevas oportunidades y emprendimientos, pero también en un entorno vulnerable a diversos factores de riesgo.

En los siguientes capítulos de esta investigación, se abordarán los aspectos de mayor relevancia relacionados con la seguridad informática, el ciberespacio, la ciberseguridad y la ingeniería social. Además, se presentarán datos tanto a nivel internacional como nacional en relación con estas temáticas, con el propósito de resaltar la importancia de comprender, prevenir y mitigar los riesgos y amenazas asociados a la ingeniería social, los cuales afectan a los usuarios activos en el ciberespacio.

4. Marco Teórico

4.1.Seguridad Informática

4.1.1. ¿Qué es la seguridad informática?

En la actualidad, la tecnología desempeña un rol fundamental en la vida cotidiana de las personas, convirtiéndose en un tema de interés público de gran impacto. Por consiguiente, es imperativo comprender el concepto de seguridad informática.

La seguridad informática puede definirse como el conjunto de medidas, controles y salvaguardas diseñadas para proteger los sistemas de información y los recursos de accesos, modificaciones o disrupciones no autorizados que puedan comprometer la integridad, confidencialidad y disponibilidad de los datos e infraestructura tecnológica. Se constituye en un proceso continuo en el que se implementan técnicas, prácticas y procedimientos orientados a prevenir daños o alteraciones indebidas en los recursos informáticos, garantizando así su adecuado funcionamiento. (Costas, Jesús, 2014)

La seguridad informática, también conocida como seguridad de la tecnología de la información, se refiere a la práctica de proteger los sistemas informáticos, redes, dispositivos digitales, datos de acceso no autorizado, filtraciones de datos, ataques cibernéticos y otras actividades maliciosas. Su alcance es amplio y suele implicar una combinación de tecnologías y soluciones de seguridad que trabajan de manera conjunta para abordar las vulnerabilidades en dispositivos digitales, redes informáticas, servidores, bases de datos y aplicaciones de software. (IBM, 2023)

A partir de estas definiciones, la seguridad informática se concibe como un proceso integral cuyo objetivo primordial es evitar el acceso no autorizado a los sistemas de información y recursos, previniendo modificaciones o alteraciones que puedan afectar su correcto desempeño. Esto con el fin de preservar los principios fundamentales de la triada de la seguridad de la información.

4.1.2. Tipos de seguridad informática

Según Escrivá, Gema et al., (2013) la seguridad informática es definida como una disciplina derivada de la seguridad de la información, cuyo propósito fundamental es proteger los recursos y activos de datos que son procesados, almacenados o transmitidos a través de infraestructuras informáticas y de telecomunicaciones. En este ámbito se distinguen los siguientes tipos de seguridad informática:

- En función de lo se quiere proteger:

Seguridad física: Consiste en el conjunto de controles y medidas de protección aplicadas sobre los componentes físicos de un sistema informático, con el objetivo de resguardarlos frente a amenazas o incidentes tales como incendios, inundaciones, accesos no autorizados, vandalismo, robo de equipos, entre otros. Abarca la implementación de barreras de seguridad, sistemas de control de acceso, monitoreo por circuito cerrado, planes de contingencia y protocolos de respuesta ante eventos que puedan comprometer la integridad de la infraestructura tecnológica.

Seguridad lógica: Comprende el conjunto de mecanismos, herramientas y técnicas enfocadas en proteger los componentes no físicos o intangibles de un sistema informático. Su alcance incluye salvaguardar la integridad, confidencialidad y disponibilidad de los datos, aplicaciones, sistemas operativos y código fuente que conforman la infraestructura tecnológica de una organización. Algunos de los principales mecanismos de seguridad lógica son: El control y gestión de accesos mediante autenticación robusta, el cifrado criptográfico para proteger información sensible, la implementación de cortafuegos, antivirus y sistemas de detección de intrusos, así como el monitoreo continuo de actividades y eventos de seguridad.

- En función del momento en que tiene lugar la protección:

Seguridad activa: Son el conjunto de medidas, controles y procedimientos de carácter preventivo orientados a identificar, mitigar y neutralizar de manera proactiva cualquier amenaza o incidente potencial contra los sistemas informáticos antes de que estos ocurran. Su enfoque principal es desplegar mecanismos de protección que permitan evitar el impacto negativo de acontecimientos no deseados sobre la infraestructura tecnológica. Algunos ejemplos de seguridad activa incluyen el uso de contraseñas seguras y políticas de cambio periódico, la implementación de cortafuegos y sistemas de detección de intrusos, el cifrado de datos sensibles, la actualización de software, así como la ejecución de evaluaciones de vulnerabilidades y pruebas de penetración.

Seguridad pasiva: engloba el conjunto de técnicas, herramientas y procedimientos enfocados en minimizar el impacto y consecuencias de un incidente de seguridad informática una vez que este ha ocurrido. Su finalidad es implementar mecanismos reactivos y correctivos que permitan contener la propagación de la amenaza, restaurar la operación normal de los sistemas afectados y recuperar la información dañada en el menor tiempo posible. Algunos ejemplos representativos de controles de seguridad pasiva son: la generación periódica de copias de respaldo y puntos de restauración, la activación de protocolos de contingencia y la implementación de sistemas de tolerancia a fallas.

4.1.3. Principios fundamentales de la seguridad informática

La recomendación X.800 de la UIT (Unión Internacional de Telecomunicaciones) sugiere considerar los siguientes principios para proteger la información, los sistemas informáticos y de telecomunicaciones contra amenazas y riesgos de seguridad:

- Confidencialidad: Impide la divulgación de información a individuos, entidades o procesos no autorizados.
- Integridad: Garantiza que los datos no han sido modificados de manera no autorizada o accidental.
- Autenticidad: Permite confirmar la identidad de un sujeto o entidad.
- No repudio: Previene que una entidad niegue haber realizado una actividad o evento en particular.
- Control de acceso: Restringe el acceso a recursos, instalaciones, servicios, etc. Solo permite el acceso a entidades autorizadas de acuerdo con sus derechos y privilegios.
- Disponibilidad: Garantiza que los sistemas, servicios y recursos estén accesibles y utilizables cuando se requieran por las entidades autorizadas.

Estos principios son definidos por la UIT como objetivos fundamentales que deben cumplir las medidas de seguridad implementadas en cualquier arquitectura de seguridad de la información.

Dentro del conjunto de principios enlistados previamente, tres sobresalen conformando la reconocida y ampliamente recomendada triada de la seguridad de datos e información: confidencialidad, integridad y disponibilidad. Este trío de propiedades se establece como los pilares esenciales sobre los cuales se sustentan todas las iniciativas, regulaciones, mecanismos de control y programas de ciberseguridad adoptados por organizaciones y naciones. Dada su trascendencia, esta triada de principios es ampliamente avalada por expertos, normativas y estándares a nivel global como el eje medular de las estrategias de ciberseguridad

La seguridad informática se fundamenta en la implementación de diversas técnicas y controles, con el objetivo principal de salvaguardar los principios básicos considerados en la triada de la seguridad, reconocidos como los pilares tradicionales de este campo. Estos conceptos nos permiten determinar qué información, sistemas y componentes deben protegerse, así como cuándo y dónde aplicar las medidas de seguridad pertinentes en el entorno computacional. Van más allá de limitarse a aspectos puramente técnicos o de centrarse únicamente en qué partes específicas del sistema hay que proteger. (Beswick, 2019)

La IETF (Internet Engineering Task Force) define los conceptos de la triada de la seguridad de la siguiente manera:

Figura 1

Triada de la seguridad informática

Fuente: Autor.

- La confidencialidad: Se define como el concepto en el cual la información sea compartida únicamente entre partes autorizadas. La información debe permanecer inaccesible para personas, entidades o procesos no autorizados. (IETF, 2000)
- La integridad: Se define como el hecho de que los datos no han sido alterados ni destruidos de manera no autorizada o accidental. La integridad cubre los flujos de datos y/o el software apropiado. (IETF, 2000)
- La disponibilidad: Se refiere a que el servicio estará disponible para su uso cuando sea requerido por la entidad autorizada, de acuerdo con el contrato de nivel de servicio especificado u otras reglas de operación acordadas. (IETF, 2000)

Si bien es cierto que la mayoría de expertos coinciden en que no existe ningún sistema 100 % infalible y completamente seguro, el propósito fundamental es implementar un conjunto robusto de salvaguardas que brinden un nivel de seguridad razonable y aceptable para los usuarios, protegiendo adecuadamente la información crítica y la infraestructura tecnológica que la procesa, almacena y transmite. Para que un sistema informático pueda considerarse razonablemente seguro, debe cumplir a cabalidad con los principios mencionados anteriormente. (Escrivá, Gema et al., 2013)

Cabe destacar que la seguridad informática no es un estado estático, sino un proceso continuo y cíclico de identificación, prevención, detección y respuesta frente a amenazas y vulnerabilidades emergentes. A medida que evolucionan las tecnologías y se sofistican los ciberataques, los profesionales de ciberseguridad deben mantenerse constantemente

actualizados, fortaleciendo las defensas y adaptándose dinámicamente al panorama de riesgos cambiante.

4.1.4. Amenazas y vulnerabilidades informáticas

Baca, Gabriel, (2017) establece una clara diferencia entre los conceptos de amenaza y vulnerabilidad en el contexto de la seguridad informática, los mismos que describen a continuación:

- Una amenaza se define como cualquier circunstancia, evento o condición que representa un riesgo potencial de provocar un incidente no deseado, capaz de ocasionar daños, perjuicios o impactos negativos sobre los recursos y activos de información de una organización. Estas pueden originarse tanto en el entorno interno como externo a la infraestructura tecnológica, e incluyen factores como ataques maliciosos, desastres naturales, errores humanos, etc.
- Una vulnerabilidad es una debilidad, falla o condición intrínseca de fragilidad presente en un sistema, aplicación, dispositivo o componente informático que lo hace susceptible a ser explotado por una amenaza, permitiendo la materialización de un evento adverso y el posible compromiso de la confidencialidad, integridad o disponibilidad de la información. Las vulnerabilidades pueden derivarse de defectos en el diseño, configuración inadecuada, falta de controles apropiados, entre otros factores.

4.1.5. Ataques informáticos

Según el RFC-2828 (Request For Comments: 2828, Internet Security Glossary) de la IETF, un ataque se define como un asalto a la seguridad del sistema que se deriva cuando hay una amenaza inteligente, es decir, un acto deliberado y astuto que busca evadir los servicios de seguridad y violar la política de seguridad del sistema. Esto incluye actividades como intentos de acceso no autorizado, alteración de datos, destrucción de recursos, suplantación de identidad, entre otros.

En otras palabras, un ataque se refiere a cualquier actividad maliciosa destinada a causar daño o vulnerar la seguridad de un sistema o red.

Los ataques informáticos se clasifican en varios tipos, que se enumeran a continuación:

- Ataques activos: Son aquellos ataques que intentan alterar los recursos de un sistema o afectar su funcionamiento. (IETF, 2000)
- Ataques pasivos: Son ataques que intentan aprender o hacer uso de información del sistema, pero sin generar afectaciones a los recursos. (IETF, 2000)

- Ataques internos: Ataques iniciados por una entidad dentro del perímetro de seguridad (un "interno"), es decir, una entidad que está autorizada a acceder a los recursos del sistema, pero los utiliza de una manera no aprobada por quienes otorgaron la autorización. (IETF, 2000)
- Ataques externos: Son los ataques iniciados desde fuera del perímetro por un usuario no autorizado o ilegítimo del sistema (un "externo"). En Internet, los posibles atacantes externos van desde bromistas aficionados hasta delincuentes organizados, terroristas internacionales y gobiernos hostiles. (IETF, 2000)
- Ataques intencionales: Los ataques intencionales se definen como actividades que tienen la intención directa de causar daño, interferir con el funcionamiento normal de sistemas o redes, o comprometer la confidencialidad, integridad o disponibilidad de la información. (NIST, 2012)
- Ataques no intencionales: Los ataques no intencionales se refieren a actividades que, aunque no tienen la intención directa de causar daño o comprometer la seguridad, pueden resultar en vulnerabilidades, fallos o incidentes de seguridad debido a errores humanos, malentendidos, configuraciones incorrectas o fallos técnicos. (NIST, 2012)

4.1.6. Medidas de seguridad informática

En el ámbito de la seguridad informática, las actividades de mantenimiento y soporte desempeñan un rol esencial e irremplazable. Estas tareas operativas y rutinarias, engloban la gestión sistémica, la resolución de incidencias técnicas, la implementación y actualización de software, así como la asistencia y atención a los usuarios finales, son fundamentales para asegurar el adecuado funcionamiento, integridad y protección de toda la infraestructura tecnológica de una organización, independientemente de su escala o alcance. (Nieles et al., 2017)

Nieles et al., (2017) en su publicación "An Introduction to Information Security" señalan que la falta de consideración de la seguridad como parte integral de los procesos de mantenimiento y soporte puede ser perjudicial para cualquier entidad. La literatura dedicada a sistemas de seguridad de la información documenta numerosos casos en los que las organizaciones han socavado e invalidado sus costosas medidas de ciberseguridad debido a deficiencias en aspectos como la documentación técnica, la gestión de cuentas de usuario obsoletas, la presencia de software conflictivo, inconsistente o desactualizado y el control deficiente de las cuentas de mantenimiento y privilegios administrativos.

En este sentido, el reconocido estándar ISO/IEC 27002 sobre códigos de buenas prácticas para la gestión de la seguridad de la información, enfatiza la necesidad de establecer procedimientos operativos estándar que incorporen plenamente los requisitos y controles de seguridad aplicables. Esto implica que las organizaciones deben asegurar que sus políticas y procesos asociados al mantenimiento y soporte de sistemas contemplen de manera rigurosa los aspectos de confidencialidad, integridad y disponibilidad de la información y los activos tecnológicos.

En conclusión, una estrategia sólida de seguridad informática debe abarcar no solo la implementación de soluciones y herramientas técnicas, sino también la adopción de prácticas operativas y de soporte alineadas con los objetivos de ciberseguridad, a fin de preservar los recursos y activos críticos, cumpliendo las políticas de seguridad establecidas, frente a amenazas y vulnerabilidades emergentes.

Si bien las medidas de seguridad informática suelen enfocarse en controles técnicos como cortafuegos, sistemas de detección de intrusos, cifrado de datos, entre otros, es imperativo no descuidar la importancia de contar con sólidos procesos de soporte y operaciones debidamente alineados con los objetivos de seguridad.

Algunas de las medidas de seguridad informática más relevantes según Nieles et al., (2017):

- Implementación de gestión de accesos y controles de autenticación robustos: El Instituto Nacional de Estándares y Tecnología (NIST) enfatiza la importancia crítica de establecer procesos rigurosos para la identificación, autenticación y control de accesos a los sistemas, aplicaciones y datos. Esto incluye el uso de contraseñas seguras, autenticación multifactor, principios de menor privilegio y revisiones periódicas de cuentas y permisos.
- Protección de la integridad mediante listas de control de acceso y firmas digitales: El documento recomienda implementar mecanismos criptográficos como firmas digitales y listas de control de acceso para garantizar que sólo las entidades autorizadas puedan modificar datos, asegurando su integridad.
- Asegurar la confidencialidad a través de cifrado: Una de las medidas prioritarias es el cifrado de información sensible en transmisión y/o almacenada, utilizando algoritmos criptográficos sólidos y gestionando las claves de manera segura.
- Mantener el software actualizado y parches de seguridad: Se insta a las organizaciones a establecer procesos para mantenimiento y actualizaciones

periódicas de sistemas operativos, aplicaciones y firmware, con el fin de mitigar vulnerabilidades conocidas.

- Implementación de soluciones de respaldo y recuperación de datos: El NIST recalca la importancia de contar con mecanismos robustos de respaldo y poder restaurar datos críticos ante incidentes, asegurando la disponibilidad y continuidad operativa.
- Capacitación y concientización del personal en seguridad: La guía destaca la necesidad de programas continuos de capacitación y concientización en temas de seguridad para todo el personal, abordando políticas, amenazas, buenas prácticas, etc.

