UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

GUIA DE PREVENCIÓN DE RIESGOS DE CIBERSEGURIDAD DERIVADO DEL USO DEL INTERNET Y LAS REDES SOCIALES EN NIÑOS Y ADOLESCENTES DEL CANTÓN CAÑAR

TRABAJO DE TITULACIÓN PREVIO

A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR: FERNANDA MICHAELLE NARVÁEZ OCHOA.

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS.

CAÑAR - ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACIÓN

"GUÍA DE PREVENCIÓN DE RIESGOS DE CIBERSEGURIDAD DERIVADO DEL USO DEL INTERNET Y LAS REDES SOCIALES EN NIÑOS Y ADOLESCENTES DEL CANTÓN CAÑAR"

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR: FERNANDA MICHAELLE NARVÁEZ OCHOA

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS, MGS.

CAÑAR - ECUADOR

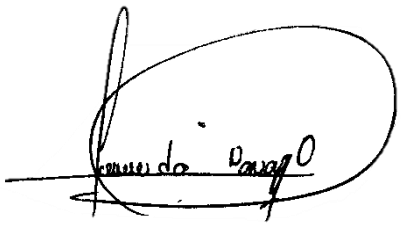
2023

DIOS, PATRIA, CULTURA Y DESARROLLO.

DECLARACIÓN

Yo, Fernanda Michaelle Narváez Ochoa, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Católica de Cuenca extensión Cañar puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y la Normativa actual de la institución.

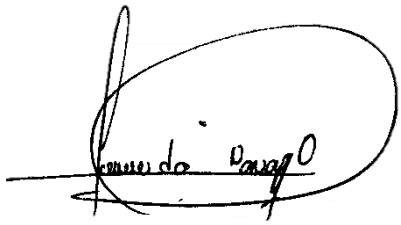


Narváez Ochoa Fernanda Michaelle

C.I: **0302358601**

RESPONSABILIDAD

“La responsabilidad del contenido de esta tesis de grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Universidad Católica de Cuenca Extensión Cañar”.



Narváez Ochoa Fernanda Michaelle

C.I: 0302358601

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por la Estudiante Fernanda Michaelle Narváez Ochoa, bajo mi supervisión.

_____

Ing. Cristhian Flores Urgilés, Mgs.

DIRECTOR DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA EXTENSION CAÑAR

DEDICATORIA

A Dios principalmente por darme la vida, guiarme y bendecirme cada día.

A mi padre, *Klever Vinicio Narváez Calle* por su cariño, paciencia y su apoyo para salir adelante. A mi madre *Bélgica Priscila Ochoa López*, quien ha sido mi pilar fundamental y mi gran motivación para poder cumplir cada uno de mis sueños y metas, por sus consejos y sus palabras de motivación. A mi hermano *Jesús Eduardo Narváez Ochoa*, por su apoyo incondicional y por estar siempre conmigo en este proceso.

Dedico también este título a mi abuelito *Blasco Alejandrino Ochoa Amoroso*, quien siempre creyó en mí y en mis sueños. Siento su ausencia con cada logro, y sé que estaría orgulloso de ver lo que he logrado. Este título es también un homenaje a su memoria.

Fernanda Michaelle Narváez Ochoa

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios por brindarme la sabiduría y la fortaleza necesaria para poder lograr mis objetivos. Su guía y protección me han permitido llegar hasta este punto de mi carrera.

A mi familia, amigos y demás personas especiales en mi vida, les agradezco por su amor y apoyo incondicional. Sin ustedes, nada de esto hubiera sido posible. Su confianza en mí me ha motivado a seguir adelante, incluso en los momentos más difíciles.

A los docentes de la Carrera de Ingeniería de Sistemas de Información, les agradezco por su dedicación y compromiso con la educación. Sus conocimientos y experiencias me han ayudado a crecer como profesional y como persona.

De manera especial, deseo expresar mi agradecimiento al Ing. Cristhian Humberto Flores Urgilés, Mgs., director de mi trabajo de titulación. Su guía y orientación han sido fundamentales para el desarrollo de este proyecto.

RESUMEN

El acceso a internet y las plataformas sociales ha crecido significativamente entre los jóvenes y niños a escala global, principalmente usando teléfonos inteligentes y otros dispositivos portátiles. No obstante, este acceso no está exento de peligros, tales como contenido no apto, acoso virtual, chantajes, entre otros. El presente documento propone la creación de una guía de prevención en ciberseguridad para menores del cantón Cañar. Como parte de este proceso, se llevó a cabo una encuesta sobre la seguridad digital y su impacto en los niños de los diferentes colegios del centro urbano del cantón Cañar. Posteriormente, se hizo una evaluación de riesgos utilizando la metodología Magerit, siguiendo cada una de sus fases, ayudando así a determinar los aspectos más críticos en cuanto a privacidad y seguridad para los jóvenes, además de identificar las principales vulnerabilidades y amenazas que enfrentan diariamente. Los hallazgos mostraron que estos jóvenes son altamente susceptibles a los riesgos de la web y las redes sociales. En base a esto, se diseñó un manual de prevención en ciberseguridad dirigido a padres y profesionales de la educación, con el objetivo de capacitar a los niños y adolescentes para que desarrollen habilidades y conocimiento para navegar de forma segura.

Palabras Clave: ciberseguridad, niños, adolescentes, amenazas, internet.

ABSTRACT

Access to the internet and social platforms has significantly increased among young people and children worldwide, mainly using smartphones and other portable devices. However, this access is not exempt from dangers, such as inappropriate content, cyberbullying, blackmail, among others. This document proposes the development of a cybersecurity prevention guide for minors in the Cañar canton. As part of this process, a survey was conducted on digital security and its impact on the children in various schools of the urban center of the Cañar canton. Subsequently, a risk assessment was carried out using the MAGERIT methodology, following each phase to determine the most critical aspects in terms of privacy and security for young people, in addition to identifying the main vulnerabilities and threats they face on a daily basis. The findings showed that these young people are highly susceptible to the risks of the web and social networks. Based on this, a cybersecurity prevention handbook was designed for parents and education professionals to enable children and adolescents to develop skills and knowledge to navigate safely.

Keywords: cybersecurity, MAGERIT methodology, digital threats, social networks.

Índice de Ilustraciones

Índice de Tablas

INTRODUCCIÓN

Con la rápida expansión de la tecnología y el acceso a Internet se ha transformado la manera en la que los niños y adolescentes interactúan con el mundo, presentando múltiples oportunidades y desafíos. Sin embargo, esto ha conllevado a un aumento de riesgos de seguridad y privacidad en línea, especialmente para los menores de edad. El cantón Cañar no es una excepción ante esta realidad, y se ha convertido en un desafío cada vez más apremiante para los padres, educadores y autoridades locales, el garantizar la seguridad en línea en los nativos digitales.

En este contexto, el presente trabajo tiene como objetivo principal desarrollar una guía de prevención de riesgos de ciberseguridad para niños y adolescentes en el cantón Cañar. Para ello, se llevará a cabo un análisis detallado de los riesgos específicos a los que se enfrentan los menores de edad en línea, y se revisarán las mejores prácticas en prevención de riesgos y protección de la privacidad.

A continuación, se realiza una breve descripción de los capítulos presentados en el documento:

Capítulo I: Hace mención al marco referencial, mismo que abarca la explicación del problema de investigación, antecedentes, objetivos (general, específicos), limitaciones y delimitaciones.

Capítulo II: Contiene el marco teórico, en el que se dan a conocer conceptos relacionados con los riesgos de ciberseguridad, las redes sociales y el internet enfocado directamente en niños y adolescentes. Además de un marco legal y normativo que rige la ciberseguridad.

Capítulo III: Marco metodológico, se detallan las necesidades de los niños y adolescentes del cantón Cañar mediante una encuesta con el objetivo de analizar las amenazas del internet a las que se encuentran expuestos. Se identifica además la metodología de la investigación y su enfoque.

Capítulo IV: Este último capítulo engloba un análisis de riesgos utilizando la metodología Magerit con el fin de determinar activos, vulnerabilidades, amenazas y riesgos de ciberseguridad; para construir la guía de prevención de riesgos.

CAPÍTULO I

MARCO REFERENCIAL

1. Planteamiento del problema

Desde hace algunos años, el uso del internet así como las redes sociales se ha vuelto cada vez más común entre niños y adolescentes del cantón Cañar. Sin embargo, el acceso a la tecnología también conlleva riesgos en términos de seguridad y privacidad en línea. Es por ello, que resulta importante diseñar una guía de prevención de riesgos de ciberseguridad para estos grupos.

A pesar de que existen diferentes iniciativas que buscan educar sobre la seguridad en línea, en el cantón Cañar en las instituciones, no se cuenta con una guía específica que brinde información sobre los peligros y riesgos asociados con el uso de internet y las redes sociales por parte de niños y adolescentes. Calderas (2022) manifiesta que esta falta de orientación puede resultar en situaciones como la exposición a contenidos inapropiados, acoso cibernético, robo de identidad o incluso ser víctimas de fraudes en línea. En consecuencia, es necesario abordar este problema a través de la elaboración de una guía de prevención de riesgos de ciberseguridad dirigida a niños y adolescentes del cantón Cañar, que contenga información relevante y actualizada sobre cómo utilizar las herramientas tecnológicas de manera segura y responsable.

Esta guía no solo ayudará prevenir problemas relacionados con la seguridad en línea, sino que también fomentaría el uso consciente y responsable de la tecnología en la población joven del cantón, beneficiando a las diferentes unidades educativas.

1.1.Formulación del Problema

El problema central del presente proyecto, surge debido a que no existe una guía de prevención de riesgos de ciberseguridad que presente medidas de prevención, bajo este contexto se plantea la siguiente pregunta:

- ¿Cuál es el impacto potencial de la guía de prevención de riesgos de ciberseguridad para niños y adolescentes del cantón Cañar en la disminución de los riesgos derivados del uso del Internet y las redes sociales?

1.2. Antecedentes de la investigación

El analizar el impacto negativo del internet y las diferentes redes sociales en niños y adolescentes es fundamental, ya que de esta manera se puede identificar vulnerabilidades y amenazas. Siendo así un factor social que afecta a nivel mundial; es por ello que varios autores han desarrollado investigaciones que van en beneficio de los jóvenes en vista de que se abordan problemáticas de seguridad informática.

Claes & Deltell en el año (2019), realizan un análisis de la comunicación digital en museos, determinando el uso de las diferentes redes sociales y páginas webs en estudiantes, en donde definen que el Internet debe ser usado por los estudiantes para fines académicos y se debe limitar el acceso a las redes sociales en establecimientos y museos. Tomando esta investigación como referencia para el análisis de indicadores que los autores utilizan para analizar las páginas web.

Así mismo, un artículo realizado por Luque & Herrero (2019), analizan el impacto de la tecnología en adolescentes en Ecuador, realizando el estudio de manera cualitativa, mediante una prueba de test-retest. Los autores efectúan 6 preguntas referentes al uso de los dispositivos móviles, las redes sociales, la conectividad y la comunicación,

considerando también la afectación de las redes sociales, en donde ultiman que si en las diferentes escuelas, colegios e incluso universidades no se hace hincapié del buen manejo de la tecnología, no se puede asegurar un buena productividad de los jóvenes. Siendo este artículo una línea base para analizar la encuesta y sobre todo sus indicadores.

Por otro lado Torres (2021), analiza y evalúa el impacto de los ciberataques en adolescentes en el rango de 12 a 17 años de edad en la ciudad de Quito, a través de la metodología descriptiva utilizando la técnica cuantitativa para realizar una encuesta, utilizando también herramientas para la generación de ciberataques. El autor analiza los artículos del COIP relacionados a la ciberseguridad, además obtiene como resultado que los ataques que se dan con mayor frecuencia en un 42% de los adolescentes son los enlaces enviados por correo electrónico para el robo de información. El documento antes mencionado permite identificar los artículos del Código Orgánico Integral Penal que se enfocan en los delitos informáticos, mismos que se tomará como valor de referencia para la construcción de la guía.

Un documento elaborado por Area et al. en el año (2022), permite visualizar una guía de buenas prácticas, misma que posee estrategias para el buen uso de las TIC dirigida no solamente a los niños, sino también a los padres de familia, así como a los docentes. De esta manera este trabajo, permite considerar los puntos abordados así como las imágenes que presentan para la elaboración de la guía.

En cuanto a investigaciones nacionales, Peña & Sánchez en el año (2022), elaboran una guía de buenas prácticas con el objetivo de mitigar los riesgos a los adolescentes entre el rango de 13 a 15 años, utilizando una metodología cualitativa, que permite identificar en primera instancia la manera en la que los jóvenes utilizan el internet. Sin embargo, con la aplicación de la guía se pudo ultimar el cambio en cuanto al manejo de

las redes sociales, siendo este favorable. El documento antes mencionado, sirve como referencia de cómo estructurar la guía de buenas prácticas enfocada en los adolescentes.

1.3. Justificación de la investigación

Los nativos digitales, tienden a confiar demasiado en la tecnología, y es por eso que publican información personal que podría ser usada sin su consentimiento. Siendo un grupo vulnerable ante varios riesgos, ya que a menudo carecen de la experiencia y la educación necesaria para protegerse adecuadamente en línea. Además, los padres y tutores pueden o no estar al tanto de todos los peligros cibernéticos que sus hijos enfrentan a diario y cómo prevenirlos.

Por lo tanto, es importante proporcionar una guía de prevención de riesgos de ciberseguridad específica para los niños y adolescentes del cantón Cañar, que ayude a los jóvenes a entender los peligros en línea y a tomar medidas para protegerse de ellos. Esta guía incluirá información sobre la privacidad en línea, el acoso cibernético, la suplantación de identidad en línea, el grooming, la exposición a contenidos inapropiados, entre otros.

En definitiva, será de gran utilidad para los jóvenes, padres, tutores y educadores del cantón Cañar, al proporcionar información clara y práctica para protegerse en línea y disfrutar de internet y las redes sociales de manera segura y responsable.

1.4. Objetivos

1.4.1. Objetivo General

Generar una guía de prevención de riesgos de ciberseguridad derivado del uso del internet y las redes sociales en niños y adolescentes del cantón Cañar

1.4.2. Objetivos Específicos

2. Realizar un estudio teórico sobre las amenazas y vulnerabilidades más comunes de las redes sociales y su impacto en los niños y adolescentes.
3. Realizar un tratamiento de gestión de riesgos de ciberseguridad sobre el uso del internet y las redes sociales en los niños y adolescentes utilizando un marco de referencia reconocido.
4. Crear una guía estratégica para prevenir y mitigar las amenazas y vulnerabilidades en los adolescentes del cantón Cañar.

5. Limitaciones

- Falta de colaboración de los estudiantes de las diferentes Unidades Educativas del cantón Cañar.
- Cambio constante de las tecnologías y tendencias
- Falta de compromiso de las partes interesadas.
- Riesgos en el manejo o funcionalidad del equipo de cómputo
- Tiempo mínimo de 5 meses para la elaboración de la investigación

6. Delimitaciones

La presente investigación se elaborará en beneficio de los niños y adolescentes en el rango de edad de 12-17 años; padres de familia y educadores del cantón Cañar de los colegios “Andrés F Córdova”; “José Peralta”; “San José de Calasanz”; “Santa Rosa de Lima” “Intercultural Bilingüe Quilloac”. El tiempo para llevar a cabo el desarrollo del proyecto será de 5 meses.

Basándose en la técnica del análisis de riesgos, con la finalidad de evaluar los peligros cibernéticos del Internet y las redes sociales como Tik Tok, Facebook, Instagram, WhatsApp.

CAPÍTULO II

MARCO TEÓRICO

En años recientes, la popularidad y la utilización de las redes sociales e internet han experimentado un crecimiento notable. Vale la pena resaltar que la pandemia de COVID-19 ha influido considerablemente en este fenómeno, propiciando un incremento en el número de usuarios en diversas plataformas sociales de forma especial en niños y adolescentes, ampliando la duración del tiempo que estos pasan conectados (Paschke, Austermann, Simon-Kutscher, & Thomasius, 2021).

Los jóvenes en Ecuador tienen un índice muy alto de uso de internet. De hecho, el 93,5 % de las personas de entre 16 y 24 años usan Internet, lo que es significativamente más alto que la tasa general de penetración de Internet del 81,3 %. Esto apunta que los jóvenes en Ecuador son muy activos en línea y usan Internet para una variedad de propósitos, incluidas las redes sociales, la educación y el entretenimiento (DATAREPORTAL, 2023).

2.1. Vulnerabilidades en el uso del Internet y las redes sociales

Los niños, niñas y adolescentes son particularmente vulnerables a los riesgos asociados con internet y las redes sociales. Esto se debe a que todavía están desarrollando sus habilidades de pensamiento crítico y es posible que no puedan distinguir entre lo que es real y lo que no lo es. También es más probable que compartan información personal en línea, lo que puede convertirlos en objetivos de acoso cibernético, depredadores en línea y otras formas de abuso (Montes Vozmediano, Pastor Ruiz , Martín Nieto, & Atuesta Reyes, 2020).

Las vulnerabilidades de las redes sociales y el internet en los niños y adolescentes resaltan las debilidades o puntos ciegos comunes por parte de este grupo de edad.

2.1.1. Ámbito Familiar

2.1.1.1. Falta de Control parental

Muñoz (2022), manifiesta que:

La falta de control parental en el uso de las redes sociales y el internet, contribuye a que los niños y/o adolescentes accedan a contenido inapropiado, interacciones dañinas, entre otros.

Cuando los padres no están involucrados en el uso de las redes sociales de sus hijos, pueden no estar conscientes de con quién están interactuando sus hijos, qué tipo de información están compartiendo, y qué tipo de contenido están viendo. Esto puede exponer a los niños a una variedad de riesgos, incluyendo el ciberacoso, la exposición a contenido inapropiado, la explotación y el robo de identidad (Alonso, 2020). Por lo tanto, es crucial que los padres estén activos y comprometidos en la vida digital de sus hijos para ayudar a protegerlos de estos riesgos.

2.1.2. Ámbito Técnico

2.1.2.1. Ausencia antivirus

Este factor es una vulnerabilidad para el usuario al navegar en internet, ya que al no disponer de uno no se puede proteger al usuario de todas las amenazas. Sin embargo, es importante considerar que los usuarios son quienes deben tener buenos hábitos de navegación y conocimiento sobre la ciberseguridad (Kahimise & Shava, 2020).

Ilustración 1. Ausencia de Antivirus. Fuente: Autoría Propia.