4.1.7. La importancia de la gestión de identidad y acceso

Como lo señala Task, J, (2013), miembro del NIST, en su documento "Security and Privacy Controls for Federal Information Systems and Organizations" la gestión de identidades y control de accesos es un componente crítico de la seguridad informática, mencionando lo siguiente:

"Los controles de gestión de identidades y accesos son fundamentales para la protección de la información y los sistemas informáticos. La implementación y gestión adecuada de estos controles es esencial para establecer dominios operativos, asignar derechos de acceso y establecer privilegios apropiados, al tiempo que previene la propagación de actividades no autorizadas dentro de los sistemas."

Asimismo, la certificación ISO/IEC 27001 sobre sistemas de gestión de seguridad de la información, establece como uno de sus controles clave en el Anexo A "Gestión de accesos de usuario", el cual comprende:

- Registro y cancelación de usuarios y derechos de acceso.
- Gestión de altas, bajas y revisiones de privilegios de acceso.
- Seguimiento y monitoreo de actividades de los usuarios.
- Restricción del acceso a información y sistemas de información.

Resumiendo, una sólida estrategia de gestión de identidades y control de accesos, que incluye autenticación robusta, principios de menor privilegio, monitoreo continuo y procesos rigurosos de revisión de cuentas y permisos, es indispensable para proteger los recursos y activo críticos, cumpliendo las políticas de seguridad establecidas frente a amenazas internas y externas. Por ello, organismos líderes y expertos en ciberseguridad la consideran una de las medidas prioritarias a implementar.

4.2.Ciberespacio

4.2.1. Definición de ciberespacio

El ciberespacio representa una nueva dimensión social y tecnológica, paralela a la realidad física, pero con dinámicas y características distintivas. Lejos de ser un simple reflejo o extensión del entorno tradicional, constituye un ámbito virtual autónomo y establecido, diseñado para satisfacer las necesidades y requerimientos de los usuarios en la sociedad contemporánea. Esta realidad se conforma por un entramado global de redes informáticas y sistemas de comunicación interconectados digitalmente. Es un espacio lógico integrado por componentes de hardware y software que posibilitan interacciones, transacciones e intercambios de información en formato digital. (Bytiak, Yuriy et al., 2021)

El ciberespacio no cuenta con una ubicación física o específica, como se mencionó anteriormente, es una realidad virtual dinámica y en continua transformación que trasciende las fronteras geográficas y temporales. Se superpone e impacta de manera significativa las barreras sociales, económicas, políticas y culturales del mundo físico tangible. Además, facilita el flujo global de datos, la comunicación sin barreras espaciales y la interacción humana en tiempo real mediante tecnologías de información y comunicaciones. (Bytiak, Yuriy et al., 2021)

Profesionales del Instituto Español de Estudios Estratégicos establecen que el ciberespacio es un entorno amplio e interconectado, basándose en el uso generalizado de la tecnología en diversas áreas de la vida cotidiana, incluso en aspectos que anteriormente se consideraban ajenos a estos ámbitos. Esta interconexión ha vuelto difícil establecer límites claros sobre qué situaciones están relacionadas específicamente con el ciberespacio. Por ejemplo, el uso de redes sociales es un caso que ilustra esta falta de definición, ya que algunas personas lo ven como un tema puramente tecnológico, mientras que otros lo interpretan desde una perspectiva más amplia que abarca temas de índole social, económico, comunicacional, político e incluso de relaciones internacionales, entre otros. Además, los fundamentos tecnológicos que dan lugar al ciberespacio han llevado a incluir cuestiones tecnológicas dentro de este ámbito, especialmente debido a la creciente necesidad de conectividad asociada a todas las tecnologías. (IEEE, 2021)

En la actualidad, el ciberespacio está experimentando la introducción de metaversos, que son entornos virtuales que ofrecen experiencias multidimensionales en diversas áreas como entretenimiento, educación a distancia, salud virtual y, especialmente, en la economía digital. Estos espacios en línea están integrados en el mundo real denominado mundo offline, lo que permite a las personas informarse, interactuar, disfrutar, enfrentar desafíos y consumir

información tanto en Internet como en el Internet de las cosas. Por lo tanto, el análisis social del ciberespacio se centra en el orden social relacionado con la interacción entre las personas y las tecnologías digitales. (Rodríguez et al., 2023)

4.2.2. Evolución e importancia del ciberespacio

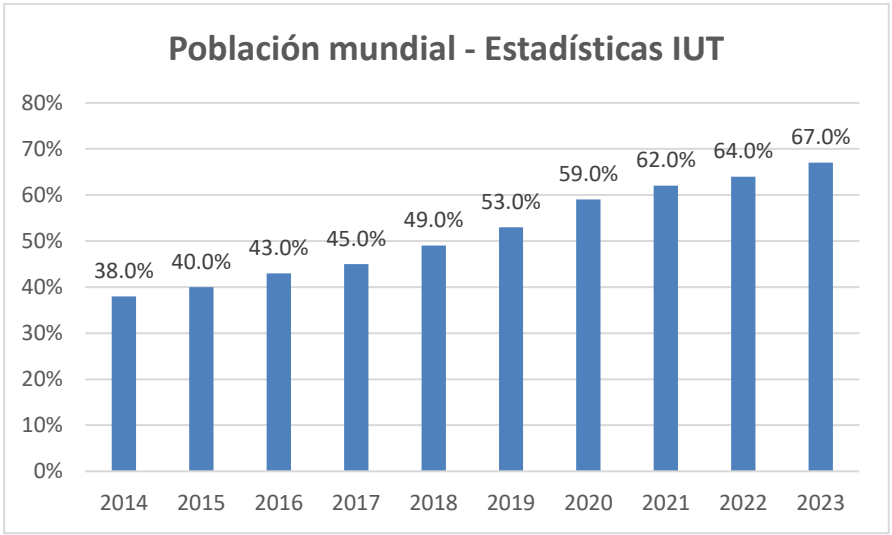
La importancia creciente del ciberespacio en la actualidad se refleja en las cifras más recientes sobre conectividad global. Según estadísticas publicadas en 2023 por la Unión Internacional de Telecomunicaciones (UIT), alrededor de 5 400 millones de personas, es decir, el 67 % de la población mundial, cuentan con acceso a Internet. Si bien esta cifra representa un avance significativo, aún persiste una brecha digital, ya que 2 600 millones de personas, equivalente al 33 %, permanecen desconectadas de este vasto dominio virtual. (*Comunicado de prensa UIT.*, 2023)

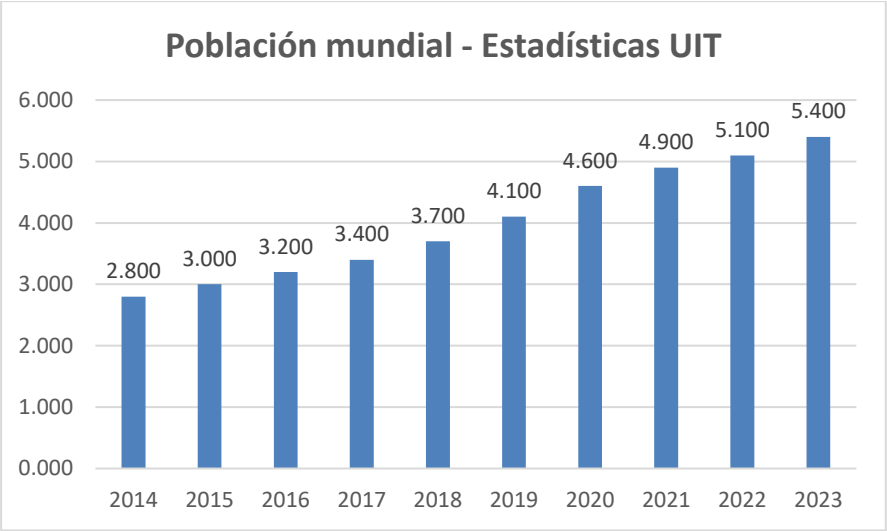
No obstante, al comparar estos datos con los expuestos por el mismo organismo en 2020, cuando se estimaba que 4 600 millones de personas (59 % de la población global) tenían el servicio de acceso a Internet, se evidencia una tendencia de crecimiento en la adopción del servicio de Internet y la infraestructura cibernética a nivel mundial. Esta expansión gradual de nuevos usuarios al ciberespacio resalta su consolidación como una realidad paralela de la vida cotidiana. (*Comunicado de prensa UIT.*, 2021)

En la Figura 2 se muestran los datos estadísticos proporcionados anualmente por la UIT. Estos datos corresponden a los últimos diez años y reflejan la tendencia creciente del acceso mundial a Internet, lo cual se relaciona directamente con un aumento constante en la cantidad de usuarios en el ciberespacio.

Figura 2

Población mundial con acceso a Internet





Fuente: UIT.

Se aprecia un incremento sustancial (6 %) en el acceso a Internet entre los años 2019 y 2020, periodo durante el cual se produjo la pandemia de COVID-19. Esta tendencia demuestra que las restricciones impuestas, como los confinamientos, el teletrabajo obligatorio y la implementación masiva de la educación en línea, provocaron un aumento significativo en la demanda y necesidad de contar con conexión a Internet. Consecuentemente, una mayoría de la población se vio en la necesidad de contratar servicios de acceso a Internet para poder hacer frente a las nuevas realidades y exigencias derivadas de la crisis sanitaria global

A medida que más individuos, comunidades y sectores se suman a la economía y sociedad digitales facilitadas por el ciberespacio, su relevancia se vuelve aún más crítica. Este ámbito virtual transforma áreas tan diversas como el comercio global, las transacciones financieras, los modelos de negocio innovadores, el acceso a la información, la comunicación interpersonal, la expresión creativa y la participación ciudadana en movimientos sociales de alcance mundial.

4.2.3. Particularidades del ciberespacio

El ciberespacio es una realidad paralela al mundo real, brinda una dimensión virtual, descentralizada, transfronteriza y en constante evolución, en la que la percepción del espacio y el tiempo se ve transformada. Los usuarios tienen la oportunidad de preservar el anonimato y gestionar de forma dinámica sus identidades y presencia en línea de manera controlada. Esta capacidad de moldear identidades virtuales volátiles en el entorno cibernético ejerce una influencia directa en las conductas y dinámicas de interacción dentro del mismo.

Tales posibilidades, facilitadas por la convergencia de realidades físicas y virtuales, conllevan la aparición de nuevos riesgos, amenazas asimétricas y desafíos emergentes en materia de privacidad y ciberseguridad. Es por ello que el ciberespacio, como escenario global

sin un punto de control central y con una noción espacial y temporal difusa, se establece como uno de los mayores retos a los que la sociedad moderna debe hacer frente en la era digital, al constituir un ámbito con vulnerabilidades inherentes que requiere soluciones integrales y estrategias sólidas para mitigar sus riesgos y salvaguardar los derechos y la privacidad de los usuarios.

En el siguiente capítulo, se profundizará de manera específica sobre los ciberdelitos en el ciberespacio, enfocándose en el contexto del estado ecuatoriano. Es esencial comprender las particularidades mencionadas anteriormente para realizar un análisis completo. Este análisis detallará el tipo de delito y la pena correspondiente, haciendo referencia al Código Orgánico Integral Penal de Ecuador.

4.2.4. El ciberespacio y el rol de las Redes Sociales

En Ecuador, la Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL) gestiona el Sistema de Información y Estadística de Telecomunicaciones (SIETEL), donde se mantienen y actualizan periódicamente los datos relacionados con los usuarios y servicios de acceso a Internet (SAI), servicios de portador de telecomunicaciones (SPT), y los servicios de audio y video por suscripción (AVS). Considerando el registro correspondiente al último trimestre del año 2023, publicado en enero de 2024, refleja el aumento progresivo de habitantes ecuatorianos con acceso a Internet, quienes son considerados participantes activos del ciberespacio. (SIETEL, 2024)

En la Tabla 1, se muestra el registrado recopilado de la base de datos del SIETEL.

Tabla 1

Población del Ecuador con servicio de acceso a Internet

Año	Población Ecuador SAI (%)	Población Ecuador SAI (N° de habitantes)
2014	39,0 %	6 256 878
2015	44,1 %	7 184 673
2016	56,8 %	9 387 842
2017	63,1 %	10 586 476
2018	66,4 %	11 297 151
2019	66,2 %	11 428 791
2020	68,1 %	11 921 796
2021	71,7 %	12 563 020
2022	74,4 %	13 390 898
2023	78,2 %	14 239 130

Fuente: Base de datos SIETEL.

El Instituto Nacional de Estadísticas y Censos (INEC) de Ecuador, en su presentación de los principales resultados de las estadísticas de Tecnologías de la Información y Comunicación (TIC) realizada en julio de 2023 y basándose en la Encuesta de Empleo, Desempleo y Subempleo (ENEMDU), indica que el uso de Internet en servicios y/o actividades como primera opción está orientado de la siguiente manera: un 79,2 % para comunicaciones y redes sociales, un 9,6 % para actividades de entretenimiento, un 7,7 % para educación y aprendizaje, un 1,8 % por razones laborales, un 1 % para obtención de información, y finalmente, otros propósitos como compra/venta de productos o servicios, almacenamiento en la nube, trámites gubernamentales, banca electrónica o agendado de citas médicas. Estos datos se refieren a la población que dispone del servicio de acceso a Internet. (INEC, 2023)

Como se ha demostrado previamente, el ciberespacio ha experimentado un crecimiento exponencial en los últimos años, convirtiéndose en un entorno virtual donde millones de personas interactúan, se comunican y acceden a una amplia gama de servicios y contenidos. En el caso de Ecuador, los datos reflejados por la Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL) y el Instituto Nacional de Estadísticas y Censos (INEC) muestran una tendencia al alza en el número de usuarios con el servicio de acceso a Internet, lo que implica un aumento en la participación activa en el ciberespacio.

En este sentido, las redes sociales han adquirido un papel fundamental, convirtiéndose en las plataformas más utilizadas para la comunicación y la interacción en línea. Según los datos del INEC, un abrumador 79,2 % de los usuarios de Internet en Ecuador utilizan estas herramientas como su principal actividad en línea. Las redes sociales han revolucionado la forma en que las personas se conectan, comparten información, expresan opiniones y establecen relaciones, trascendiendo barreras geográficas y culturales.

Finalmente, el ciberespacio y las redes sociales han transformado profundamente la forma en cómo nos relacionamos, aprendemos y accedemos a información, brindando oportunidades sin precedentes para la conectividad global. No obstante, también plantean desafíos en términos de privacidad, seguridad y responsabilidad en el uso de estas herramientas, lo que requiere un enfoque equilibrado y consciente por parte de los usuarios y las autoridades reguladoras. (Aparicio-Izurieta, 2022)

4.3.Ciberseguridad

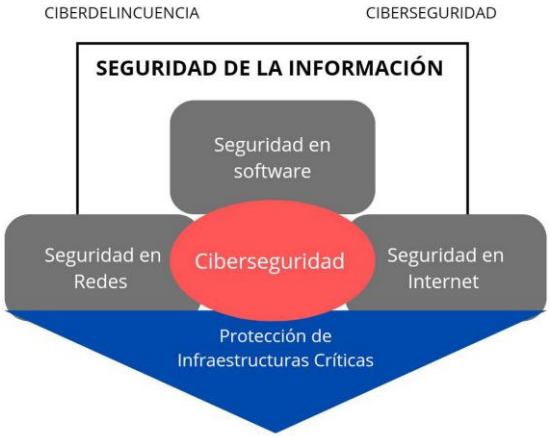
4.3.1. ¿Qué es la ciberseguridad?

Con la creciente dependencia de la tecnología y la interconexión de redes y sistemas a través de Internet, la protección de la información y activos digitales se ha convertido en una

prioridad crítica para países, empresas, organizaciones e individuos por igual. En este sentido, comprender la importancia de la ciberseguridad es fundamental para mitigar riesgos, proteger la privacidad y garantizar el funcionamiento seguro de cada uno de ellos.

Figura 3

La ciberseguridad en la seguridad de la información



Fuente: Autor.

A continuación, se enuncian las definiciones de ciberseguridad proporcionadas por empresas referentes que brindan servicios en esta temática:

IBM define la ciberseguridad como la práctica orientada a proteger los sistemas críticos y la información confidencial frente a ataques digitales. Conocida también como seguridad de la tecnología de la información, estas medidas están diseñadas para hacer frente a las amenazas dirigidas a sistemas en red y aplicaciones, las cuales pueden surgir tanto desde el interior como desde el exterior de una organización. (IBM, 2023)

Por su parte, CISCO define la ciberseguridad como la práctica dedicada a proteger sistemas, redes y programas de ataques digitales. Estos ataques suelen tener como objetivo acceder, modificar o destruir información confidencial, extorsionar a usuarios o interrumpir la continuidad de un servicio o negocio. La creciente implementación de medidas de seguridad digital se debe al hecho de que existen más dispositivos conectados que personas, y los atacantes están desarrollando cada vez métodos más creativos para llevar a cabo sus acciones. (CISCO, 2023)

Finalmente, Kaspersky define la ciberseguridad como la práctica destinada a proteger las computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos contra ataques maliciosos. También conocida como seguridad de la tecnología de la información o seguridad de la información electrónica, este término abarca una amplia gama de contextos, desde entornos empresariales hasta la informática móvil. (Kaspersky, 2023)

A partir de estas definiciones podríamos concluir que la ciberseguridad es un concepto fundamental en la era digital actual, donde la interconexión y la dependencia de la tecnología están en aumento. Las definiciones proporcionadas por las empresas líderes en el campo resaltan la importancia de proteger los sistemas, redes, información y activos digitales contra ataques maliciosos, amenazas internas y externas, y desarrollar prácticas y medidas de seguridad adecuadas para mitigar los riesgos y garantizar la continuidad de las operaciones de manera segura.

La creciente relevancia de la ciberseguridad no solo se limita al ámbito empresarial, sino que también se ha convertido en una prioridad para los gobiernos alrededor del mundo. Los ciberataques representan una amenaza significativa para la seguridad nacional, las infraestructuras críticas y la privacidad de los ciudadanos. Por esta razón, los países están invirtiendo recursos considerables en desarrollar estrategias nacionales de ciberseguridad, fortalecer sus capacidades de ciberdefensa y promulgar leyes y regulaciones para proteger el ciberespacio. La cooperación internacional también es clave, ya que los ciberataques no reconocen fronteras. Los gobiernos buscan establecer alianzas y mecanismos de coordinación para enfrentar de manera conjunta estas amenazas globales y salvaguardar la integridad de sus sistemas y datos sensibles

4.3.2. Organismos públicos de ciberseguridad en el Ecuador

En Ecuador, existen dos organismos encargados del análisis y tratamiento de los ciberdelitos, los cuales son: La Unidad de Ciberdelito y la Unidad Nacional Especializada en Investigación de Ciberdelito. Ambas entidades desempeñan un papel crucial en la lucha contra los delitos informáticos que han ido en aumento en los últimos años, a medida que la tecnología y el uso del ciberespacio se han vuelto más omnipresentes en la sociedad ecuatoriana.

La Unidad de Ciberdelito de la Policía Nacional del Ecuador es una división especializada que forma parte de la Dirección Nacional de Delitos Contra la Propiedad, y su labor se enfoca en la investigación y el procesamiento de casos relacionados con delitos informáticos, tales como el fraude electrónico, el acceso no autorizado a sistemas informáticos, la difusión de material ilegal en línea, entre otros. Esta unidad cuenta con personal altamente capacitado en ciberseguridad y técnicas forenses digitales, lo que les permite recopilar y analizar pruebas electrónicas de manera efectiva.

Por otro lado, la Unidad Nacional Especializada en Investigación de Ciberdelito pertenece a la Fiscalía General del Estado y se encarga de llevar a cabo las investigaciones preliminares y formular cargos en casos relacionados con delitos cibernéticos. Esta unidad trabaja en estrecha colaboración con la Unidad de Ciberdelito de la Policía Nacional,

compartiendo información y coordinando esfuerzos para abordar de manera integral los casos de ciberdelitos.

Ambas instituciones son fundamentales para garantizar la seguridad en el ciberespacio ecuatoriano, protegiendo a ciudadanos, empresas e instituciones de amenazas digitales que pueden comprometer su privacidad, información confidencial y recursos financieros. Su labor es especialmente relevante en un mundo cada vez más interconectado, donde la dependencia de las tecnologías de la información y la comunicación es creciente

4.3.3. Ciberdelitos en el Ecuador

Los ciberdelitos, también conocidos como delitos cibernéticos, se refieren de manera general a toda actividad ilícita que se lleva a cabo utilizando computadoras, sistemas informáticos u otros dispositivos de comunicación electrónicos. Estos delitos tienen como objetivo principal el robo o adulteración de información, el robo de credenciales digitales, daño o interrupción de servicios, fraudes financieros, la difusión de pornografía infantil, entre otros actos ilícitos realizados en el ciberespacio.

Desde el ámbito jurídico, los delitos informáticos se definen como conductas tipificadas, antijurídicas y culpables que implican el uso de medios tecnológicos para vulnerar o poner en riesgo la seguridad informática. Estas acciones delictivas atentan contra los principios fundamentales considerados en la triada de la seguridad informática. (FGE-Ecuador, 2021)

En este contexto, en el Ecuador, el Código Orgánico Integral Penal (COIP) contempla y establece sanciones para los ciberdelitos de acuerdo con las siguientes tipificaciones:

Pornografía infantil.

- Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.

Pena privativa: 13 a 16 años.

Si la víctima sufre discapacidad o enfermedad grave o incurable.

Pena privativa: 16 a 19 años.

Si la víctima sufre discapacidad o enfermedad grave o incurable.

Pena privativa: 16 a 19 años.

Si la persona infractora es familiar o cercana a la víctima.

Pena privativa: 22 a 26 años.

- Art. 104.- Comercialización de pornografía con utilización de niñas, niños o adolescentes.

Pena privativa: 10 a 13 años.

Instigación al suicidio a través de medios digitales o electrónicos.

- Art. 154.1.- Instigación al suicidio.

Pena privativa: 1 a 3 años

Hostigamiento usando medios tecnológicos o digitales.

- Art. 154.2.- Hostigamiento

Pena privativa: 6 meses a 1 año.

Si la víctima es menor de edad, sufre discapacidad no puede comprender el significado del acto.

Pena privativa: 1 a 3 años.

Ciberacoso sexual.

- Art. 166.-Acoso sexual.

Pena privativa: 1 a 5 años.

Si la víctima es menor de edad, sufre discapacidad no puede comprender el significado del acto.

Pena privativa: 3 a 5 años

Gromming.

- Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.

Pena privativa: 1 a 3 años.

Si el acercamiento es por intimidación o coacción.

Pena privativa: 3 a 5 años.

Si el infractor suplanta la identidad de un tercero mediante medios electrónicos y si la víctima es menor de edad y sufre discapacidad.

Pena privativa: 3 a 5 años.

Sexting u oferta de servicios sexuales en medios electrónicos.

- Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos

Pena privativa: 7 a 10 años.

Delitos contra la intimidad personal.

- Art. 178.- Violación a la intimidad.

Pena privativa: 1 a 3 años.

Revelación de información personal.

- Art. 179.- Revelación de secreto o información personal de terceros.

Pena privativa: 1 a 3 años.

Defraude tecnológicos o electrónicos.

- Art. 186.- Estafa.

Pena privativa: 5 a 7 años.

Si los perjudicados son mayor a dos personas o el delito se comete a través de una institución del Sistema Financiero Nacional.

Pena privativa: 7 a 10 años.

Aprovechamiento o prestación ilícita de servicios de TICs.

- Art. 188.- Aprovechamiento ilícito de servicios públicos

Aprovechamiento ilícito:

Pena privativa: 6 meses a 2 años.

Prestación ilícita:

Pena privativa: 1 a 3 años.

Apropiación fraudulenta.

- Art. 190.- Apropiación fraudulenta por medios electrónicos.

Pena privativa: 1 a 3 años.

Delitos referentes a terminales móviles y su información de identificación.

- Art. 191.- Reprogramación o modificación de información de equipos terminales móviles.

Pena privativa: 1 a 3 años.

- Art. 192.- Intercambio, comercialización o compra de información de equipos terminales móviles.

Pena privativa: 1 a 3 años.

- Art. 193.- Reemplazo de identificación de terminales móviles.

Pena privativa: 1 a 3 años.

- Art. 194.- Comercialización ilícita de terminales móviles.

Pena privativa: 1 a 3 años.

- Art. 195.- Infraestructura ilícita.

Pena privativa: 1 a 3 años.

Violación de la propiedad intelectual y derechos de autor.

- Art. 208A.- Actos lesivos a la propiedad intelectual.

Pena privativa: 6 meses a 1 año.

Multa: 8 a 300 salarios básicos unificados.

- Art. 208B.- Actos lesivos a los derechos de autor.

Pena privativa: 1 a 3 años.

Multa: 8 a 300 salarios básicos unificados.

Delitos contra la identidad.

- Art. 211.- Supresión, alteración o suposición de la identidad y estado civil.

Pena privativa: 1 a 3 años.

- Art. 212.- Suplantación de identidad.

Pena privativa: 1 a 3 años.

Revelación ilegal de información de base de datos.

- Art. 229.- Revelación ilegal de base de datos.

Pena privativa: 1 a 3 años.

Si son realizados por servidores públicos, empleados o encargados de las bases de datos de la misma organización.

Pena privativa: 3 a 5 años.

Pharming y Phishing de información.

- Art. 230.- Interceptación ilegal de datos.

Pena privativa: 3 a 5 años.

Fraudes informáticos.

- Art. 231.- Transferencia electrónica de activo patrimonial.

Pena privativa: 3 a 5 años.

Daños informáticos, malware, ataques DoS y DDoS.

- Art. 232.- Ataque a la integridad de sistemas informáticos.

Diseño, venta y distribución de malware.

Destrucción de infraestructura física.

Pena privativa: 3 a 5 años.

Destrucción de bienes informáticos destinados a servicios públicos o vinculados a la seguridad ciudadana.

Pena privativa: 5 a 7 años

Exposición de información pública reservada.

- Art. 233.- Delitos contra la información pública reservada legalmente.

Pena privativa: 5 a 7 años.

Si son realizados por servidores públicos.

Pena privativa: 3 a 5 años.

Si la información pueda comprometer gravemente la seguridad del estado.

Pena privativa: 7 a 10 años.

Accesos no autorizados.

- Art. 234.- Acceso no consentido a un sistema informático, telemático o e telecomunicaciones.
- Art. 234.1.- Falsificación informática.

Pena privativa: 3 a 5 años.

- Art. 234.2.- Agravación de las penas.

Si existe afectación grave o duradera a un sistema informático que sea destinado a servicios públicos o funciones sociales críticas.

Pena privativa: Pena agravada en un tercio de la pena máxima.

Delitos de terrorismo.

- Art. 366.- Terrorismo.

Pena privativa: 10 a 13 años.

4.3.4. Estrategias de defensa y protección

La Policía Nacional del Ecuador, en uno de sus boletines informativos sobre ciberseguridad, ofrece las siguientes recomendaciones para que la ciudadanía se mantenga alerta, ya que los ciberatacantes emplean diversas estrategias para acceder a redes y dispositivos, así como para extorsionar o robar información valiosa: (Policía Nacional del Ecuador, 2020)

Mantener cautela ante mensajes no solicitados: Si se tiene desconfianza del remitente, es recomendable abstenerse de abrir el mensaje. En caso de que resulte sospechoso, se aconseja eliminarlo de inmediato.

Ejercer discreción al proporcionar información: Si los usuarios no divulgan voluntariamente datos personales o información, se reduce la efectividad del phishing como estafa.

Evitar la exposición del correo institucional en foros o redes sociales: Los spambots, conocidos como "cazacorreos", rastrean páginas web y plataformas sociales en busca de direcciones de correo electrónico.

Ser cauteloso con ofertas gratuitas: La premisa "si parece demasiado bueno para ser verdad, probablemente no lo sea" aplica para prevenir estafas. Antes de realizar compras en línea, se sugiere investigar el dominio para mitigar riesgos.

No compartir cadenas de mensajes: Evitar reenviar mensajes que solicitan reenvíos para alcanzar un objetivo, ya que esto expone las direcciones de contactos a spam adicional.

Mantener el navegador actualizado y aplicar parches de seguridad regularmente en el ordenador.

No responder a correos de spam: Responder a este tipo de correos solo confirma la validez de la dirección de correo, fomentando más spam.

Utilizar el sistema antispam para marcar como SPAM los mensajes considerados como tal, contribuyendo así a mejorar el filtrado.

Limitar el uso de la cuenta de correo institucional exclusivamente para fines laborales.

Emplear contraseñas robustas y cambiarlas periódicamente.

Evitar la instalación de software de fuentes desconocidas, ya que las descargas desde la web pueden representar un riesgo de infección para el equipo.

Utilizar conexiones WiFi seguras: Las redes WiFi públicas y gratuitas son objetivos comunes para ataques, por lo que se recomienda utilizar redes seguras y protegidas.

En conclusión, la Policía Nacional del Ecuador busca concienciar a la ciudadanía sobre la importancia de mantenerse alerta frente a las diversas estrategias de ciberataque, recomendando precaución al abrir mensajes no solicitados, ser prudente al compartir información personal, evitar la exposición del correo institucional en redes sociales, ser cauteloso con ofertas sospechosamente buenas, no reenviar cadenas de mensajes, mantener actualizado el navegador y aplicar parches de seguridad, no responder a correos de spam, utilizar sistemas antispam, limitar el uso de correo institucional, emplear contraseñas robustas y cambiarlas periódicamente, evitar la instalación de software desconocido, y utilizar conexiones WiFi seguras para protegerse de posibles ataques cibernéticos y preservar la seguridad de sus dispositivos y datos.

4.3.5. Estándares de ciberseguridad internacionales.

Los estándares de ciberseguridad son recomendaciones técnicas establecidas en documentación publicada a nivel mundial, para establecer la protección del entorno cibernético, abarcando a los usuarios, redes, dispositivos, software, procesos, información almacenada o en tránsito, aplicaciones, servicios y sistemas conectados directa o indirectamente a las redes. El objetivo principal de estos estándares es reducir los riesgos, incluyendo la prevención o mitigación de ciberataques.

En el ámbito de la ciberseguridad, existen varios estándares y marcos de referencia ampliamente reconocidos y utilizados. Estos estándares son fundamentales para establecer prácticas de seguridad efectivas y garantizar la protección integral de la información y los sistemas en entornos digitales.

Algunos de los estándares más relevantes y ampliamente adoptados en el campo de la ciberseguridad incluyen:

- ISO/IEC 27001: Sistemas de Gestión de Seguridad de la Información (SGSI): Proporciona requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI, ayudando a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información, y siendo ampliamente utilizado como marco de referencia para la implementación de controles de seguridad.
- NIST Cybersecurity Framework (NIST CSF): Desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, el cual proporciona un enfoque estandarizado para identificar, evaluar y gestionar el riesgo cibernético, constando de cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperar. Este marco de trabajo es ampliamente adoptado a nivel global como guía de buenas prácticas en ciberseguridad. Estos estándares son fundamentales para establecer prácticas de seguridad efectivas y garantizar la protección integral de la información y los sistemas en entornos digitales.
- ISO/IEC 27032: Directrices para la ciberseguridad, proporciona lineamientos para abordar la ciberseguridad y su interacción con áreas como la seguridad de la información, seguridad de redes y seguridad de Internet, ayudando a las organizaciones a comprender y abordar los desafíos de la ciberseguridad de manera efectiva.
- PCI DSS (Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago): Establece requisitos de seguridad para las organizaciones que procesan, almacenan o transmiten datos de tarjetas de crédito, con el objetivo de proteger a los consumidores contra el fraude y el robo de datos de tarjetas, siendo obligatorio para cualquier empresa que acepte pagos con tarjeta de crédito. Estos estándares son fundamentales para establecer prácticas de seguridad efectivas y garantizar la protección integral de la información y los sistemas en entornos digitales.
- COBIT (Control Objectives for Information and Related Technology): Proporciona un enfoque integral para las organizaciones y la gestión de las tecnologías de la información, abarcando aspectos como la alineación estratégica, la entrega de valor, la gestión de riesgos y el desempeño. Estos estándares son fundamentales para establecer prácticas de seguridad efectivas y garantizar la protección integral de la información y los sistemas en entornos digitales.