2.1.2.2. Contraseñas débiles

El uso de contraseñas débiles o la repetición de contraseñas puede hacer que las cuentas de las redes sociales sean fácilmente hackeables. Los atacantes suelen utilizar técnicas de fuerza bruta, en las que prueban todas las combinaciones posibles de contraseñas, o de diccionario, en las que prueban palabras y combinaciones comunes, para intentar acceder a las cuentas. Por lo tanto, el uso de contraseñas débiles puede poner en riesgo la seguridad de las cuentas en internet y en las redes sociales (Xylogiannopoulos, Karampelas, & Alhajj, 2020).

2.1.2.3. Seguridad de los datos

Otra vulnerabilidad dentro del contexto del uso de las redes sociales y el internet es la falta de conciencia sobre la privacidad. Las redes sociales recopilan una gran cantidad de datos del usuario, que pueden ser vulnerables a los ataques cibernéticos.

La privacidad en línea se refiere a la protección de la información personal que se comparte en Internet. Muchos usuarios de redes sociales, especialmente los más jóvenes, a menudo no son conscientes de las implicaciones de la privacidad en línea y pueden compartir sin querer información personal sensible que podría ser utilizada de manera perjudicial (Koohang, Nord, Floyd, & Paliszkiewiz, 2022).

2.1.3. Ámbito Legal

2.1.3.1. Normas legales no estandarizadas

La regulación y las leyes en torno a las redes sociales varían significativamente entre diferentes países y regiones, lo que puede crear incertidumbre y posibles brechas en la protección de los datos y la privacidad del usuario.

2.1.3.2. Difamación y noticias falsas

Las redes sociales pueden ser usadas para difamar a individuos u organizaciones, lo que puede llevar a acciones legales. “La difusión de noticias falsas en las redes sociales es de especial preocupación, ya que la comunicación en ellas tiende a ser percibida como algo privado y la información así obtenida, en consecuencia, como algo veraz y altamente creíble” (Slavko, Zavhorodnia, & Shevchenko, 2020, pág. 2016).

2.1.3.3. Usuarios falsos

Los perfiles falsos en las redes sociales son cuentas que han sido creadas con la intención de engañar a otros usuarios. Pueden ser utilizados por personas o entidades con una variedad de intenciones.

“Los usuarios crean cuentas falsas para realizar actividades maliciosas como difundir noticias falsas, virus y spam” (Kaur, Uslu, & Durresi, 2021, pág. 643).

Ilustración 2. Usuarios Falsos. Fuente: Autoría Propia.

2.2. Amenazas derivadas del uso del internet y las redes sociales

El internet y las redes sociales se han convertido en una parte integral de la vida de las personas, sin embargo, plantean una serie de amenazas, llegando a tener un impacto grave en su seguridad y bienestar. Por un lado, Realpe & Cano (2020), definen que una amenaza cibernética es cualquier acto malicioso que busca dañar, robar o interrumpir datos y la vida digital en general. Por otro lado, Dahbur et al. (2011), comenta que una amenaza es cualquier entidad que puede explotar una vulnerabilidad para causar daños.

2.2.1. Ámbito Familiar

2.2.1.1. Exposición a contenido inapropiado

Las redes sociales pueden exponer a los usuarios a contenido violento, sexual o de otro tipo que puede ser perjudicial, especialmente para los usuarios más jóvenes.

Garitaonandia et al. (2020) manifiestan:

La exposición a contenido inapropiado o dañino se refiere a los contenidos disponibles en internet y en las plataformas de redes sociales que pueden no ser apropiados debido a factores como la edad, el género, la raza y las orientaciones

sexuales, entre otros. Esta información podría tener implicaciones psicológicas adversas para los jóvenes.

Ilustración 3. Contenido inapropiado. Fuente: (Flash Start, 2022)

2.2.1.2. Cyberbullying

De acuerdo con Chiza et al. (2020)

La violencia cibernética considerada como ciberbullying se ha convertido en un problema que ha incrementado en los últimos años, de forma especial en los adolescentes (pág. 44). Moretti & Herkovits (2021) definen al ciberbullying como "una práctica que ha sido introducida como un problema novedoso en los campos de salud y educación" (pág. 2).

Ilustración 4. Ciberacoso. Fuente: Autoría Propia.

2.2.1.3. Ciberacoso / Grooming

De acuerdo con Astorga & Schmidt (2019), el grooming hace referencia al acoso cibernético que se da por parte de una persona adulta hacia un niño o adolescente, utilizado perfiles falsos con la intención de ganar y confianza y establecer una relación emocional con ellos a través de tácticas de manipulación emocional (pág. 10).

Ilustración 5. Grooming. Fuente: (Pedriatía Salud , 2018)

2.2.1.4. Sexting

(Pineda & Torres, 2020) afirma:

> El sexting consiste en enviar, recibir o compartir imágenes, mensajes o videos sexuales por medio de dispositivos tecnológicos, este puede ser consensuado por personas adultas como menores de edad. Este último puede conllevar a la producción y distribución de pornografía infantil. (pág. 16)

Por ello es importante que los padres o tutores, dialoguen con sus hijos sobre los riesgos y las consecuencias del sexting y la importancia de comprender la privacidad de

los datos personales e integridad del adolescente y de las demás personas (Cardoso, Falcke, & Mosmann, 2019).

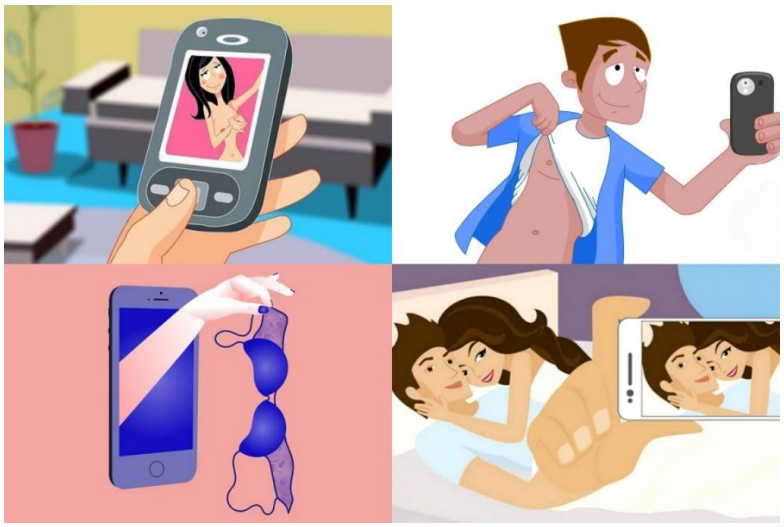


Ilustración 6. Sexting. Fuente: (Garcia, 2023)

2.2.1.5 Ciberadicción

La ciberadicción de acuerdo con Cobacango et al. (2019), es el uso desmedido de internet en dispositivos como Tablet, celulares, computadoras; este uso puede proporcionar a los niños y adolescentes el acceso a una gran cantidad de información que puede intervenir en su vida cotidiana.

Existen algunos criterios que permiten diagnosticar la adicción al internet tales como:

- Cambios drásticos en los hábitos de vida a fin de tener más tiempo para conectarse
- Descuido de la salud propia
- Disminución de la sociabilidad (Pérdida de amistades)
- Rechazo a actividades físicas

- Negligencia respecto al trabajo y las obligaciones personales (Prieto, 2019, pág. 133).

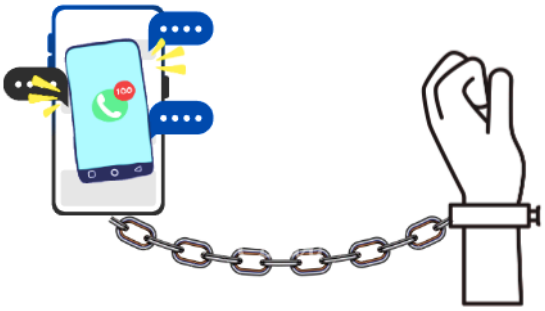


Ilustración 7. Ciberadicción. Fuente: Autoría Propia.

2.2.1.6 Pornografía infantil

El término pornografía infantil es un delito que se refiere a cualquier material visual o escrito como imágenes, historias, videos, entre otros; que representa a menores de edad en actos sexuales explícitos o sugerentes (Noguera, Edotti, Galofre, Martínez, & Gonzales, 2023) (ICMEC, 2018).

Ilustración 8. Pornografía infantil. Fuente: (Ministerio de Educación, 2023)

2.2.2. Ámbito técnico

2.2.2.1. Ataques de phishing

El phishing es una amenaza que enfrentan los usuarios de internet, empresas e incluso gobiernos. Utiliza correos electrónicos o sitios web fraudulentos para engañar a las víctimas para que revelen información personal, como contraseñas, números de tarjetas de crédito u otros datos confidenciales (Zafar, Javed, & Kifayat, 2021).

Ilustración 9. Ataques de Phishing. Fuente: Autoría Propia.

2.2.2.2. Ciberdelincuencia

Se refiere a cualquier actividad delictiva que se realiza mediante computadoras o internet. Esto puede incluir una variedad de acciones maliciosas, que van desde el robo de identidad, el fraude, la estafa, la distribución de malware (como virus o ransomware), el hacking, la invasión de la privacidad, el acoso cibernético, hasta la pornografía infantil y la trata de personas. (Cordero Ruiz, 2021).