Estos estándares proporcionan lineamientos, requisitos y las mejores prácticas que las organizaciones y usuarios de Internet pueden adoptar para fortalecer su postura de seguridad y hacer frente de manera efectiva a los desafíos y amenazas en el ciberespacio.

4.4.Ingeniería social

4.4.1. Definición

La ingeniería social es el arte de la manipulación psicológica y la explotación de la confianza de las personas para la obtención de información confidencial o la ejecución de acciones no autorizadas. Los ciberdelincuentes en lugar de descubrir y explotar posibles vulnerabilidades tecnológicas, emplean este arte para aprovecharse de las debilidades humanas como los sentimientos y la confianza para obtener información o datos relevantes de personas declaradas como objetivo de ataque. (Salahdine & Kaabouch, 2019M; Chetioui et al., 2022)

El crecimiento del Internet y los avances tecnológicos han facilitado la comunicación e interacción entre seres humanos, volviéndola fácil e instantánea. Sin embargo, esta conveniencia también ha expuesto la información personal y sensible de cada usuario en la red, especialmente a través de las redes sociales. Lamentablemente, estas plataformas no siempre mantienen un nivel adecuado de seguridad, convirtiendo la información en un objetivo de gran interés para los ciberdelincuentes. (Ariza et al., 2023; Albladi & Weir, 2016)

4.4.2. Ciclo de vida típico de un ataque de ingeniería social

Los ataques de ingeniería social buscan establecer una conexión entre el atacante y la víctima, en donde el atacante intenta manipular a la víctima para que le entregue información sensible y se comprometa. (Chetioui et al., 2022; Gallegos-Segovia et al., 2017)

En la Figura 4 se muestra el ciclo de vida típico de un ataque de ingeniería social.

Figura 4

Basado en (Chetioui et al., 2022)

El ciclo de vida típico de un ataque ingeniería social está conformado por diversas etapas estratégicamente planificadas:

Definición: Es la etapa inicial, el atacante selecciona a la víctima, determina el objetivo del ataque y elabora un plan de ataque detallado.

Investigación: Siguiendo al plan establecido, el atacante estudia a su víctima con el fin de identificar posibles lazos de conexión y puntos de vulnerabilidad.

Enganche: Una vez recopilada la información necesaria, el atacante se acerca a su víctima, tratando de establecer una conexión y trabajando para ganarse su confianza de manera efectiva.

Juego: Con la confianza de la víctima asegurada, el atacante la manipula hábilmente hasta la consecución del objeto del ataque.

Salida: Finalmente, una vez logrado el objetivo del ataque, el atacante se retira, desapareciendo de la escena sin dejar rastro.

Este ciclo demuestra cómo la ingeniería social implica un proceso cuidadosamente planificado que abarca desde la selección de la víctima hasta la exitosa consecución del objetivo del atacante.

4.4.3. Perfiles y comportamiento de riesgo en redes sociales

En la actualidad, como se mencionó anteriormente, los ciberdelincuentes utilizan la información que la ciudadanía en general comparte en Internet con el objeto de explotarla para su propio beneficio.

Los profesionales en áreas como la ingeniería, la medicina, el derecho, el comercio y las artes son objetivos principales para los ciberdelincuentes, quienes buscan extorsionarlos haciendo uso de la información y servicios que prestan y publican en Internet, especialmente en sus redes sociales. (Diario La Hora, 2022)

A partir de la pandemia del 2020, hubo un aumento progresivo en la participación de los adultos mayores en Internet, convirtiéndolos en los nuevos migrantes digitales en el ciberespacio. Lamentablemente, este grupo social corre el riesgo de convertirse en uno de los blancos principales de los ciberdelincuentes, ya que su falta de conocimiento y exceso de confianza pueden llevarlos a relacionarse con perfiles, entablar charlas y desarrollar sentimientos hacia usuarios cuyos perfiles no siempre son reales o que están suplantando la identidad de otras personas o usuarios, muchos de ellos familiares lejanos o que viven en otro país. (Sadvisor, 2022)

A pesar de tener acceso limitado a los servicios de Internet, los adolescentes en Ecuador son víctimas del acoso cibernético o ciberbullying. Esta situación se da debido a que los

adolescentes son un grupo vulnerable y suelen tener una presencia activa y participativa en las redes sociales, compartiendo información personal que puede ser utilizada en su contra por los acosadores. Además, la falta de supervisión parental y el desconocimiento de los riesgos en línea contribuyen a que sean blancos fáciles para el ciberbullying. (El Comercio, 2019)

Uno de los principales motivos por los cuales los adolescentes son víctimas de ciberataques es la falta de educación digital. El conocimiento del manejo de redes sociales y tecnologías digitales por parte de los adolescentes se encuentra por debajo de lo adecuado, revelando vulnerabilidades frente a ciberataques o robo de información. Una de las situaciones más claras y peligrosas es el uso descuidado de conexiones a redes inalámbricas gratuitas para acceder a Internet. Los adolescentes carecen del conocimiento necesario sobre la fiabilidad y seguridad de dichas redes, lo que los expone a diversos riesgos presentes en el ciberespacio. (Cánovas, José, s. f.)

Independientemente de la edad, el riesgo de ser víctima de ciberataques es constante. Diversos factores contribuyen a esta vulnerabilidad, como la sobreexposición de información personal, la interacción y exceso de confianza con extraños en línea, y el desconocimiento en el manejo de la privacidad en las redes sociales. Además, existe un descuido por parte de los adultos, quienes permiten que los niños accedan a Internet sin ningún tipo de supervisión, a pesar de que existen restricciones de edad para acceder a determinadas plataformas.

En este contexto, la educación sobre el uso seguro de las redes sociales es fundamental para disminuir los riesgos de ciberataques y fomentar una cultura digital responsable. Tanto niños como adultos deben recibir capacitación en temas como privacidad, seguridad en línea y manejo adecuado de la información personal, con el fin de reducir significativamente los peligros asociados a los ciberataques.

4.4.4. Ciberataques basados en ingeniería social

Existen diferentes tipos de ciberataques basados en ingeniería social, a continuación, se analizarán los más utilizados y se presentarán ejemplos de su aplicación:

Malware: Es un término que se usa para describir cualquier tipo de software malicioso, como spyware, ransomware, virus y gusanos. Este tipo de programas dañinos se infiltran en las redes, generalmente cuando un usuario hace click en enlaces o archivos adjuntos procedentes de correos electrónicos, mensajes de texto o redes sociales que no son de confianza. (CISCO, s. f.)

El malware puede llegar a bloquear el acceso a componentes clave de la red, llegando incluso a volver inoperativo el equipo afectado. Por lo tanto, los usuarios deben mantener una

actitud cautelosa al interactuar con contenidos de procedencia desconocida, ya que esto puede derivar en la infección del sistema.

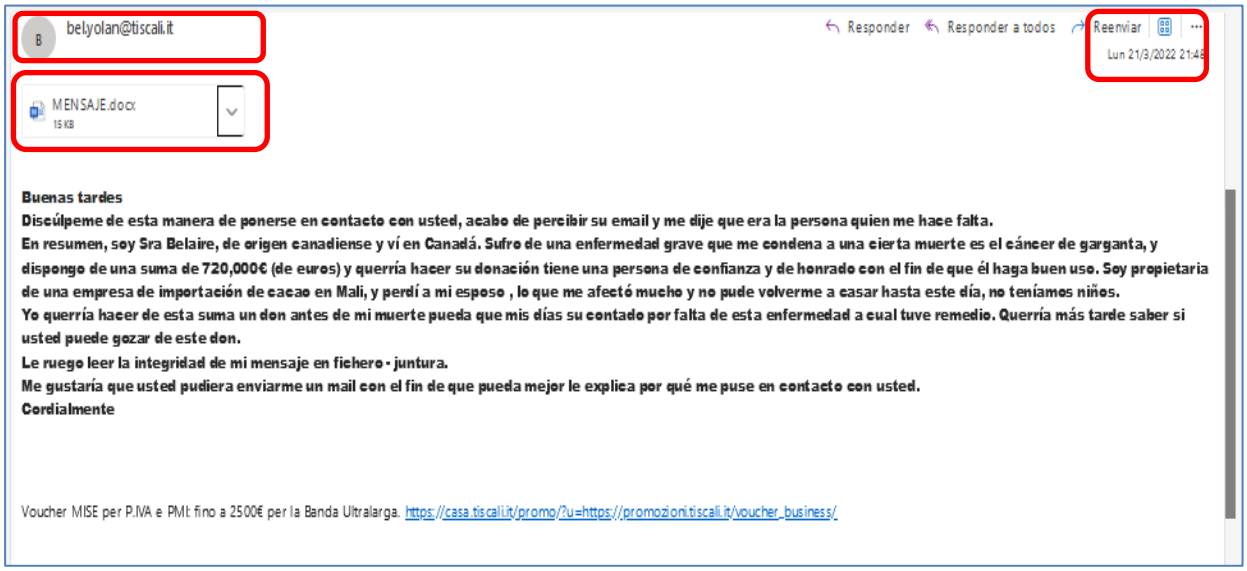
Figura 5

Ejemplo 1 de malware

Fuente: Autor.

Figura 6

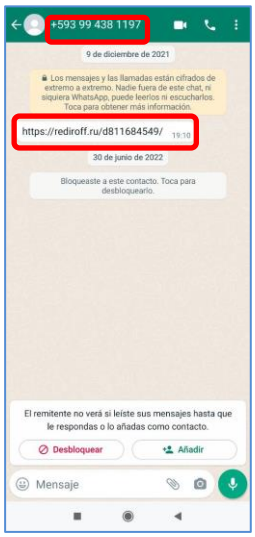
Ejemplo 2 de malware



Fuente: Autor.

Figura 7

Ejemplo 3 de malware



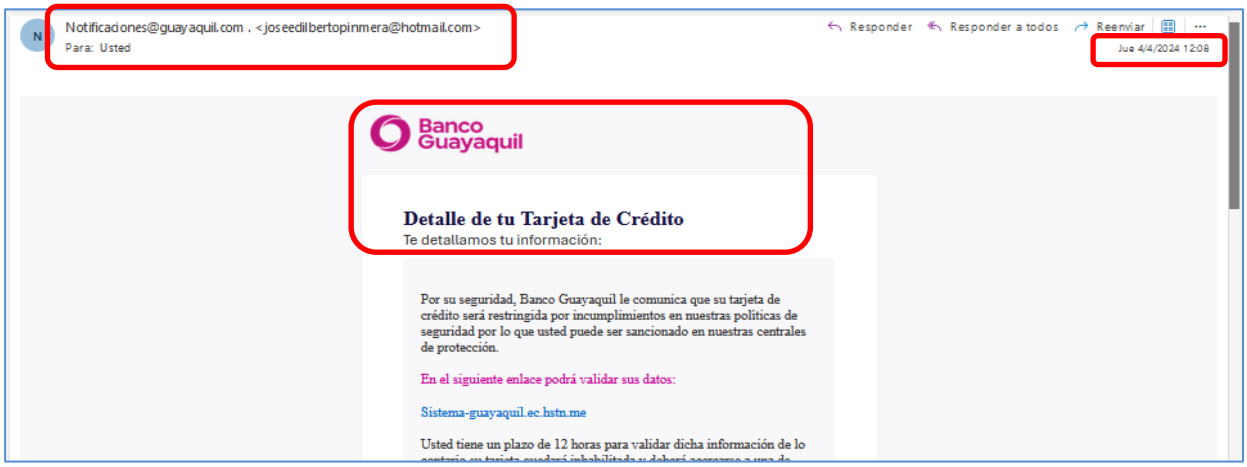
Fuente: Autor.

Phishing: Es una práctica fraudulenta que consiste en el envío de comunicaciones que aparentan provenir de fuentes confiables, generalmente a través de correos electrónicos. El objetivo principal de estos ataques es robar datos sensibles de los usuarios, como credenciales de inicio de sesión y números de tarjetas de crédito. Adicionalmente, los ataques de phishing también pueden tener como fin la instalación de malware en los dispositivos de las víctimas. (CISCO, s. f.)

Este tipo de engaños se aprovecha de la confianza de los usuarios en marcas y entidades conocidas para obtener información confidencial o acceder de manera no autorizada a sistemas y cuentas. Por lo tanto, es crucial que los usuarios mantengan una actitud crítica y desconfíen de cualquier comunicación sospechosa, incluso si parece provenir de fuentes aparentemente legítimas.

Figura 8

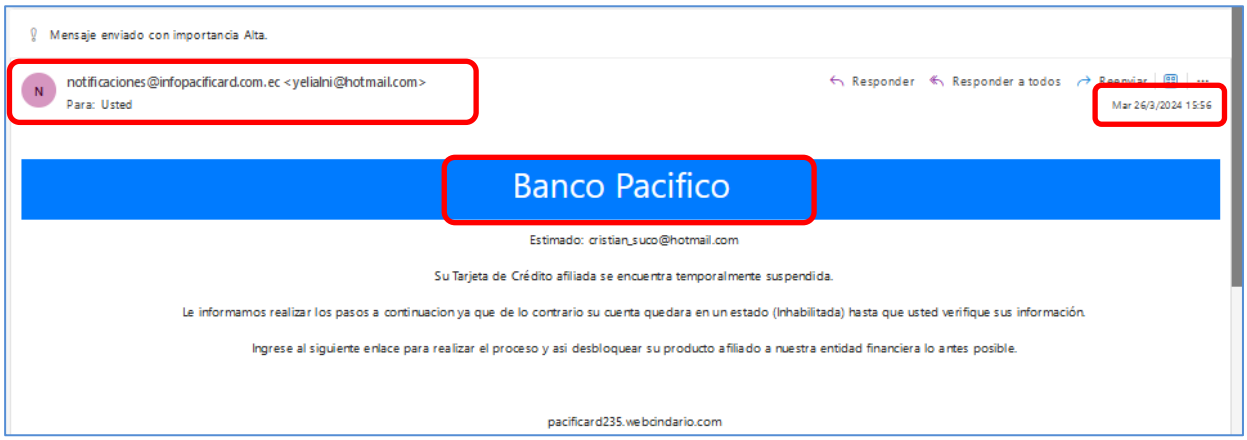
Ejemplo 1 de phishing



Fuente: Autor

Figura 9

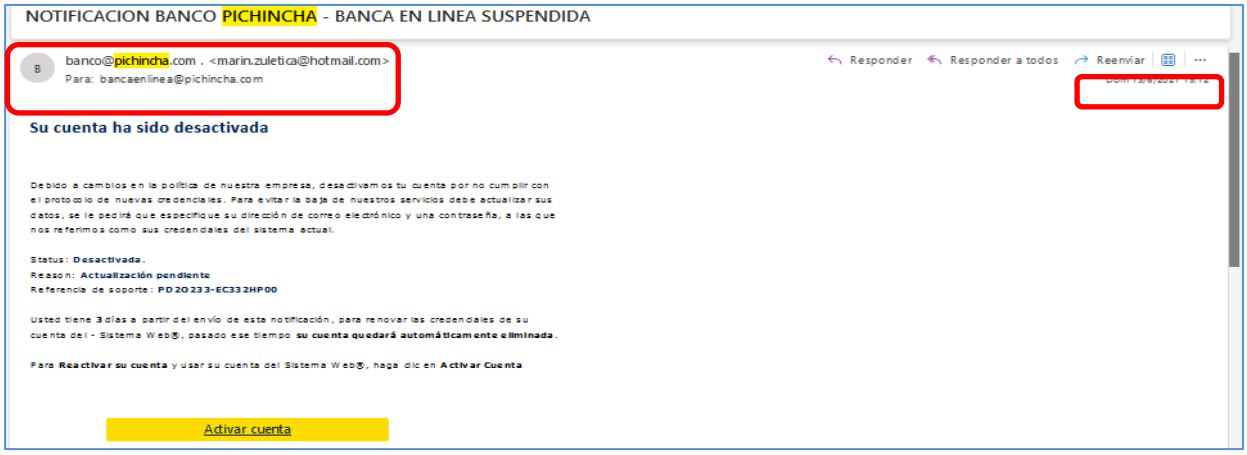
Ejemplo 2 de phishing



Fuente: Autor.