2.2.2.3. Ataques de malware

Los cibercriminales pueden usar las redes sociales para propagar software malicioso, como virus y ransomware. Estos ataques pueden provocar:

- Pérdida de privacidad: La información que se comparte en las redes sociales puede ser vista por cualquier persona, incluyendo desconocidos o personas malintencionadas.
- Difusión de información falsa: Las noticias falsas o los rumores pueden propagarse de forma inmediata a través de las redes sociales, lo que puede generar confusión y causar daño.
- Pérdida de productividad: El uso excesivo de las redes sociales en los adolescentes puede afectar la productividad académica (Méndez, 2022).

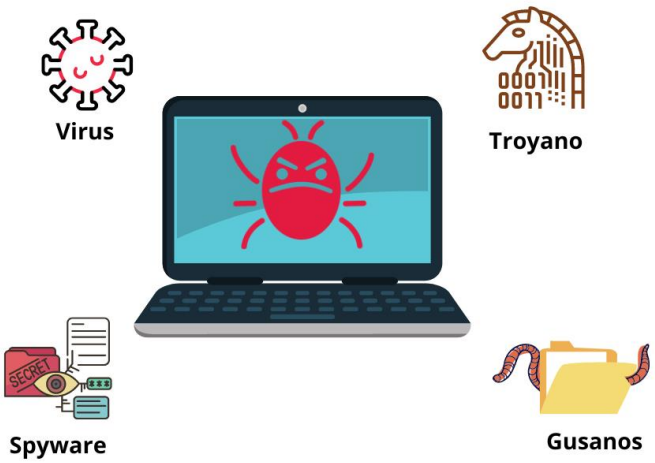


Ilustración 10. Malware. Fuente: Autoría Propia.

2.2.2.4. Ransomware

Jain & Rani (2019) comentan que:

El ransomware es un tipo de malware que cifra los archivos de la víctima y exige el pago de un rescate a cambio de la clave de descifrado, llegando a ser muy costosos, tanto en términos de pérdidas financieras como en interrupción de actividades comerciales e incluso dañar la reputación de personas o empresas. En el contexto de las redes sociales y el internet este virus es utilizado para publicar enlaces en sitios web maliciosos; enviar correos electrónicos de phishing, publicar datos robados, entre otros.

Ilustración 11. Ransomware. Fuente: Autoría Propia.

2.2.2.5. Acceso no autorizado

Kumar et al. (2021) manifiestan que:

> El acceso no autorizado es cuando alguien obtiene acceso a un sistema informático, cuentas, red o datos sin permiso. Esta amenaza poder ser el resultado de varias actividades maliciosas como el phishing, hacking, robo de contraseñas, entre otros.

Así, puede tener una gran variedad de consecuencias negativas, por ello, es crucial que los usuarios puedan protegerse contra estas amenazas utilizando contraseñas más fuertes, antivirus actualizado, concienciación en seguridad cibernética (Thilini B. G. Herath & Ahmed, 2022).

Ilustración 12. Acceso no autorizado. Fuente: Autoría Propia.

2.2.3. Suplantación de identidad

Hernández (2019) comenta que:

La suplantación de identidad se refiere a la acción de hacerse pasar por otra persona, incluyendo la usurpación ya sea del nombre, de una imagen, entre otros. Es así que los estafadores pueden crear perfiles falsos o enviar mensajes que parecen proceder de fuentes legítimas para engañar a los usuarios y obtener información personal o financiera.

Ilustración 13. Suplantación de identidad. Fuente: (Ministerio de Educación, 2023)

2.2.4. Desinformación y noticias falsas

Las redes sociales pueden ser utilizadas para difundir desinformación o noticias falsas, lo cual puede tener consecuencias perjudiciales en muchos ámbitos, desde la política hasta la salud pública. “Las Fake News provocan un peligroso círculo de desinformación” (FIP, 2018, pág. 1).

Tusa & Durán (2019), determinan que en los últimos años “las noticias falsas tienen una mayor irrupción en plataformas de acceso abierto y gratuito, generando que este tipo de información crezca de manera exponencial en segundos” (Tusa & Durán, 2019, pág. 20).

2.2.5. Daño emocional, físico o psicológico en niños y adolescentes

Dados las amenazas mencionadas anteriormente, se puede ultimar que las redes sociales pueden tener una serie de efectos negativos en los niños, niñas y adolescentes que incluye:

- Daño emocional: Las redes sociales pueden provocar sentimientos de ansiedad, depresión, soledad y baja autoestima. Esto debido a que tienen a ser un lugar que expone contenidos negativos (Keles, McCrae, & Grealish, 2019).

- Daño físico: Las redes sociales pueden generar problemas como falta de sueño, fatiga visual y dolores de cabeza, esto debido a la ciberadicción. También puede conducir a problemas como el aislamiento social (Russell M Viner, 2019).

- Daño psicológico: las redes sociales pueden generar problemas como ansiedad, depresión y baja autoestima. También puede conducir a problemas como la adicción y el aislamiento social (Wartberg, Thomasius, & Paschke, 2021).

Ilustración 14. Daño emocional causado por el Internet y las redes sociales. Fuente: Autoría Propia.

2.3. Riesgos

De acuerdo con Fragoso & Ramírez (2022), los riesgos de ciberseguridad, tanto en niños como en adolescentes pueden llegar a tener un impacto negativo tanto en la salud mental como de manera emocional, así como en su reputación y seguridad en línea; por ello es fundamental que los niños y jóvenes estén al tanto de los riesgos para tomar medidas preventivas y mantenerse seguros en línea. Los riesgos hacen referencia a la probabilidad de que una amenaza en particular explote una vulnerabilidad y la gravedad del impacto. El riesgo informático es la posibilidad de que una amenaza informática se materialice y cause un daño, pérdida, o impacto no deseado en los sistemas de información y los activos digitales de una organización. Este riesgo se mide a través de la combinación de la probabilidad de ocurrencia de una amenaza y el impacto que tendría en caso de que ocurriera.

2.3.1. Análisis de riesgos

Un análisis de riesgos es un proceso sistemático y proactivo para identificar, evaluar y preparar respuestas a incertidumbres que pueden afectar a un proyecto, proceso o decisión. Este proceso se utiliza a menudo en el contexto de la gestión de proyectos, la seguridad de la información y la planificación financiera, aunque es relevante en prácticamente cualquier campo donde existan riesgos. El riesgo es calculado multiplicando el valor cuantitativo de la probabilidad por el impacto del daño (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020).

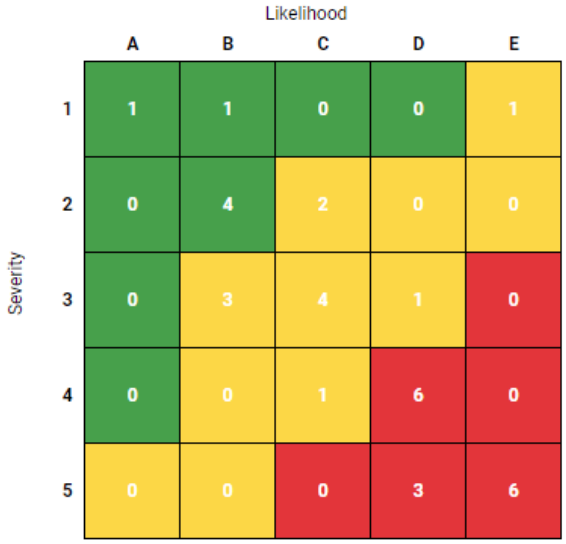


Ilustración 15. Matriz de análisis de riesgos. Fuente:

2.4. Controles

Los controles de ciberseguridad en las redes sociales e Internet son las medidas que las personas y las organizaciones pueden tomar para proteger sus datos y su privacidad de las ciber amenazas. Están diseñados para mitigar y gestionar los riesgos informáticos que enfrenta una organización; cada riesgo identificado requiere controles específicos para minimizar su probabilidad de ocurrencia o reducir su impacto. El propósito de los controles es garantizar los principios de la seguridad de la información, así como proteger los sistemas de información contra amenazas y vulnerabilidades.

2.4.1. Ámbito familiar

2.4.1.1. Software de control parental

Un software de control parental es un tipo de herramienta de seguridad informática diseñada para ayudar a los padres a supervisar y controlar el uso que sus hijos hacen del internet y de los dispositivos digitales. Estos tienen una serie de características como el filtrado de contenido y bloqueo de sitios web, control de tiempo de pantalla, monitoreo de actividad en línea, geolocalización, control de aplicaciones, entre otros (Gallego, Malamud, & Eleches, 2020).

Existen aplicaciones como **Qustodio o Kaspersky Safe Kids** que permiten establecer límites de tiempo en los diferentes dispositivos, bloquear contenido, sitios web con la finalidad de proteger a los niños.

- **Qustodio**: es un software de control parental muy popular y altamente valorado que proporciona una serie de características que ayudan a los padres a monitorear y controlar el uso que sus hijos hacen de sus dispositivos electrónicos.
- **Kaspersky Safe Kids:** Permite proteger la privacidad del usuario y mantener a los niños seguros en línea, permite obtener la geolocalización en tiempo real, además de controlar la actividad de aplicaciones y de sitios web. Permite también que no se ejecuten aplicaciones o sitios web específicos, este software controla el tiempo en línea del usuario y oculta contenido inapropiado con filtros web y Sage Search (Kaspersky, 2023, pág. 2)

2.4.1.2. Educación

Es fundamental educar a los miembros de la familia sobre los riesgos en línea y enseñarles prácticas seguras, como no compartir información personal y ser escépticos respecto a ofertas o mensajes no solicitados. Así la educación en el ámbito de ciberseguridad ayuda a los niños y adolescentes y también a padres de familia, a comprender temas de protección de información personal, a usar las redes sociales de forma segura, a prevenir el acoso cibernético.