Figura 10

Ejemplo 3 de phishing

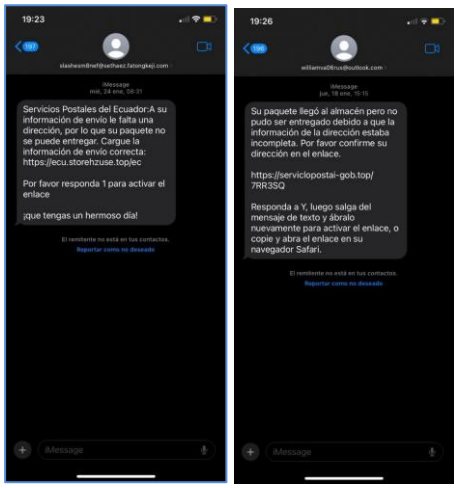


Fuente: Autor

Smishing: Al igual que en los ataques de phishing, el objetivo del smishing es engañar a los usuarios para que revelen información confidencial o caigan en la instalación de malware. Estos mensajes de texto a menudo incluyen sistemas automatizados de respuesta que intentan persuadir a la víctima a que proporcione datos sensibles de manera inmediata.

Figura 11

Ejemplo de smishing



Fuente: Autor.

Grooming: Consiste en un proceso en el cual el abusador emplea una serie de tácticas y engaños para lograr un acercamiento con el menor, ganarse su confianza, y finalmente conseguir un encuentro físico con el objetivo de cometer abusos de naturaleza sexual. Este es un mecanismo sumamente dañino y manipulador que explota la vulnerabilidad de los niños y adolescentes. Implica un abuso de poder, confianza y autoridad por parte del depredador, quien utiliza trucos y mentiras para satisfacer sus propios intereses perversos. (FGE-Ecuador, 2020)

Ejemplo: En mayo de 2022, después de seis meses de investigaciones, impulsados por la Fiscalía General del Estado ecuatoriano, se logró identificar al sujeto que se hacía pasar por mujer para obtener las fotografías de una menor de edad, quien denunció que el hombre la amenazaba sino enviaba dichas imágenes. En el celular del implicado se encontró material pornográfico. (FGE-Ecuador, 2022)

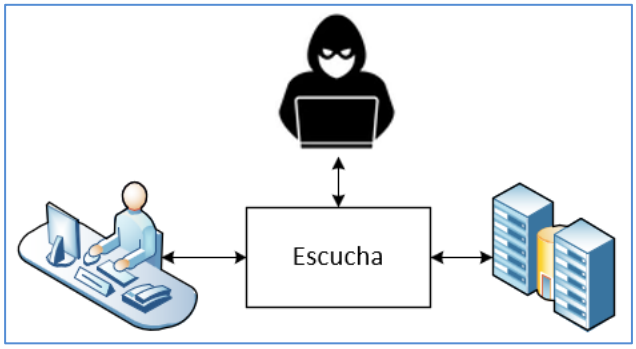
Ataque de intermediario: Los ataques de intermediario, también conocidos como ataques de escucha (man-in-the-middle), ocurren cuando los ciberdelincuentes se insertan en las transacciones que se llevan a cabo entre dos partes. Una vez que los atacantes logran interrumpir el tráfico de comunicación, pueden filtrar los datos de interés y proceder a robarlos. (CISCO, s. f.)

Este tipo de ataques se aprovecha de la confianza entre las partes que participan en la comunicación o transacción. Al posicionarse en el medio, los delincuentes pueden interceptar

y manipular la información que se transmite, comprometiendo así la confidencialidad y la integridad de los datos.

Figura 12

Ejemplo de ataque de intermediario



Fuente: Autor.

Ataque de denegación de servicio (DoS): Tienen como objetivo saturar los sistemas, servidores o redes con un tráfico excesivo, con el fin de agotar los recursos y el ancho de banda disponibles. Como resultado de esta sobrecarga, el sistema no puede completar las solicitudes legítimas de los usuarios. Estos ataques representan una amenaza significativa, ya que pueden interrumpir el funcionamiento normal de sitios web, aplicaciones y servicios en línea, impactando gravemente la disponibilidad y accesibilidad para los usuarios legítimos. (CISCO, s. f.)

En algunos casos, los atacantes utilizan múltiples dispositivos comprometidos, formando una red de equipos infectados conocida como botnet, para lanzar estos ataques de denegación de servicio a gran escala. Al emplear una gran cantidad de fuentes de tráfico malicioso, los ciberdelincuentes logran abrumar y colapsar los sistemas y servicios afectados.

Ejemplo: En octubre de 2021, el Banco de Pichincha, una importante institución financiera ecuatoriana, sufrió un ciberataque que impactó negativamente en parte de sus servicios. Como consecuencia del ataque, la página web del banco quedó inhabilitada temporalmente. (Juan Harán, 2021)

4.4.5. Estadísticas en Ecuador y la provincia de Loja.

A continuación, se presenta la información proporcionada por la Dirección de Estadística y Sistemas de Información de la Fiscalía General del Estado, referente a las Noticias del Delito (NDDs) a nivel nacional y local, relacionadas con ciberdelitos en Ecuador. El periodo analizado se comprende desde enero de 2023 hasta marzo de 2024.

En la Tabla 2 se visualiza el número total de denuncias por cada una de las veinticuatro provincias que conforman al Ecuador, son un total de cincuenta mil trescientas sesenta y cuatro (50 364) denuncias en los quince meses analizados.

Tabla 2

Noticias del delito por año de registro, escala nacional

Provincia de incidente	Total 2023	Total Ene-Mar 2024	Total NDDs	Porcentajes
PICHINCHA	13 565	3 365	16 930	33.62 %
GUAYAS	9 329	2 292	11 621	23.07 %
MANABI	2 267	587	2 854	5.67 %
AZUAY	1 894	497	2 391	4.75 %
EL ORO	1 435	435	1 870	3.71 %
IMBABURA	1 398	330	1 728	3.43 %
CHIMBORAZO	1 217	346	1 563	3.10 %
LOJA	1 115	280	1 395	2.77 %
TUNGURAHUA	1 116	237	1 353	2.69 %
SANTO DOMINGO DE LOS TSACHILAS	981	268	1 249	2.48 %
LOS RIOS	788	219	1 007	2.00 %
COTOPAXI	740	171	911	1.81 %
ESMERALDAS	642	152	794	1.58 %
SANTA ELENA	549	136	685	1.36 %
SUCUMBIOS	499	142	641	1.27 %
CANAR	491	135	626	1.24 %
ORELLANA	400	112	512	1.02 %
CARCHI	359	94	453	0.90 %
BOLIVAR	324	74	398	0.79 %
MORONA SANTIAGO	298	56	354	0.70 %
PASTAZA	251	74	325	0.65 %
NAPO	257	55	312	0.62 %
ZAMORA CHINCHIPE	190	67	257	0.51 %
GALAPAGOS	99	36	135	0.27 %
Total Noticias Del Delito:	**40 204**	**10 160**	**50 364**	**100 %**

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) – Analítica FGE.

Se evidencia que las provincias con la mayor cantidad de denuncias son Pichincha y Guayas, las cuales representan conjuntamente el 56.69 % del total. Por otro lado, en el extremo opuesto se encuentran Zamora Chinchipe y Galápagos, con una suma que equivale al 0.78 % del total. Loja se ubica en el octavo lugar, con el 2.77 %, equivalente a 1 395 denuncias.

De manera específica, en la Tabla 2, se puede observar las noticias del delito de tipo penal registradas en el periodo analizado a escala nacional

Tabla 3

Noticias del delito por año de registro, según el tipo penal a escala nacional

Noticias Del Delito de tipo penal	Total 2023	Total Ene-Mar 2024	Total NDDs	Porcentajes
ESTAFA	24 312	5 988	30 300	60.16 %
SUPLANTACIÓN DE IDENTIDAD	6 478	1 450	7 928	15.74 %
APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS	3 448	874	4 322	8.58 %
VIOLACIÓN A LA INTIMIDAD	1 684	445	2 129	4.23 %
ACOSO SEXUAL	1 640	371	2 011	3.99 %
HOSTIGAMIENTO	744	225	969	1.92 %
ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTICO, TELEMÁTICO O DE TELECOMUNICACIONES	488	194	682	1.35 %
TERRORISMO	255	302	557	1.11 %
ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS	174	55	229	0.45 %
CONTACTO CON FINALIDAD SEXUAL CON MENORES DE DIECIOCHO AÑOS POR MEDIOS ELECTRÓNICOS	174	42	216	0.43 %
TRANSFERENCIA ELECTRÓNICA DE ACTIVO PATRIMONIAL	163	52	215	0.43 %
PORNOGRAFÍA CON UTILIZACIÓN DE NIÑAS, NIÑOS O ADOLESCENTES	141	31	172	0.34 %
ACTOS LESIVOS A LA PROPIEDAD INTELECTUAL	134	25	159	0.32 %
APROVECHAMIENTO ILÍCITO DE SERVICIOS PÚBLICOS	102	17	119	0.24 %

FALSIFICACIÓN INFORMÁTICA	67	36	103	0.20 %
INTERCEPTACIÓN ILEGAL DE DATOS	61	21	82	0.16 %
COMERCIALIZACIÓN ILÍCITA DE TERMINALES MÓVILES	33	7	40	0.08 %
REVELACIÓN ILEGAL DE BASE DE DATOS	29	11	40	0.08 %
REVELACIÓN DE SECRETO O INFORMACIÓN PERSONAL DE TERCEROS	11	8	19	0.04 %
INSTIGACIÓN AL SUICIDIO	16	2	18	0.04 %
OFERTA DE SERVICIOS SEXUALES CON MENORES DE DIECIOCHO AÑOS POR MEDIOS ELECTRÓNICOS	15	2	17	0.03 %
SUPRESIÓN, ALTERACIÓN O SUPOSICIÓN DE LA IDENTIDAD Y ESTADO CIVIL	15	2	17	0.03 %
ACTOS LESIVOS A LOS DERECHOS DE AUTOR	10	0	10	0.02 %
DELITOS CONTRA LA INFORMACIÓN PÚBLICA RESERVADA LEGALMENTE	5	0	5	0.01 %
REPROGRAMACIÓN O MODIFICACIÓN DE INFORMACIÓN DE EQUIPOS TERMINALES MÓVILES	3	0	3	0.01 %
INTERCAMBIO, COMERCIALIZACIÓN O COMPRA DE INFORMACIÓN DE EQUIPOS TERMINALES MÓVILES	1	0	1	0.00 %
REEMPLAZO DE IDENTIFICACIÓN DE TERMINALES MÓVILES	1	0	1	0.00 %
Total Noticias Del Delito:	**40 204**	**10 160**	**50 364**	**100 %**

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) – Analítica FGE.

Las cinco noticias del delito predominantes se distribuyen de la siguiente manera: el 60.16 % (30 300) corresponden a estafas en línea, el 15.74 % (7 928) están relacionadas con la suplantación de identidad, el 8.58 % se refieren a la apropiación fraudulenta por medios electrónicos, mientras que el 4.23 % (2 129) y el 3.29 % (2 011) corresponden a violaciones a la intimidad y acoso sexual, respectivamente.

Estos datos revelan una preocupante situación en la proliferación de ciberdelitos en nuestro país. Con más de cincuenta mil denuncias en quince meses, queda en evidencia que representan una amenaza seria para la seguridad cibernética. Es especialmente inquietante que las estafas en línea y la suplantación de identidad constituyan el 75.9 % de las denuncias. Esto

pone de manifiesto la aplicación generalizada de técnicas basadas en ingeniería social, indicando que los delincuentes están aprovechando la confianza y credulidad de los ciudadanos ecuatorianos en el ciberespacio.

En el ámbito cantonal de Loja, los mil trescientos noventa y cinco (1 395) casos denunciados se distribuyen entre los dieciséis cantones, como se detalla en la Tabla 4.

Tabla 4

Noticias del delito por año de registro, según el cantón de incidente en la provincia de Loja

Cantón de incidente y tipo penal	Total 2023	Total Ene-Mar 2024	Total NDDs	Porcentaje
LOJA	880	211	1091	78.21 %
CATAMAYO	61	14	75	5.38 %
CALVAS	25	12	37	2.65 %
MACARA	23	12	35	2.51 %
PALTAS	24	5	29	2.08 %
PUYANGO	16	7	23	1.65 %
GONZANAMA	20	2	22	1.58 %
CELICA	14	7	21	1.51 %
ZAPOTILLO	14	2	16	1.15 %
SARAGURO	13	1	14	1.00 %
ESPINDOLA	7	2	9	0.65 %
PINDAL	7	1	8	0.57 %
QUILANGA	5	1	6	0.43 %
CHAGUARPAMBA	4	1	5	0.36 %
OLMEDO	1	2	3	0.22 %
SOZORANGA	1	0	1	0.07 %
Total Noticias Del Delito:	**1 115**	**280**	**1 395**	**100.00 %**

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) – Analítica FGE.

Hay una brecha demasiado marcada entre el cantón con la mayor cantidad de denuncias de delitos y los quince restantes. El cantón Loja concentra el 78.21 % del total de las denuncias, lo que equivale a 1 091 casos, seguido muy por detrás por Catamayo con el 5.38 % (75 casos) y Calvas con el 2.65 % (37 casos).

Como se indica en la Tabla 5, en el cantón Loja las cinco noticias del delito predominantes se distribuyen de la siguiente manera: el 71.49 % (780) corresponden a estafas en línea, el 10.17 % (111) están relacionadas con la suplantación de identidad, el 5.96 % se

refieren a la violación a la intimidad, mientras que el 4.22 % (46) y el 2.02 % (22) corresponden a apropiación fraudulenta por medios electrónicos y acoso sexual, respectivamente.

Tabla 5

Noticias del delito por año de registro, en el cantón Loja

Cantón de incidente y tipo penal (Loja)	Total 2023	Total Ene-Mar 2024	Total NDDs	Porcentaje
ESTAFA	644	136	780	71.49 %
SUPLANTACIÓN DE IDENTIDAD	86	25	111	10.17 %
VIOLACIÓN A LA INTIMIDAD	55	10	65	5.96 %
APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS	33	13	46	4.22 %
ACOSO SEXUAL	19	3	22	2.02 %
HOSTIGAMIENTO	17	2	19	1.74 %
ACTOS LESIVOS A LA PROPIEDAD INTELECTUAL	6	3	9	0.82 %
TERRORISMO	4	4	8	0.73 %
TRANSFERENCIA ELECTRÓNICA DE ACTIVO PATRIMONIAL	5	2	7	0.64 %
CONTACTO CON FINALIDAD SEXUAL CON MENORES DE DIECIOCHO AÑOS POR MEDIOS ELECTRÓNICOS	5	1	6	0.55 %
INTERCEPTACIÓN ILEGAL DE DATOS	0	6	6	0.55 %
ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTICO, TELEMÁTICO O DE TELECOMUNICACIONES	0	5	5	0.46 %
PORNOGRAFÍA CON UTILIZACIÓN DE NIÑAS, NIÑOS O ADOLESCENTES	3	0	3	0.27 %
APROVECHAMIENTO ILÍCITO DE SERVICIOS PÚBLICOS	1	1	2	0.18 %
FALSIFICACIÓN INFORMÁTICA	1	0	1	0.09 %
REVELACIÓN DE SECRETO O INFORMACIÓN PERSONAL DE TERCEROS	1	0	1	0.09 %
Total Noticias Del Delito:	**880**	**211**	**1 091**	**100.00 %**

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) – Analítica FGE.