Ecuador ha implementado varios programas de ciberseguridad para niños, tal es el caso del Ministerio de Educación que no solamente cuenta con información para niños sino también para docentes y padres de familia.

2.4.2. Ámbito técnico

2.4.2.1. *Instalación de software antivirus*

El software antivirus es una herramienta de seguridad que se utiliza para detectar y eliminar virus, gusanos y otro tipo de malware de una computadora o red. El software antivirus se actualiza regularmente para detectar nuevas amenazas y mantener la protección contra ellas (Mullo Mullo, 2022, pág. 14). Por ello, es importante que los usuarios cuenten con un antivirus para proteger los sistemas de las amenazas cibernéticas y prevenir posibles daños y brechas de seguridad.

2.4.2.3. *Uso de gestores de contraseñas seguras*

Utilizar contraseñas seguras con el objetivo de mantener la seguridad de cuentas, así las contraseñas deben ser largar y contener valores alfanuméricos con caracteres especiales. Además, los usuarios no tienen que utilizar las mismas contraseñas que usan para otras cuentas ya que si el atacante conoce esa contraseña, puede comprometer todas las cuentas (Jain, Sahoo, & Kaubiyal, 2021).

2.4.3. Ámbito Legal

Ecuador cuenta con un marco legal que proporciona una base sólida y estructurada que promueve la educación y la conciencia de las políticas y regulaciones relacionadas con la ciberseguridad.

2.4.3.1. Política pública por una Internet segura para niños, niñas y adolescentes

El Consejo Nacional para la Igualdad Intergeneracional en el año (2020) :

Establece la política pública por una Internet segura para niños, niñas y adolescentes, siendo esta esencial para proteger a estos grupos vulnerables ante riesgos y peligros que se encuentran en línea.

El documento incluye información acerca de una página web (www.internetsegura.gob.ec), que cuenta con recursos y herramientas dirigidas a los jóvenes, docentes, padres de familia, y autoridades. Manifestando además que los diálogos abiertos académicos relacionados con el correcto uso del Internet son importantes. La política pública cuenta con cinco ejes, en donde estos buscan garantizar un entorno digital seguro para niños y adolescentes mediante la reforma legislativa (Eje I) y la implementación de lineamientos técnicos (Eje II). Se enfatiza la coordinación y supervisión institucional (Eje III), la educación en seguridad digital (Eje IV) y la promoción de una cultura de protección a través de estrategias comunicativas (Eje V), todo con el fin de minimizar vulnerabilidades y asegurar un uso constructivo y protegido de las tecnologías. (CONSEJO NACIONAL PARA LA IGUALDAD INTEGENERACIONAL, 2020, pág. 34).

2.4.3.2. Código Orgánico Integral Penal del Ecuador

El COIP de Ecuador en sus artículos 103 y 104 estipula sanciones severas para quienes produzcan o comercialicen pornografía con menores. El artículo 173 penaliza el acercamiento con fines sexuales a menores por medios electrónicos, con penas más severas si se usa coacción o identidades falsas. El artículo 174 penaliza la oferta de servicios sexuales con menores por medios electrónicos.

Los artículos 178, 190, 212, 230 y 233 se refieren a la violación de la privacidad y la integridad de datos personales, la apropiación fraudulenta por medios electrónicos, la suplantación de identidad, la interceptación ilegal de datos y delitos contra la información pública reservada.

Las sanciones varían dependiendo de la gravedad y las circunstancias del delito, y van desde uno hasta diez años de privación de libertad.

2.4. Gestión de riesgos

Alfaro y Paniagua (2022), definen a la gestión de riesgo como un proceso que implica la identificación, evaluación y priorización de riesgos, seguido de la aplicación coordinada y económica de recursos para minimizar, monitorear y controlar la probabilidad o el impacto de eventos imprevistos. “Se encarga de determinar lo que va a suceder y cuáles son sus consecuencias, antes de decidir lo que se debe hacer y cuando hacerlo, con el objeto de que se reduzca el riesgo” (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020, pág. 2).

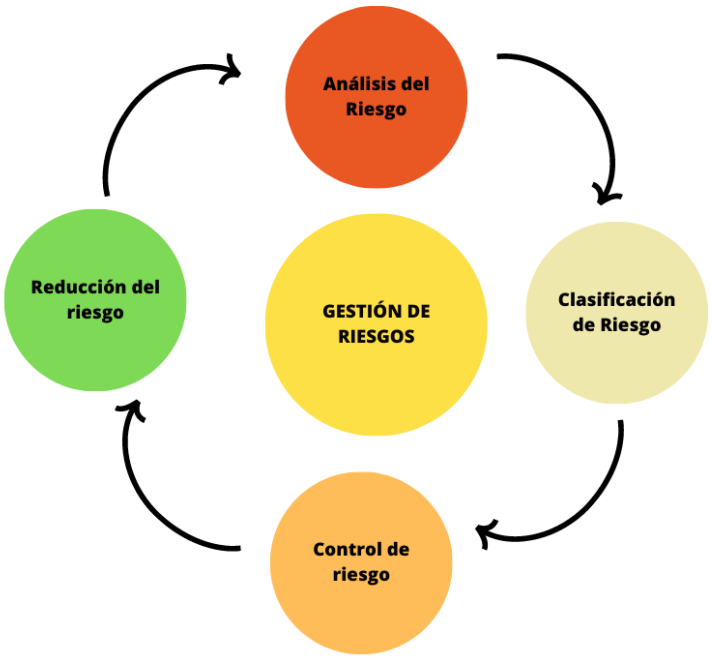


Ilustración 16. Gestión de riesgos. Fuente: Autoría Propia

2.4.1. Riesgo residual

En la gestión de riesgos, el riesgo residual es la cantidad de riesgo que queda después de que se han implementado los controles. Es el riesgo que no es eliminado por los controles (INEE, 2023).

El riesgo residual se calcula restando la cantidad de riesgo que eliminan los controles del riesgo original. La fórmula para el riesgo residual es:

$$\boldsymbol{Riesgo\ residual\ =\ Riesgo\ inherente\ -\ Control}$$

Sin embargo, es necesario recalcar que a pesar de la implementación de controles solo se minimiza el riesgo más no se elimina; la única forma de eliminar los riesgos es dejando de hacer la actividad por lo que se recomienda utilizar una gestión de riesgos efectiva que incluya un ciclo de mejora continua que consistirá en la periódica evaluación de riesgos Flores et al. (2018).

2.5. Metodologías de gestión de riesgos

Conforme con el concepto dado por Contreras (2022):

Las metodologías de gestión de riesgos permiten identificar de mejor manera los eventos de riesgo de una manera sistemática y estructurada para identificar, evaluar y gestionar los riesgos asociados a una determinada organización. Se compone de una serie de pasos que se adaptan a las necesidades y circunstancias específicas.

2.5.1. MAGERIT

La metodología Magerit permite el análisis y gestión de riesgos que se derivan del uso de la información, tiene cuatro objetivos principales tales como:

- Concientizar a los responsables de la presencia de riesgos para el Sistema de Información y la necesidad de adoptar medidas para evitarlos, controlarlos o minimizar sus daños.
- Ofrecer un método común para analizar los riesgos en las organizaciones
- Ayudar para la planificación de las medidas de adopción
- Facilitar procesos relacionados con la gestión de riesgos (Bartolomé, 2019, pág. 49)

Esta metodología cuenta con tres fases tales como:

1. **Definir el alcance:** Se identifican los activos que deben ser protegidos, que incluyen los sistemas de información, las infraestructuras, los datos y cualquier otro elemento relevante. También se identifican las amenazas potenciales y se estima el impacto que podrían tener en caso de materializarse.
2. **Análisis de riesgos:** En esta fase, se realiza un análisis detallado de los riesgos identificados en la fase anterior. Esto implica la evaluación de la probabilidad de que las amenazas se materialicen y el impacto que tendrían si lo hicieran. Esto da como resultado una clasificación de los riesgos, desde los más altos hasta los más bajos.
3. **Gestión:** Se determinan las medidas de seguridad que deben ser implementadas para gestionar los riesgos identificados (Gastelo Fernandez & Rodríguez Flores , 2023)

2.5.2. OCTAVE

Esta metodología permite identificar y administrar los riesgos de seguridad de la información, se enfoca en tres aspectos fundamentales:

- Activo: Identifica los activos críticos de la organización, tales como la información que es crucial para la operación y supervivencia del negocio
- Amenaza: Identifica y evalúa las amenazas a estos activos, que pueden ser tanto internas (por ejemplo, empleados descontentos o errores de operación) como externas (por ejemplo, hackers o competidores)
- Vulnerabilidad: Evalúa las vulnerabilidades o debilidades que podrían ser explotadas por las amenazas para dañar los activos (Llauce Valdera, 2022) (Hurtado, 2018).

2.5.3. ISO 27005

De acuerdo con la ISO / IEC (2022), la norma ISO 27005 se centra en la gestión de la seguridad de la información, incluyendo la identificación, evaluación y tratamiento de los riesgos, incluye:

1. **Identificación de riesgos**: Esto implica identificar los activos de información que requieren protección, así como las amenazas y vulnerabilidades que podrían comprometer esos activos.
2. **Evaluación de riesgos**: Esto implica determinar el impacto potencial y la probabilidad de los riesgos identificados.
3. **Tratamiento de riesgos**: Esto implica seleccionar y aplicar controles para mitigar los riesgos a un nivel aceptable.
4. **Aceptación de riesgos**: Los riesgos que no se pueden mitigar o que se consideran aceptables después de la aplicación de los controles se aceptan.
5. **Comunicación de riesgos**: Los riesgos, así como las decisiones tomadas para tratarlos y aceptarlos, se comunican a todas las partes interesadas.
6. **Monitoreo y revisión de riesgos**: Los riesgos y la eficacia de los controles se revisan y monitorean regularmente para asegurarse de que la gestión de riesgos se mantiene efectiva (García & Alexey, 2022).

2.5.4. Cuadro comparativo de las Metodologías para la Gestión de Riesgos

El siguiente análisis comparativo se ha elaborado mediante una matriz con indicadores en las categorías de enfoque, aplicación, adaptabilidad y componentes clave. Estos indicadores permiten contrastar de forma resumida los aspectos distintivos de cada metodología. El enfoque se seleccionó por ser un marco orientador fundamental. La aplicación muestra el contexto y alcance de utilización preferente. La adaptabilidad indica la flexibilidad para distintos tipos de organizaciones. Finalmente, los componentes clave reflejan las etapas y procesos característicos abordados por cada metodología.

Esta selección de indicadores ofrece una visión integral de los aspectos diferenciadores, facilitando la comparación entre las metodologías analizadas.

Table 1. Cuadro comparativo de las metodologías de Gestión de Riesgos. Fuente: Autoría Propia

	MAGERIT	**OCTAVE**	**ISO 27005**
Enfoque	Se centra en la identificación y protección de los activos de información	Enfoque basado en la participación de la organización y la evaluación de los riesgos operativos críticos, con énfasis en los activos, las amenazas y las vulnerabilidades.	Enfoque amplio y sistemático para la gestión de riesgos de seguridad de la información, con énfasis en la identificación, evaluación y tratamiento de los riesgos.

Aplicación		Se aplica a PYMES, empresas pequeñas y medianas	Se puede aplicar a cualquier organización, protegiendo todo aquello que afecte a la seguridad de la información
Adaptabilidad	Desarrollada principalmente para la administración pública española, pero puede ser adaptada a otros contextos	Diseñada para ser adaptada a las necesidades y objetivos específicos de la organización.	Diseñada para ser aplicable a cualquier tipo de organización, independientemente de su tamaño o naturaleza.
Componentes Clave	Identificación de activos, evaluación de amenazas, análisis de impacto, evaluación de riesgos, implementación de medidas de seguridad.	Identificación de activos, identificación y evaluación de amenazas y vulnerabilidades, desarrollo de estrategias de mitigación de riesgos.	Identificación de riesgos, evaluación y estimación de riesgos, tratamiento de riesgos, aceptación de riesgos, comunicación de riesgos, revisión y monitoreo de riesgos.

De acuerdo al análisis comparativo realizado, se selecciona a Magerit como la metodología más apropiada ya que sus componentes clave cubren de manera integral los procesos requeridos para una adecuada gestión de riesgos de seguridad de la

información: identificación de activos, evaluación de amenazas y riesgos, selección de salvaguardas, etc. Además es una metodología flexible que se adapta a diferentes tipos de organizaciones y tamaños.

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Enfoque de la investigación

Para la elaboración del presente trabajo se ha tomado en cuenta variables cualitativas y cuantitativas, que permiten la recolección de la información para realizar el análisis de los riesgos en los niños y adolescentes del cantón Cañar.

3.2. Nivel de la investigación

La presente investigación es de carácter descriptivo ya que se realizará una serie de pasos para la realización de una gestión de riesgos de ciberseguridad.

3.3. Población y muestra

3.3.1. Población

La población se centra en los estudiantes de los diferentes colegios del centro urbano del cantón Cañar, en los que consta:

- Unidad Educativa Fiscomisional Santa Rosa de Lima
- Unidad Educativa Fiscomisional San José de Calasanz
- Unidad Educativa Andrés F. Córdova
- Unidad Educativa José Peralta
- Unidad Educativa Comunitaria Intercultural Bilingüe Quiollac

Contando con un total de 630 estudiantes.

3.3.2. Muestra

Tamaño de Muestra $n = \frac{N*Z^2*p*q}{e^2(N-1)+Z^2*p*q}$

Donde:

- n: tamaño de la muestra.

- N: tamaño de la población.
- Z: valor crítico de la distribución normal estándar correspondiente al nivel de confianza deseado. Con un nivel de confianza del 95%, Z es igual a 1.96.
- p: proporción estimada de la característica que se está estudiando en la población.
- e: margen de error máximo permitido del 5%.

Obteniendo así una muestra de 240 estudiantes.

3.4. Técnicas e instrumentos de recolección

Para la recolección de la información, se realiza una encuesta a los niños y adolescentes de los colegios del centro urbano del cantón Cañar.

3.5. Tratamiento de la información

La información obtenida de las encuestas será debidamente tratada y sistematizada en matrices.

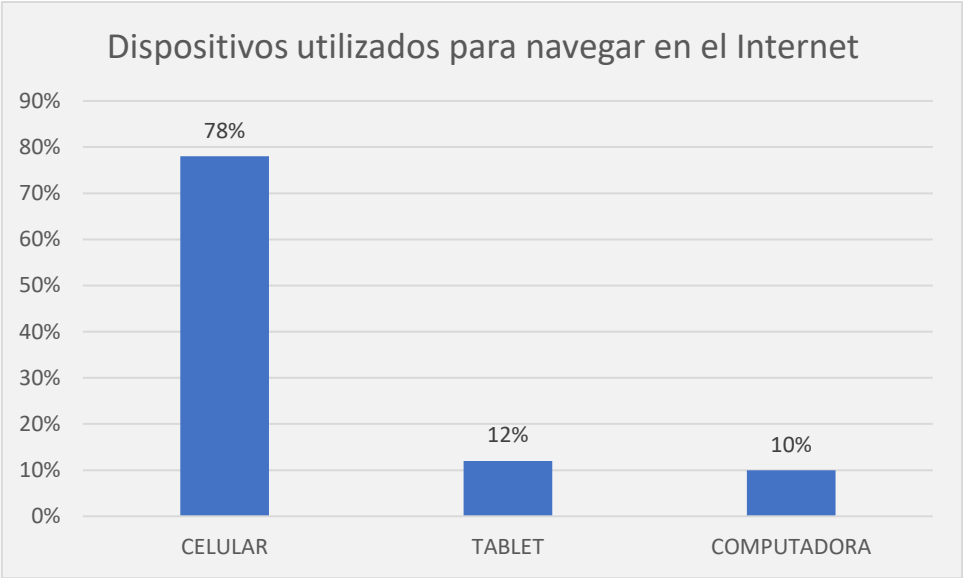
3.6. Resultados

Tras haber definido las interrogantes que serán abordadas en la encuesta, se inicia la fase de implementación de la misma, con la finalidad de determinar el estado del uso del internet así como de las redes sociales en los adolescentes.

A continuación, se presenta los resultados de la encuesta realizada a los niños y adolescentes de los diferentes colegios del centro urbano del cantón Cañar, con el fin de determinar la situación actual de la ciberseguridad y sus riesgos; e identificar las tendencias de uso a lo largo del tiempo y grupos de niños que pueden estar en riesgo de uso excesivo o indebido.

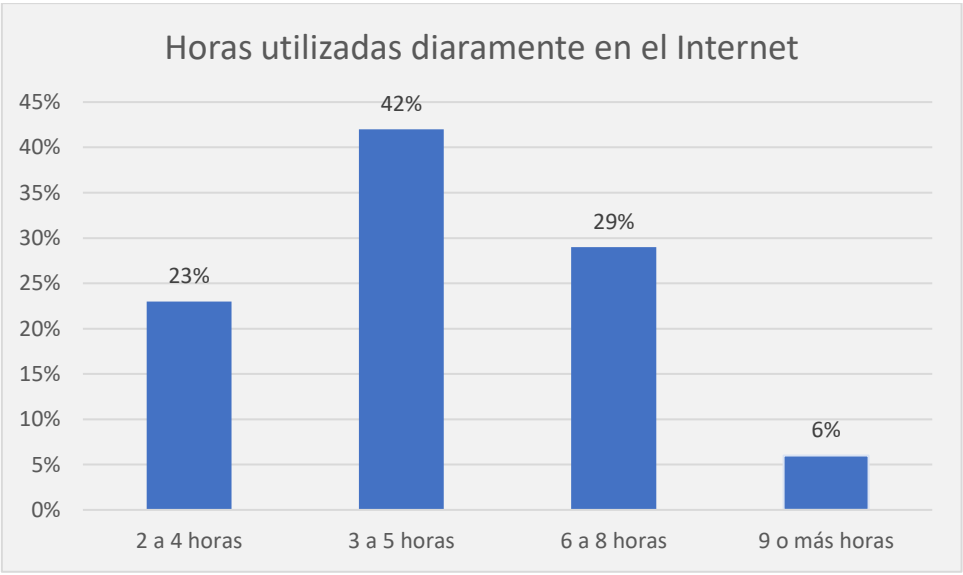
Los resultados se representan con un análisis en la parte inferior de cada ilustración.