Estas estadísticas reflejan la preocupante situación en el contexto del cibercrimen, el ciberespacio y la ingeniería social en el cantón de Loja. La abrumadora cantidad de denuncias concentradas en un solo cantón, Loja, indica un posible foco de actividad delictiva en esta área. Además, el hecho de que un solo cantón represente más del 78 % del total de las denuncias sugiere la presencia de estrategias altamente persuasivas basadas en la ingeniería social. El gran número de denuncias en Loja podría indicar que los delincuentes están aprovechando las debilidades de los ciudadanos, como la confianza y la falta de conocimiento, para llevar a cabo sus actividades delictivas en línea.

5. Metodología

Para el desarrollo del presente proyecto de investigación se utilizó la metodología de avance por fases, las cuales se detallan a continuación:

1) Fase inicial: Comprendió la investigación y recopilación de información esencial para el desarrollo del proyecto. Para la ejecución de esta fase, se llevó a cabo el análisis de artículos y publicaciones científicas con el objetivo de obtener la mayor cantidad de información y, a partir de esto se generaron aportes fundamentados en el marco teórico.
2) Fase de desarrollo: En esta etapa se ejecutó una encuesta a la población urbana de la ciudad de Loja, que permitió determinar la eficacia de la aplicación de las técnicas más utilizadas de ingeniería social y establecer el nivel de conciencia y conocimiento sobre la posible vulneración de información personal en redes sociales.
3) Fase final: Se ejecutó el análisis de los resultados obtenidos de las encuestas realizadas y, a partir de estos, se recomendó estrategias adecuadas para la prevención y mitigación de ataques relacionados a la aplicación de la ingeniería social en redes sociales.

Con el empleo de esta metodología se integró la investigación teórica, la recopilación de datos empíricos y la evaluación práctica para proporcionar un análisis completo de la ingeniería social en el contexto de las redes sociales, con el objetivo final de contribuir al conocimiento y fortalecer las defensas contra este tipo de amenazas.

5.1.Aspectos de interés

Para la fase de ejecución de las encuestas, se definió un formato que aborda las siguientes cuestiones clave:

- ¿Cuál es el sexo y la edad?
- ¿Tiene conocimiento sobre el ciberespacio?
- ¿Se considera miembro activo en el ciberespacio?
- ¿Qué tiempo promedio se encuentra en línea y cuál es la actividad que realiza?
- ¿Tiene conocimiento sobre las redes sociales?
- ¿Cuántas redes sociales posee?
- ¿Las credenciales o preguntas para acceso a sus redes sociales están relacionadas con algún familiar, fecha especial, color favorito, comida favorita, mascotas, o algún tópico personal?

- ¿Alguna vez ha configurado la privacidad de su información personal, laboral, fotos y publicaciones que comparte en sus redes sociales?
- ¿Alguna vez el usuario se ha sentido interrogado, acosado o intimidado por personas desconocidas en redes sociales?
- ¿Cree haber sido víctima de algún ataque cibernético?
- ¿Alguna vez ha hecho click en enlaces enviados por personas desconocidas?
- ¿Alguna vez perdió el control o acceso a alguna de sus redes sociales?
- ¿Tiene conocimiento sobre la ingeniería social?
- ¿Ha sido capacitado en temas relacionados a la seguridad informática, seguridad de la información o ciberseguridad?
- ¿Cuándo fue la última vez que fue capacitado?

De esta manera, el cuestionario busca recopilar información relevante sobre el nivel de conocimiento, participación y experiencias de los usuarios en el ciberespacio y las redes sociales, con el objetivo de analizar su grado de conocimiento, exposición y vulnerabilidad ante posibles amenazas de ingeniería social.

6. Resultados

La etapa de ejecución de encuestas se llevó a cabo en la zona urbana de Loja, durante el mes de mayo del año 2024. Se aplicaron dos tipos de encuestas: 136 de manera digital o en línea y 254 de forma presencial o física, sumando un total de 390 muestras para el análisis y obteniendo los siguientes resultados:

De las 390 personas encuestadas, 168 (43.1 %) son de sexo femenino y 222 (56.9 %) corresponden a sexo masculino y la categoría de edad se distribuye de la siguiente manera:

- 262 (67.2 %) Adultos menores (20 a 59 años).
- 75 (19.2 %) Adolescentes (12 a 19 años).
- 53 (13.6 %) Adultos mayores (mayores a 60 años).

En los resultados se establece que 250 personas (64.1 %) conocen lo que es el ciberespacio, mientras que 140 (35.9 %) no. De las 250 personas que tienen conocimiento sobre el ciberespacio, 234 (93.6 %) se consideran miembros activos, mientras que 16 (6.4 %) personas no se consideran así. No obstante, entre las 140 personas que desconocen sobre el ciberespacio, 18 se consideran miembros activos. En total, 252 personas se consideran miembros activos en el ciberespacio, representando el 64.6 % de las personas encuestadas.

El 69.3 % de los adolescentes (52), el 60.7 % de los adultos menores (159) y el 43.4 % de los adultos mayores (23) saben lo que es el ciberespacio y se consideran miembros activos.

El tiempo promedio que las personas encuestadas se encuentran en línea o hacen uso de Internet es de 6 horas y 17 minutos al día. A continuación, se muestran los resultados para cada grupo de interés:

- Para el sexo masculino el tiempo promedio al día es: 6 horas con 15 minutos.
- Para el sexo femenino el tiempo promedio al día es: 6 horas con 21 minutos.
- Para los adolescentes el tiempo promedio al día es: 7 horas con 20 minutos.
- Para los adultos menores el tiempo promedio al día es: 6 horas con 28 minutos.
- Para los adultos mayores el tiempo promedio al día es: 3 horas con 57 minutos.

Entre las principales actividades a las cuales las personas dedican su tiempo en línea son:

- Redes sociales y comunicación (76.7 %).
- Educación y aprendizaje (54.6 %).
- Actividades de entretenimiento (51 %).
- Trabajo (32.6 %).
- Otras: Programación y diseño, juegos en línea, trading, etc. (1.2 %)

En cuanto a redes sociales, el 99 % de las personas sabe lo que son las redes sociales, solamente 4 personas no tienen el conocimiento. Los resultados indican que:

- 197 personas (50.5 %) tienen de 1 a 3 redes sociales.
- 150 personas (38.5 %) tienen de 3 a 5 redes sociales.
- 43 personas (11 %) poseen más de 5 redes sociales.

El 83,1 % (324 personas) relacionan sus credenciales o preguntas de acceso a sus redes sociales con tópicos personales. Analizando por grupo de interés:

Desglose por sexo:

- El sexo femenino las relaciona en un: 86.3 % (145 personas).
- El sexo masculino las relaciona en un: 80.6 % (179 personas).

Desglose por grupos de edad:

- Los adolescentes las relaciona en un: 85.3 % (64 personas).
- Los adultos menores las relaciona en un: 82.1 % (215 personas).
- Los adultos mayores las relaciona en un: 84.9 % (45 personas).

El 69,2 % (270 personas) han configurado o realizado ajustes en las opciones de privacidad de sus redes sociales. Analizando por grupo de interés:

Desglose por sexo:

- El sexo femenino: 66.7 % (112 personas).
- El sexo masculino: 71.2 % (158 personas).

Desglose por grupos de edad:

- Los adolescentes: 69.3 % (52 personas).
- Los adultos menores: 80.5 % (211 personas).
- Los adultos mayores: 13.2 % (7 personas).

El porcentaje de personas que se han sentido interrogados, acosados o intimidados por personas desconocidas en sus redes sociales es de 41.5 % (162 personas). Analizando por grupo de interés:

Desglose por sexo:

- El sexo femenino: 51.8 % (87 personas).
- El sexo masculino: 33.8 % (75 personas).

Desglose por grupos de edad:

- Adolescentes: 56 % (42 personas).
- Adultos menores: 37.4 % (98 personas).
- Adultos mayores: 41.5 % (22 personas).

De las 162 personas que indican haberse sentido interrogados, acosados o intimidados el 32.7 % (53 personas) se atrevió a denunciar de manera formal este tipo de comportamiento.

Desglose por sexo:

- Sexo femenino: 33.3 % (29 personas).
- Sexo masculino: 32 % (24 personas).

Desglose por grupos de edad:

- Adolescentes: 19 % (8 personas).
- Adultos menores: 43.9 % (43 personas).
- Adultos mayores: 9.1 % (2 personas).

De todas las muestras obtenidas, el 35.6 % (139 personas) cree que pudo haber sido víctima de un ataque cibernético. Analizando por grupo de interés:

Desglose por sexo:

- Sexo femenino: 41.7 % (70 personas).
- Sexo masculino: 31.1 % (69 personas).

Desglose por grupos de edad:

- Adolescentes: 48 % (36 personas).
- Adultos menores: 30.5 % (80 personas).
- Adultos mayores: 43.4 % (23 personas)

Los resultados indican que el 40.5 % (158 personas) ha hecho click en enlaces compartidos por personas desconocidas. Analizando por grupo de interés:

Desglose por sexo:

- Sexo femenino: 39.3 % (66 personas).
- Sexo masculino: 41.4 % (92 personas).

Desglose por grupos de edad:

- Adolescentes: 42.7 % (32 personas).
- Adultos menores: 38.2 % (100 personas).
- Adultos mayores: 49.1 % (26 personas)

El 43.6 % (170 personas) de las personas encuestadas reportan haber perdido el control o acceso a sus redes sociales. Analizando por grupo de interés:

Desglose por sexo:

- Sexo femenino: 49.4 % (83 personas).
- Sexo masculino: 39.2 % (87 personas).

Desglose por grupos de edad:

- Adolescentes: 48 % (36 personas).

- Adultos menores: 42 % (110 personas).
- Adultos mayores: 45.3 % (24 personas)

Respecto a ingeniería social, solamente el 17.9 % (70 personas) tiene conocimiento, mientras que el 82.1 % (320 personas) no. El desglose por grupos de edad que sabe lo que es la ingeniería social se conforma de la siguiente manera: El 16.0 % de los adolescentes (12 personas), el 21.0 % de los adultos menores (55 personas) y el 5.7 % correspondiente a los adultos mayores (3).

Finalmente, el 35.6 % (139 personas) del total de las personas encuestadas ha recibido capacitación en temas referentes a seguridad informática, seguridad de la información o ciberseguridad, mientras que el 64.4 % (251 personas) no. Analizando por grupo de interés:

Desglose por sexo:

- Sexo femenino: 35.7 % (60 personas).
- Sexo masculino: 35.6 % (79 personas).

Desglose por grupos de edad:

- Adolescentes: 38.7 % (29 personas).
- Adultos menores: 39.3 % (103 personas).
- Adultos mayores: 13.2 % (7 personas).

De las 139 personas que afirman haber sido capacitadas:

- 19.48 % (27 personas) recibieron capacitación en un periodo menor a 6 meses.
- 30.9 % (43 personas) en un periodo menor a 1 año.
- 45.3 % (63 personas) fueron capacitadas hace más de un año

Existen 6 personas (4.3 %) que afirmaron haber sido capacitadas en temas relacionados, sin embargo, respondiendo “nunca” en la encuesta.

Finalmente, en la tabla 6 se presenta el resumen de los resultados obtenidos de cada pregunta planteada en la encuesta.

Tabla 6

Resultados de las encuestas

1) Sexo.			
Femenino	Masculino		
43.1 %	56.9 %		
2) Edad.			
Adolescentes	Adultos menores	Adultos mayores	
19.2 %	67.2 %	13.6 %	
3) Conocimiento: Ciberespacio.			

Si	No
64.1 %	35.9 %

4) Se considera miembro activo del ciberespacio.	
Si	No
64.6 %	35.4 %

Conoce lo que es el ciberespacio y se considera miembro activo.		
Adolescentes	Adultos menores	Adultos mayores
69.3 %	60.7 %	43.4 %

5) Tiempo promedio al día en línea.				
9 horas	6 horas	4 horas	2 horas	Otras
29.2 %	41.5 %	24.1 %	1.5 %	3.7 %

Tiempo promedio al día en línea según el sexo.	
Femenino	Masculino
6 horas 21 minutos	6 horas 15 minutos

Tiempo promedio al día en línea según el grupo de edad.		
Adolescentes	Adultos menores	Adultos mayores
7 horas 20 minutos	6 horas 28 minutos	3 horas 57 minutos

6) Actividades en línea.	
Redes sociales y comunicación	76.7 %
Educación y aprendizaje	54.6 %
Actividades de entretenimiento	51.0 %
Trabajo	32.6 %
Otras	1.2 %

7) Conocimiento: Redes Sociales.	
Si	No
99.0 %	1.0 %

8) Cantidad de redes sociales.	
1 a 3 redes sociales	50.5 %
3 a 5 redes sociales	38.5 %
Más de 5 redes sociales	11.0 %

9) Credenciales de seguridad relacionadas a tópicos personales.	
Si	No
83.1 %	16.9 %

Credenciales de seguridad relacionadas a tópicos personales según el sexo.	
Femenino	Masculino

86.3 %	80.6 %	
Credenciales de seguridad relacionadas a tópicos personales según el grupo de edad.		
Adolescentes	Adultos menores	Adultos mayores
85.3 %	82.1 %	84.9 %
10) Configuración de privacidad en las redes sociales.		
Si	No	
69.2 %	30.8 %	
Configuración de privacidad en las redes sociales según el sexo.		
Femenino	Masculino	
66.7 %	71.2 %	
Configuración de privacidad en las redes sociales según el grupo de edad.		
Adolescentes	Adultos menores	Adultos mayores
69.3 %	80.5 %	13.2 %
11) Percepción de sentirse interrogado, acosado o intimidado.		
Si	No	
41.5 %	58.5 %	
Percepción de sentirse interrogado, acosado o intimidado según el sexo.		
Femenino	Masculino	
51.8 %	33.8 %	
Percepción de sentirse interrogado, acosado o intimidado según el grupo de edad.		
Adolescentes	Adultos menores	Adultos mayores
56.0 %	37.4 %	41.5 %
12) Denunció de manera formal alguna de las actitudes mencionadas anteriormente.		
Si	No	
15.6 %	84.4 %	
Afirma la percepción y denunció de manera formal.		
Si	No	
32.7 %	67.3 %	
Afirma la percepción y denunció de manera formal según el sexo.		
Femenino	Masculino	
33.3 %	32.0 %	
Afirma la percepción y denunció de manera formal según el grupo de edad.		
Adolescentes	Adultos menores	Adultos mayores
19.0 %	43.9 %	9.1 %
13) Percepción de haber recibido ciberataques.		

Si	No
35.6 %	64.4 %

Percepción de haber recibido ciberataques según el sexo.	
Femenino	Masculino
41.7 %	31.1 %

Percepción de haber recibido ciberataques según el grupo de edad.		
Adolescentes	Adultos menores	Adultos mayores
48.0 %	30.5 %	43.4 %

14) Clicks en enlaces de personas desconocidas.	
Si	No
40.5 %	59.5 %

Clicks en enlaces de personas desconocidas según el sexo.	
Femenino	Masculino
39.3 %	41.4 %

Clicks en enlaces de personas desconocidas según el grupo de edad.		
Adolescentes	Adultos menores	Adultos mayores
42.7 %	38.2 %	49.1 %

15) Perdió el control o acceso a sus redes sociales.	
Si	No
43.6 %	56.4 %

Perdió el control o acceso a sus redes sociales según el sexo.	
Femenino	Masculino
49.4 %	39.2 %

Perdió el control o acceso a sus redes sociales según el grupo de edad.		
Adolescentes	Adultos menores	Adultos mayores
48.0 %	42.0 %	45.3 %

16) Conocimiento: Ingeniería Social.	
Si	No
17.9 %	82.1 %

Conocimiento: Ingeniería Social según el grupo de edad.		
Adolescentes	Adultos menores	Adultos mayores
16.0 %	21.0 %	5.7 %

17) Capacitación: Seguridad informática, seguridad de la información o ciberseguridad.	
Si	No
35.6 %	64.4 %

Capacitación: Seguridad informática, seguridad de la información o ciberseguridad según el sexo.			
Femenino	Masculino		
35.7 %	35.6 %		
Capacitación: Seguridad informática, seguridad de la información o ciberseguridad según el grupo de edad.			
Adolescentes	Adultos menores	Adultos mayores	
38.7 %	39.3 %	13.2 %	
18) Tiempo desde la última capacitación.			
Menos de 6 meses	Menos de 1 año	Más de 1 año	Nunca
7.7 %	11.0 %	17.7 %	63.6 %
Tiempo desde la última capacitación de las personas que afirman haber sido capacitadas.			
Menos de 6 meses	Menos de 1 año	Más de 1 año	Nunca
19.5 %	30.9 %	45.3 %	4.3 %

Fuente: Autor.