Pregunta 1. ¿Qué dispositivos utilizas para navegar en el internet?



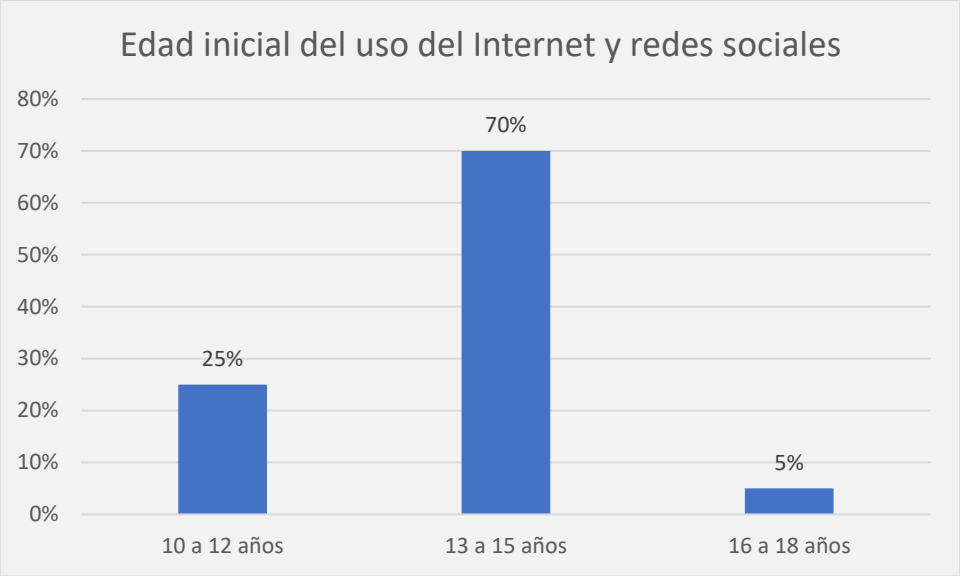
La mayoría de los encuestados (alrededor del 78%) utilizan principalmente el celular para conectarse a internet y redes sociales. Esto indica que el celular es el dispositivo predilecto entre los jóvenes para estar en línea.

Pregunta 2. ¿Cuál es el promedio de horas al día que utilizan el internet y las redes sociales?



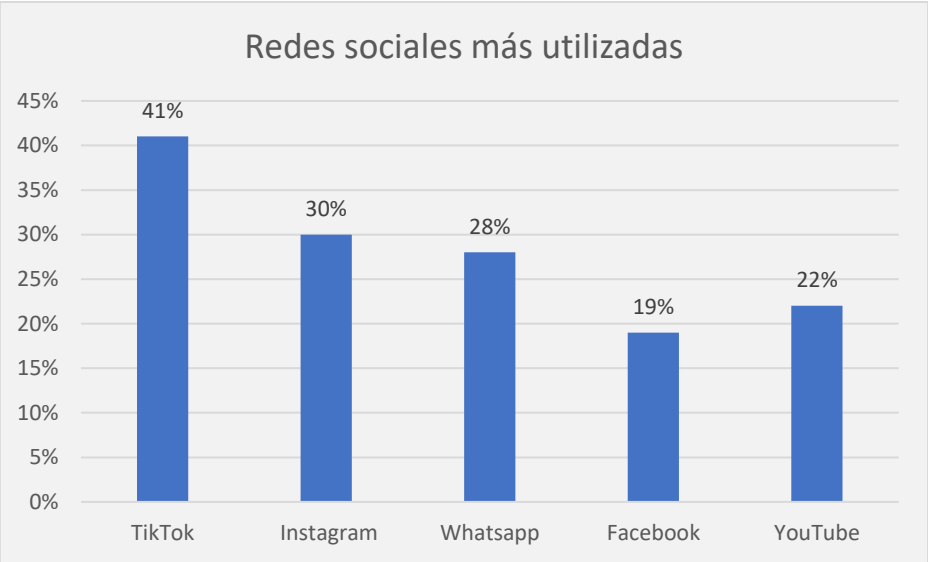
En promedio, los encuestados pasan entre 3 a 6 horas diarias utilizando internet y redes sociales. Los niños y adolescentes que utilizan dispositivos demasiado tiempo pueden descuidar sus relaciones sociales en el mundo real. Esto puede conducir a problemas de aislamiento social y soledad, además de la privación de sueño lo que afecta negativamente el rendimiento académico, el comportamiento y la salud mental de los niños y adolescentes.

Pregunta 3. ¿Desde qué edad usas Internet y redes sociales?



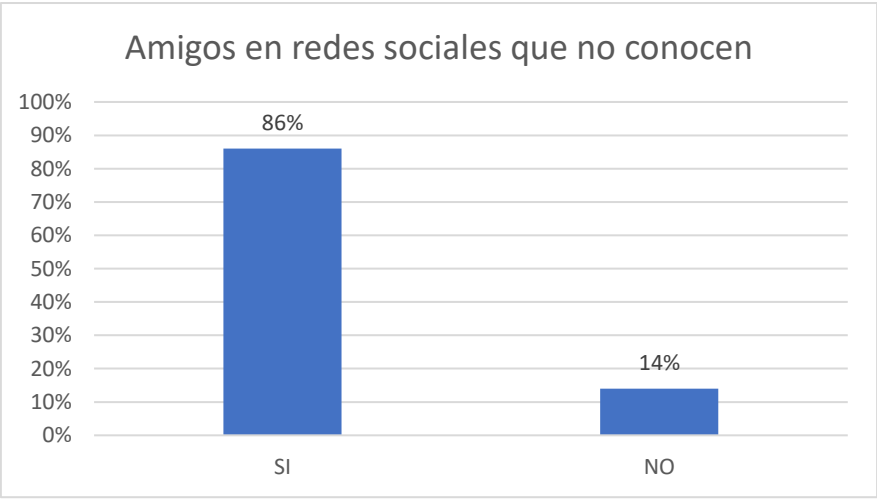
La mayoría comenzó a usar internet y redes sociales entre los 13 y 15 años. Esto indica que entran al espacio digital desde jóvenes, lo cual podría llevar a que los jóvenes y adolescentes desarrollen una adicción a la web. Por ello, es esencial que haya una supervisión y educación adecuada para garantizar un uso seguro y equilibrado de estas plataformas.

Pregunta 4. ¿Qué red social utilizas más?



Las redes sociales más populares entre los encuestados son TikTok, Instagram y WhatsApp. Facebook parece ser más utilizada por los de mayor edad, mientras que TikTok predomina en los más jóvenes. Lo que afecta gravemente a este grupo de edad, ya que TikTok es una aplicación que puede ser muy adictiva con contenido dañino ya sea violento, pornográfico o de odio. Además esta red social puede hacer que los niños se sientan inseguros sobre ellos mismos, ya que se encuentran expuestos a imágenes de personas que parecen ser perfectas.

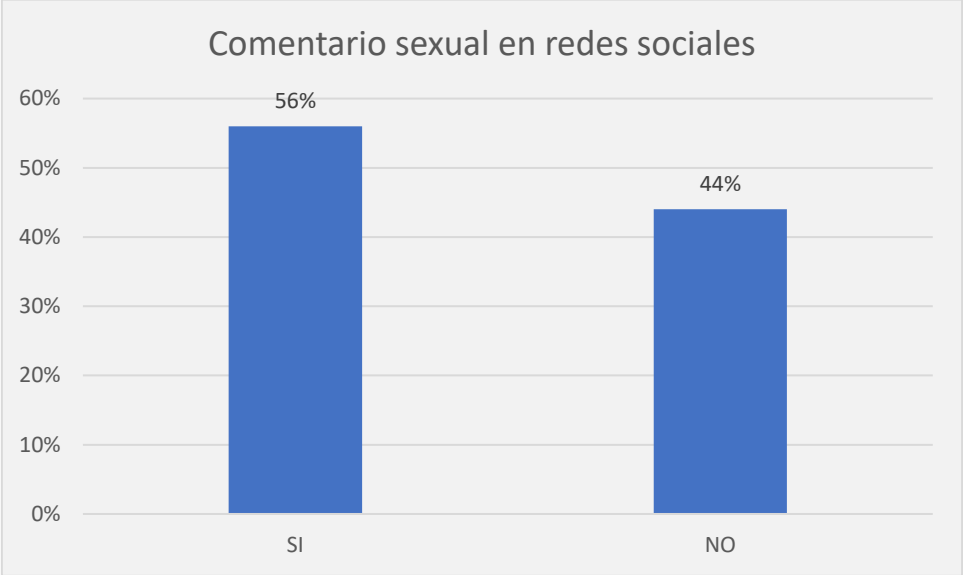
Pregunta 5. ¿Tienes amigos en tus redes sociales que no conoces en persona?



Más de un 60% de los encuestados tiene amigos o contactos en redes sociales que no conocen en persona. Esto conlleva a facilitar interacciones riesgosas con extraños; considerando que resulta difícil saber quién es realmente una persona en línea, para los niños y adolescentes, el riesgo es aún mayor, ya que son más susceptibles a la manipulación o a caer en trampas de individuos malintencionados.