7. Discusión

Los resultados expuestos en el capítulo anterior brindan una perspectiva reveladora sobre el impacto de las técnicas de ingeniería social en la seguridad de la información y la privacidad de los usuarios de redes sociales en la zona urbana de Loja. Los datos recopilados respaldan la hipótesis planteada inicialmente, la cual establece que un bajo nivel de conciencia y conocimiento sobre las técnicas empleadas en la ingeniería social se correlaciona con una mayor exposición y vulnerabilidad a los ciberataques en plataformas sociales en línea.

En primer lugar, los resultados muestran un alto grado de desconocimiento generalizado sobre el concepto de "ingeniería social", con solo el 17.9 % de los encuestados afirmando conocerlo. Esto sugiere una falta de concienciación significativa en la población estudiada, lo cual podría facilitar la efectividad de los ataques basados en estas técnicas.

En consecuencia, debido a la falta de conocimiento, los datos revelan que un porcentaje considerable de los encuestados (35.6 %) cree haber sido víctima de un ciberataque, lo cual podría estar relacionado con técnicas basadas en ingeniería social como el phishing o la suplantación de identidad. Además, el 41.5 % reportó haber sido interrogado, acosado o intimidado por desconocidos en redes sociales, un comportamiento que a menudo se utiliza en ataques de ingeniería social para obtener información sensible o comprometer las cuentas de los usuarios.

Otro hallazgo preocupante es que el 43.6 % de los encuestados perdió en algún momento el control o acceso a sus redes sociales, lo cual podría ser consecuencia de cuentas comprometidas mediante técnicas de ingeniería social. Estos resultados respaldan la premisa de que un bajo nivel de conciencia sobre estas amenazas conduce a una mayor exposición y vulnerabilidad, como se planteó en la hipótesis inicial.

Además, los datos obtenidos sugieren que las técnicas de ingeniería social han demostrado ser efectivas al engañar a los usuarios. Por ejemplo, el 40.5 % de la población encuestada admitió haber hecho click en enlaces compartidos por personas o usuarios desconocidos, una práctica comúnmente explotada en ataques basados en ingeniería social. Asimismo, el 83.1 % relaciona sus credenciales con datos personales, lo que facilita los ataques basados en pretextos o manipulación psicológica.

Es preocupante que, a pesar del alto riesgo de exposición y las consecuencias negativas reportadas, solo el 35.6 % de los encuestados ha recibido capacitación en seguridad informática o ciberseguridad. Esto refuerza la idea de que un conocimiento limitado sobre estrategias preventivas aumenta la propensión a sufrir impactos adversos en la seguridad y privacidad, como se proyectó en la hipótesis.

Un aspecto positivo a destacar es que el 69.2 % de los encuestados ha configurado las opciones de privacidad en sus redes sociales, lo cual mitiga parcialmente los riesgos asociados con la ingeniería social. Sin embargo, estas medidas pueden ser insuficientes si no se complementan con una comprensión sólida de las amenazas en línea.

En general, los resultados obtenidos respaldan la hipótesis planteada y subrayan la necesidad urgente de abordar la falta de conciencia y conocimientos sobre las técnicas basadas en ingeniería social en la población estudiada. La investigación ha demostrado una correlación clara entre el bajo nivel de conciencia y la mayor exposición y vulnerabilidad a ciberataques en redes sociales, lo que resalta la importancia de implementar programas de concientización y capacitación para mitigar estos.

8. Conclusiones

Esta investigación ha expuesto la problemática de la ingeniería social y su impacto en la seguridad de la información y privacidad de los usuarios de redes sociales en la zona urbana de Loja. A partir de los hallazgos obtenidos, se pueden extraer las siguientes conclusiones principales:

- Existe un bajo nivel de conciencia generalizado en la población estudiada sobre las técnicas de ingeniería social y sus implicaciones en la seguridad de la información que comparten los usuarios en sus redes sociales. Únicamente el 17.9 % de los encuestados afirmó conocer el concepto, lo que representa una vulnerabilidad significativa ante estas amenazas.
- La falta de conocimientos sobre la ingeniería social se correlaciona directamente con una mayor exposición y vulnerabilidad a ciberataques en redes sociales, tal como se planteó en la hipótesis inicial. Los datos revelan altos porcentajes de usuarios que han sido víctimas de acoso, interrogatorios, pérdida de control de cuentas y posibles ataques cibernéticos.
- Las técnicas de ingeniería social como el phishing, smishing, suplantación de identidades y la manipulación psicológica han demostrado ser altamente efectivas para engañar a los usuarios, aprovechando prácticas inseguras como hacer click en enlaces de usuarios desconocidos o utilizar información personal como credenciales.
- A pesar de los riesgos evidentes, una gran mayoría de los encuestados (64.4 %) no ha recibido capacitación en temas de seguridad informática o ciberseguridad, lo que perpetúa el ciclo de vulnerabilidad y exposición a amenazas relacionadas con la ingeniería social.
- Si bien algunos usuarios han implementado medidas básicas de privacidad en sus redes sociales, estas acciones aisladas son insuficientes para mitigar los riesgos si no se complementan con una comprensión profunda de las amenazas y las prácticas de seguridad.
- Los resultados sugieren una necesidad de implementar programas de concientización y capacitación enfocados en la ingeniería social, sus técnicas y métodos de prevención. Esto permitiría empoderar a los usuarios con los conocimientos necesarios para identificar y mitigar estos ataques, fortaleciendo así la seguridad de la información y la privacidad de los usuarios en el entorno de las redes sociales.

Finalmente, esta investigación ha logrado cumplir con los objetivos planteados, proporcionando una descripción detallada de las técnicas de ingeniería social más utilizadas en

ataques a redes sociales, analizando su impacto en la población estudiada y evaluando el nivel de conciencia y conocimientos existentes. Los hallazgos resaltan la importancia crítica de abordar esta problemática mediante la implementación de estrategias efectivas de concientización y capacitación, con el fin de fortalecer la seguridad digital y salvaguardar la privacidad de los usuarios en plataformas en línea.

9. Recomendaciones

Teniendo como base los hallazgos obtenidos en esta investigación y las conclusiones derivadas, se formulan las siguientes recomendaciones con el objetivo de fortalecer la seguridad de la información y la privacidad de los usuarios de redes sociales frente a las amenazas de la ingeniería social:

- Implementar programas de concientización y capacitación obligatorios sobre ingeniería social, dirigidos a todos los segmentos de la población, con especial énfasis en grupos vulnerables como adolescentes y adultos mayores. Estos programas deben estar diseñados por expertos en ciberseguridad y abordar temas como técnicas de ingeniería social comunes, posibles ataques, identificación de amenazas, mejores prácticas de seguridad y protección de la privacidad en redes sociales.
- Promover la educación en seguridad cibernética desde etapas tempranas, incorporando contenidos relacionados con la ingeniería social y la protección de la información en los planes de estudio de instituciones educativas de todos los niveles. Esto sentará las bases para una cultura de seguridad sólida y fomentará la adopción de hábitos seguros desde una edad temprana.
- Desarrollar campañas de sensibilización masivas, utilizando diversos canales de comunicación, como redes sociales, medios tradicionales y plataformas digitales, para difundir información relevante sobre ingeniería social, sus riesgos y estrategias de mitigación. Estas campañas deben ser diseñadas con un enfoque atractivo y accesible para el público general.
- Fomentar la colaboración entre autoridades gubernamentales, organizaciones de ciberseguridad, empresas de tecnología y la sociedad civil para establecer un marco regulatorio y normativo que aborde de manera integral la problemática de la ingeniería social en el entorno digital. Este marco debe contemplar medidas preventivas, protocolos de respuesta ante incidentes y mecanismos de denuncia y sanción para los perpetradores de estos ataques.
- Incentivar a las empresas y organizaciones públicas y privadas a implementar políticas y controles de seguridad robustos, incluyendo la capacitación periódica de sus empleados en temas de ingeniería social y la adopción de tecnologías de seguridad avanzadas, como soluciones de detección y prevención de amenazas basadas en inteligencia artificial y aprendizaje autónomo o redes neuronales.
- Promover la investigación continua en el campo de la ingeniería social, con el fin de mantenerse al tanto de las técnicas emergentes y desarrollar estrategias de mitigación

efectivas. Esta investigación debe ser multidisciplinaria, involucrando a expertos en ciberseguridad, psicología, sociología y otras áreas relevantes.

- Fomentar la adopción de buenas prácticas de seguridad por parte de los usuarios de redes sociales, como el uso de contraseñas robustas, la activación de la autenticación robusta o multifactor, la configuración adecuada de las opciones de privacidad y la verificación de la identidad de los contactos antes de compartir información sensible.
- Alentar a las plataformas de redes sociales a implementar medidas de seguridad más estrictas, como la detección y bloqueo automático de cuentas sospechosas, la verificación de identidad de los usuarios y la implementación de controles de seguridad avanzados para proteger la privacidad y la integridad de los datos.

La implementación efectiva de estas recomendaciones requerirá de un esfuerzo coordinado y sostenido por parte de todos los actores involucrados, incluyendo autoridades gubernamentales, políticas públicas, organizaciones de ciberseguridad, empresas de tecnología, instituciones educativas y la sociedad civil. Solo mediante un enfoque integral y proactivo podremos mitigar los riesgos asociados con la ingeniería social y fortalecer la seguridad de la información y la privacidad en el entorno digital.

10. Bibliografía

Albladi, S., & Weir, G. R. S. (2016). Vulnerability to social engineering in social networks: A proposed user-centric framework. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 1-6. https://doi.org/10.1109/ICCCF.2016.7740435

Aparicio-Izurieta, V. (2022). Delitos informáticos en Ecuador según el COIP: Un análisis documental. *Sapienza: International Journal of Interdisciplinary Studies*, *3*, 1057-1063. https://doi.org/10.51798/sijis.v3i1.284

Ariza, M., Azambuja, A. J. G. D., Nobre, J. C., & Granville, L. Z. (2023). Automated Social Engineering Attacks using ChatBots on Professional Social Networks. *Anais Do XXVIII Workshop de Gerência e Operação de Redes e Serviços (WGRS 2023)*, 43-56. https://doi.org/10.5753/wgrs.2023.747

Baca, Gabriel. (2017). *Introducción a la Seguridad Informática* (Primera). Grupo Editorial Patria.

Beswick, R. M. (2019). Computer Security as an Engineering Practice: A System Engineering Discussion. *Advances in Science, Technology and Engineering Systems Journal*, *4*(2), 357-369. https://doi.org/10.25046/aj040245

Bytiak, Yuriy et al. (2021). *CYBERSPACE AND VIRTUAL REALITY AS CHARACTERISTICS OF THE INFORMATION SOCIETY*.

Cánovas, José. (s. f.). *La seguridad cibernética en los adolescentes y su vulnerabilidad al hackeo*.

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, *198*, 656-661. https://doi.org/10.1016/j.procs.2021.12.302

CISCO. (s. f.). *Ciberataques: ¿cuáles son las ciberamenazas comunes?* Cisco. Recuperado 6 de abril de 2024, de https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html

CISCO. (2023). *¿Qué es la ciberseguridad? | CISCO*. Cisco. https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Comunicado de prensa UIT. (2021, noviembre). ITU. https://www.itu.int:443/es/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx

Comunicado de prensa UIT. (2023, septiembre). ITU. https://www.itu.int:443/es/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx

Costas, Jesús. (2014). *Seguridad informática* (Original, Vol. 1). Ra-Ma.

Diario La Hora. (2022). *Quiénes son las personas más propensas a ser extorsionadas*. https://www.lahora.com.ec/pais/victimas-preferidas-extorsion/

El Comercio. (2019). Adolescentes, más expuestos a ciberdelitos. *El Comercio*. https://www.elcomercio.com/actualidad/seguridad/adolescentes-exposicion-ciberdelitos-piratas-informaticos.html

Escrivá, Gema, Romero, Rosa, Ramada, David, & Onrubia, Ramón. (2013). *Seguridad Informática* (Vol. 14). MACMILLA IBERIAN, S.A.

FGE-Ecuador. (2020). *Child Grooming—Perfil Criminológico*.

FGE-Ecuador. (2021). *Ciberdelitos—Perfil Criminológico*. 33.

FGE-Ecuador. (2022). *Fiscalía General del Estado | Fiscalía procesa a detenido por el delito de 'grooming'*. https://www.fiscalia.gob.ec/fiscalia-procesa-a-detenido-por-el-delito-de-grooming/

Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., & Jara-Saltos, J. D. (2017). Social engineering as an attack vector for ransomware. *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, 1-6. https://doi.org/10.1109/CHILECON.2017.8229528

IBM. (2023). *¿Qué es la seguridad informática?* https://www.ibm.com/mx-es/topics/it-security

IEEE. (2021). *Introducción: Especial Ciberespacio*. https://www.ieee.es/publicaciones-new/Especial_Recopilacion_Ciberseguridad/Introduccion_Especial_Ciberseguridad.html

IETF. (2000). *Internet Security Glossary*. https://www.ietf.org/rfc/rfc2828.txt

INEC. (2023). *Tecnologías de la Información y Comunicación-TIC*. Instituto Nacional de Estadística y Censos. https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/

Juan Harán. (2021). *Banco Pichincha sufrió ataque informático que afectó parte de sus servicios*. https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/

Kaspersky. (2023). *¿Qué es la ciberseguridad? | Kaspersky*. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An introduction to information security* (NIST SP 800-12r1; p. NIST SP 800-12r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1

NIST. (2012). *Guide for conducting risk assessments* (NIST SP 800-30r1; 0 ed., p. NIST SP 800-30r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

NIST. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53r4; p. NIST SP 800-53r4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4

Policía Nacional del Ecuador. (2020). *Las Estafas Cibernéticas en la actualidad.* https://www.policia.gob.ec/wp-content/uploads/downloads/2020/11/Boletin-Estafas-Ciberneticas.pdf

Rodríguez, P., Rodríguez-Rodríguez, J., Rodriguez Rodriguez, J. C., Rodríguez Góngora, J., Martínez, A., Sousa, J., Avila, N., Roith, C., Saleh Hussein, H., Aguilera Galindo, C., Segura Sánchez, A., & Lopez, A. (2023). *El análisis social del ciberespacio* (Primera Edición).

Sadvisor. (2022, noviembre 1). Los adultos mayores son susceptibles a ser víctimas de fraudes cibernéticos. *Security Advisor*. https://sadvisor.com/los-adultos-mayores-son-susceptibles-a-ser-victimas-de-fraudes-ciberneticos/

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), Article 4. https://doi.org/10.3390/fi11040089

SIETEL. (2024). Abonados y usuarios de internet. *Agencia de Regulación y Control de las Telecomunicaciones - Promovemos el desarrollo armónico del sector de las telecomunicaciones, radio, televisión y las TIC , mediante la administración y regulación eficiente del espectro radioeléctrico y los servicios.* https://www.arcotel.gob.ec/abonados-y-usuarios/

11. Anexos

Anexo 1

Solicitud de información a Fiscalía General del Estado

Requerimiento de información estadística. Externo Recibidos ×

Cristian Fabian Guerrero Espinosa <cristian.f.guerrero@unl.edu.ec> mié, 10 abr, 21:19
para estadisticafge, john

Estimados profesionales de la Fiscalía General del Estado,

Mi nombre es Cristian Guerrero, estudiante de la Maestría en Telecomunicaciones de la Universidad Nacional de Loja.

A través del presente, me dirijo a ustedes con respeto para solicitar su colaboración en la provisión de datos estadísticos relacionados con los delitos/ciberdelitos especificados a continuación. Su asistencia es de suma importancia para el desarrollo técnico y justificado de mi trabajo de titulación titulado: "Ingeniería social: Análisis de las técnicas más utilizadas en los ataques a redes sociales y la percepción de la población urbana de Loja".

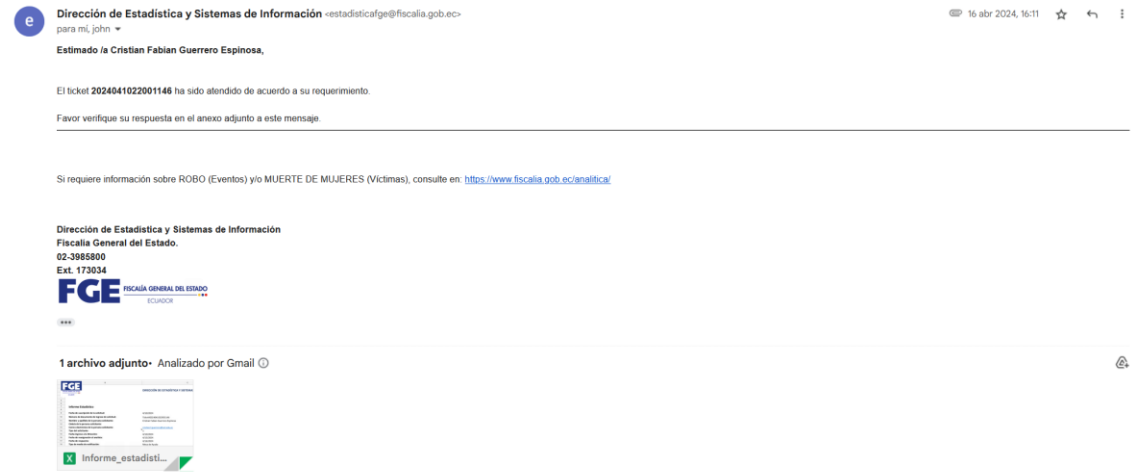
El período estadístico requerido abarca desde febrero de 2023 hasta febrero de 2024.

Las áreas geográficas de interés son: Datos Nacionales y específicos de la provincia de Loja.

Estadísticas correspondientes a los delitos/ciberdelitos según lo establecido en el Código Orgánico Integral Penal (COIP):

Anexo 2

Respuesta de Fiscalía General del Estado



Dirección de Estadística y Sistemas de Información <estadisticafge@fiscalia.gob.ec> 16 abr 2024, 16:11
para mí, john

Estimado /a Cristian Fabian Guerrero Espinosa,

El ticket **2024041022001146** ha sido atendido de acuerdo a su requerimiento.

Favor verifique su respuesta en el anexo adjunto a este mensaje.

Si requiere información sobre ROBO (Eventos) y/o MUERTE DE MUJERES (Víctimas), consulte en: https://www.fiscalia.gob.ec/analitica/

Dirección de Estadística y Sistemas de Información
Fiscalía General del Estado.
02-3985800
Ext. 173034

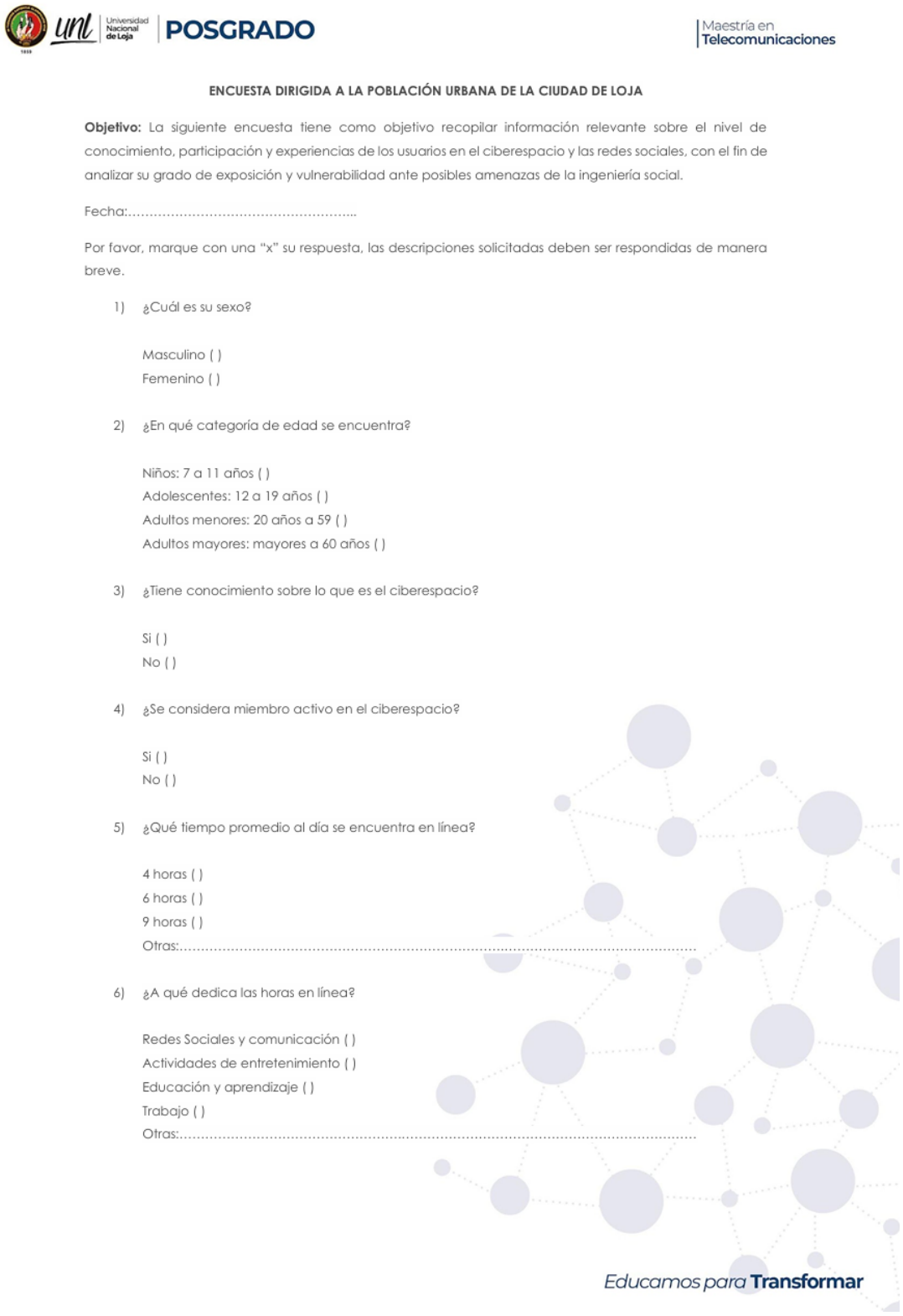
FGE FISCALÍA GENERAL DEL ESTADO ECUADOR

1 archivo adjunto · Analizado por Gmail

Informe_estadísti...

Anexo 3

Formato de encuestas, página 1



UNL Universidad Nacional de Loja | POSGRADO

Maestría en Telecomunicaciones

ENCUESTA DIRIGIDA A LA POBLACIÓN URBANA DE LA CIUDAD DE LOJA

Objetivo: La siguiente encuesta tiene como objetivo recopilar información relevante sobre el nivel de conocimiento, participación y experiencias de los usuarios en el ciberespacio y las redes sociales, con el fin de analizar su grado de exposición y vulnerabilidad ante posibles amenazas de la ingeniería social.

Fecha:.....

Por favor, marque con una "x" su respuesta, las descripciones solicitadas deben ser respondidas de manera breve.

1) ¿Cuál es su sexo?

   Masculino ( )
   Femenino ( )

2) ¿En qué categoría de edad se encuentra?

   Niños: 7 a 11 años ( )
   Adolescentes: 12 a 19 años ( )
   Adultos menores: 20 años a 59 ( )
   Adultos mayores: mayores a 60 años ( )

3) ¿Tiene conocimiento sobre lo que es el ciberespacio?

   Si ( )
   No ( )

4) ¿Se considera miembro activo en el ciberespacio?

   Si ( )
   No ( )

5) ¿Qué tiempo promedio al día se encuentra en línea?

   4 horas ( )
   6 horas ( )
   9 horas ( )
   Otras:.....

6) ¿A qué dedica las horas en línea?

   Redes Sociales y comunicación ( )
   Actividades de entretenimiento ( )
   Educación y aprendizaje ( )
   Trabajo ( )
   Otras:.....

Educamos para Transformar

Anexo 4

Formato de encuestas, página 2

7) ¿Entiende lo que son las redes sociales?

Si ( )
No ( )

8) ¿Qué cantidad de redes sociales posee?

1 a 3 redes sociales ( )
3 a 5 redes sociales ( )
Mas de 5 redes sociales ( )

9) ¿Las credenciales o preguntas de acceso a sus redes sociales están relacionadas con algún familiar, fecha especial, color favorito, comida favorita, mascotas, o algún tópico personal?

Si ( )
No ( )

10) ¿Alguna vez ha configurado la privacidad de su información personal, laboral, fotos y publicaciones que comparte en sus redes sociales?

Si ( )
No ( )

11) ¿Alguna vez se ha sentido interrogado, acosado o intimidado por personas desconocidas en redes sociales?

Si ( )
No ( )

12) ¿Se atrevió a denunciar alguna de las actividades mencionadas en la pregunta anterior de manera formal?

Si ( )
No ( )

13) ¿Cree haber sido víctima de algún ataque cibernético?

Si ( )
No ( )

14) ¿Alguna vez ha hecho click en enlaces enviados por personas desconocidas?

Si ( )
No ( )

Anexo 5

Formato de encuestas, página 3

15) ¿Alguna vez perdió el control o acceso de algunas de sus redes sociales?

Si ( )
No ( )

16) ¿Tiene conocimiento sobre lo que es la ingeniería social?

Si ( )
No ( )

17) ¿Ha sido capacitado en temas relacionados a la seguridad informática, seguridad de la información o ciberseguridad?

Si ( )
No ( )

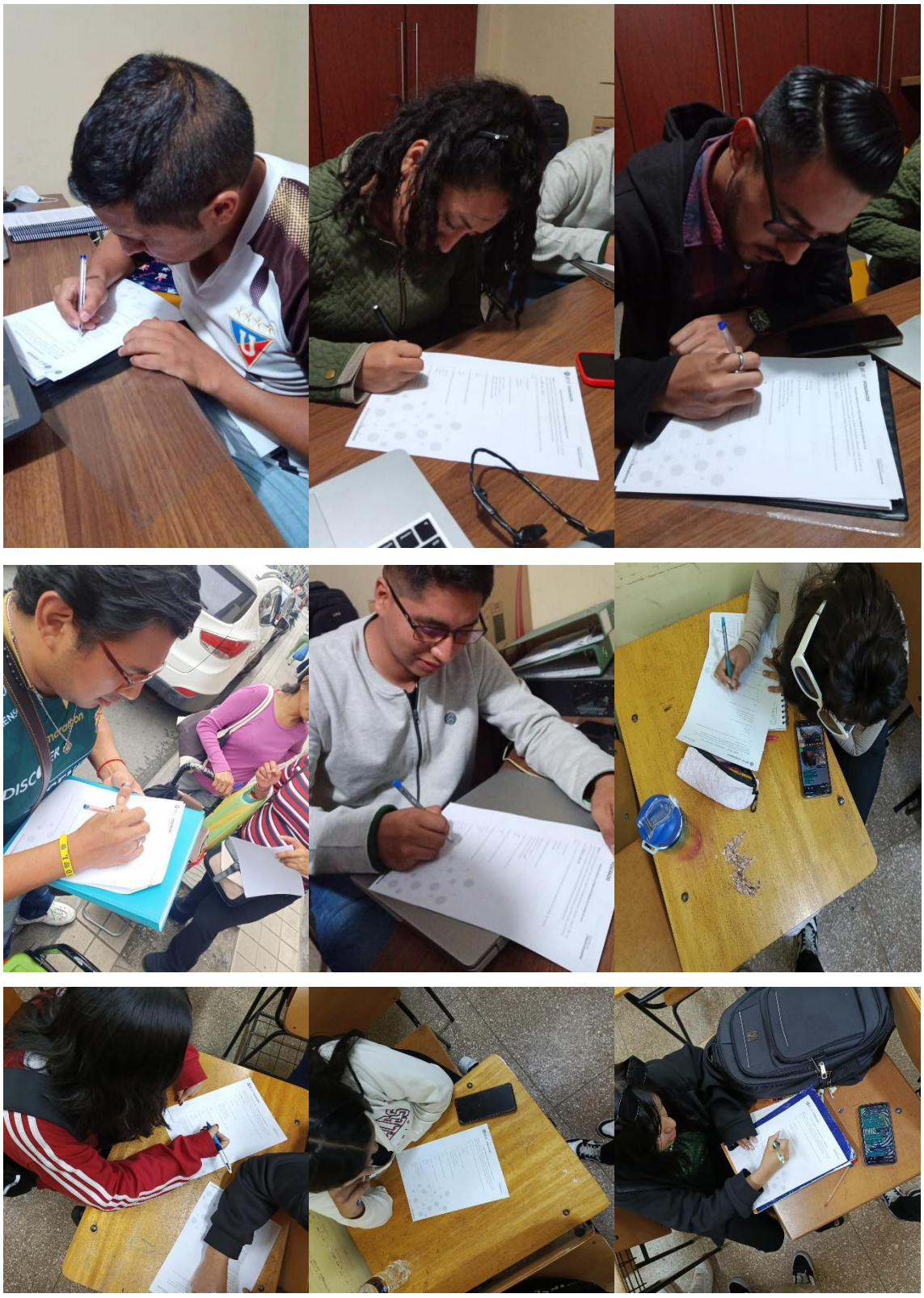
18) ¿Cuándo fue la última vez que fue capacitado en temas relacionados a la seguridad informática, seguridad de la información o ciberseguridad?

Menos de 6 meses ( )
Menos de 1 año ( )
Más de 1 año ( )
Nunca ( )

Anexo 6

Evidencia fotográfica de las encuestas físicas


High Tech



Anexo 7

Certificación de Traducción del resumen

FINE-TUNED ENGLISH LANGUAGE INSTITUTE
Líderes en la Enseñanza del Inglés

Ing. Andrea Lucia Ruiz Roa
SECRETARIA GENERAL
FINE-TUNED ENGLISH CIA. LTDA.

CERTIFICA:

Que la siguiente traducción del resumen de tesis "Ingeniería social: Análisis de las técnicas más utilizadas en los ataques a redes sociales y la percepción de la población urbana de Loja.", pertenece al Ing. GUERRERO ESPINOSA CRISTIAN FABIAN portador de la cédula de ciudadanía 110467907-9, posgradista de la Maestría en Telecomunicaciones de la Universidad Nacional de Loja, han sido traducido de su versión original al idioma inglés y cumplen con las características propias del idioma, previa autorización del autor.

Es todo cuanto puedo certificar en honor a la verdad, facultando al interesado hacer uso del presente en lo que creyera conveniente.

Loja, 27 de junio de 2024

Atentamente,

Ing. Andrea Ruiz Roa
SECRETARIA GENERAL
FINE-TUNED ENGLISH CÍA. LTDA.
Resolución Nro. MDT- SCP-2022-0110

Matriz - Loja: Macará 205-51 entre Rocafuerte y Miguel Riofrío - Teléfono: 072578899
Zamora: García Moreno y Pasaje 12 de Febrero - Teléfono: 072608169
Yantzaza: Jorge Mosquera y Luis Bastidas - Edificio Sindicato de Choferes - Teléfono: 072301329

www.fte.edu.ec