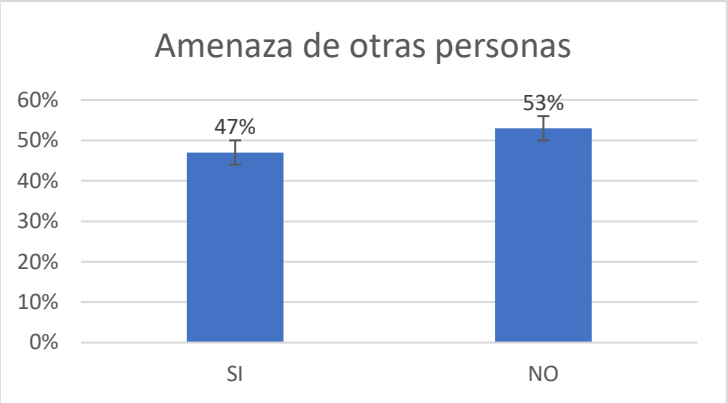
Asimismo, el permitir que desconocidos accedan a los perfiles personales puede aumentar el riesgo de ciberacoso o ciberbullying.

Pregunta 6. ¿Has recibido algún comentario sexual que te haya incomodado usando internet?



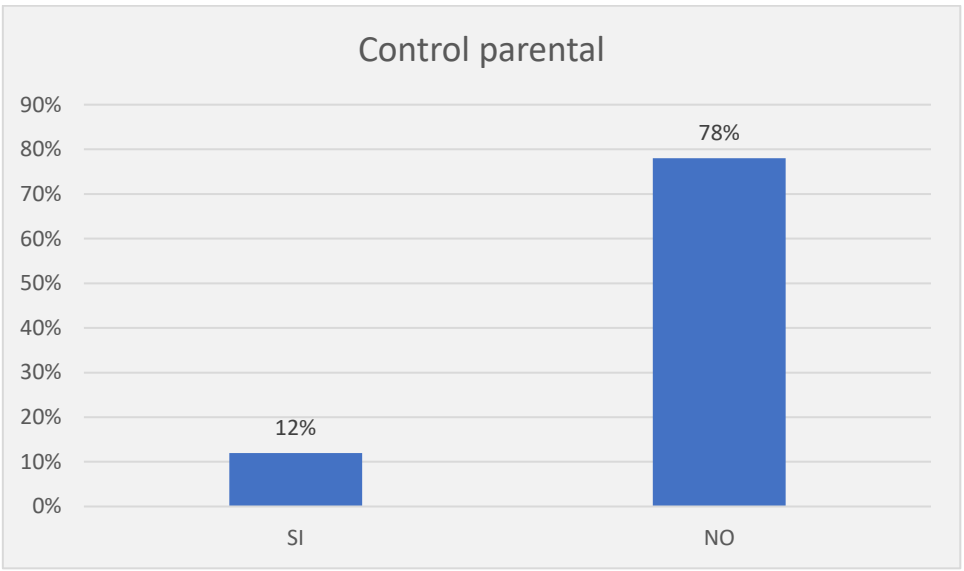
Un porcentaje no despreciable reporta haber recibido comentarios (51%). Esto indica que ya han experimentado ciberacoso o situaciones negativas en línea. SI en un 66%

Pregunta 7. ¿Has recibido alguna amenaza de otra persona usando el Internet?



Los encuestados manifiestan en su mayoría no haber recibido amenazas de otras personas al usar el Internet y las redes sociales, sin embargo, hay que tomar en cuenta que los niños no siempre son conscientes de los riesgos y no tienen experiencia para protegerse del ciberacoso o del grooming.

Pregunta 8. ¿Tus padres, representante, controlan el tiempo que pasas en Internet?



La mayoría (78%) afirma que sus padres no controlan o limitan su tiempo en internet. Esto sugiere una posible falta de supervisión parental sobre sus actividades en línea.

Los resultados exponen que los jóvenes del cantón Cañar se encuentran muy conectados y activos en redes sociales, en algunos casos de forma excesiva o sin supervisión, lo que

puede facilitar que enfrenten diversos riesgos y problemas asociados al uso de estas tecnologías.

CAPÍTULO IV

El presente capítulo expone el desarrollo del análisis de riesgos a través de la metodología Magerit con el objetivo de identificar, evaluar y mitigar los riesgos específicos a los que están expuestos los niños y adolescentes del cantón Cañar.

4.1. Identificación de activos

Uno de los primeros pasos en Magerit es la identificación y valoración de activos. En el contexto de niños y adolescentes, los activos no son solo los dispositivos que utilizan, sino su propia privacidad, bienestar psicológico y su seguridad física.

Por ello, se ha considerado la identidad digital, las comunicaciones privadas, los propios menores y sus dispositivos tecnológicos, dado que estos componentes están intrínsecamente ligados a la privacidad, integridad y bienestar de este grupo en el entorno digital. La siguiente matriz contiene los activos de información en materia de la ciberseguridad de los niños y adolescentes, para luego determinar las vulnerabilidades y enfocarse en los activos más críticos.

Tabla 1. Matriz de identificación de activos. Fuente: Autoría Propia.

ID_Activo	Activo	Descripción	Tipo de Activo
Act - 001	Redes Sociales (WhatsApp, Facebook, Instagram, TikTok)	Aplicaciones y sitios web de redes sociales comúnmente utilizados por niños y adolescentes	[SW] Software - Aplicaciones informáticas
Act – 002	Software de navegación	Navegadores web utilizados para acceder a internet y redes sociales.	[SW] aplicaciones (software)
Act – 003	Identidad digital (perfiles de redes sociales)	Información como contraseñas, correos.	[D] Datos / Información
Act – 004	Mensajes privados	Conversaciones y mensajes directos entre usuarios en redes sociales	[D] Datos / Información
Act – 005	Dispositivos digitales	Equipos utilizados por niños y adolescentes para conectarse a internet	[HW] Equipamiento informático (hardware)
Act – 006	Conexiones a Internet	Medios de acceso a la web y redes sociales, como Wi-Fi doméstico, datos móviles, entre otros.	[COM] Redes de comunicaciones

Act - 007	Niños y adolescentes	Niños y adolescentes que hacen uso de internet y redes sociales	[P] Personal

4.2. Escala de calificación de los activos de información

La identificación de los activos de alta criticidad permite enfocar los esfuerzos de evaluación de amenazas y riesgos en aquellos que podrían ocasionar el mayor impacto a los niños y adolescentes.

Para evaluar la criticidad de los activos identificados, se estableció una escala de calificación mixta.

Tabla 2. Evaluación de los activos. Fuente: Autoría Propia.

Criterio	**Valor**
Despreciable	1-5
Bajo	6-10
Medio	11-15
Alto	16-20
Muy Alto	21-25

Adicionalmente, se utilizaron criterios cualitativos que representan las principales propiedades de seguridad de la información:

- Disponibilidad: capacidad de los usuarios autorizados de acceder al activo cuando lo requieran.
- Integridad: exactitud y completitud del activo.
- Confidencialidad: limitación del acceso solo a personal autorizado.
- Autenticidad: verificación de la identidad del usuario que crea o modifica el activo.
- Trazabilidad: registro histórico de acciones relacionadas con el activo.

Esta combinación de escalas cuantitativa y cualitativa permite determinar integralmente el nivel de criticidad de cada activo, considerando tanto su valor numérico como los posibles daños sobre los aspectos más sensitivos de la información.

Los activos con mayor puntaje en la escala serán priorizados en el posterior análisis de amenazas y riesgos.

La siguiente matriz califica a los activos en base a los 5 criterios antes mencionados, los activos a tomar en cuenta son aquellos que tienen la calificación de alto y muy alto.

Tabla 3. Calificación de activos. Fuente: Autoría Propia.

Tipo de activo	**Código**	**Activo**	**Dimensiones de Valoración**	Despreciable	1-5
				Bajo	6-10
				Medio	11-15
				Alto	16-20
				Muy Alto	21-25

			Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	**TOTAL /25**
[SW] Software - Aplicaciones informáticas	Act-001	Redes Sociales (WhatsApp, Facebook, Instagram, TikTok)	3	4	5	5	3	20
	Act-002	Software de navegación 4	3	3	3	2	1	12
[D] Datos / Información	Act - 003	Identidad digital (perfiles de redes sociales)	4	5	5	5	3	22
	Act - 004	Mensajes privados	4	5	5	4	3	21
[HW] Equipamiento informático (hardware)	Act - 005	Dispositivos Digitales	3	2	5	4	1	15
[COM] Redes de comunicaciones	Act – 006	Conexiones a Internet	3	4	4	2	2	15
[P] Personal	Act - 007	Niños y adolescentes	5	5	5	5	5	25

4.3. Análisis de amenazas de acuerdo a la metodología Magerit

Tras identificar los activos, el siguiente paso es categorizar las amenazas, describiéndolas según de acuerdo al catálogo de la metodología Magerit.

En este punto, se presenta un inventario detallado de amenazas que apuntan a los activos altos y muy altos; en la siguiente matriz se presenta el código de identificación de la amenaza, los tipos de activos que podrían ser afectados por esta y las áreas de seguridad de la información que podrían ser comprometidas.

La tabla 4 permite asociar cada amenaza identificada con los activos específicos que podrían verse afectados por la materialización de la misma, relacionar las amenazas con activos facilita visualizar qué activos enfrentan mayor exposición al tener múltiples amenazas vinculadas.

Tabla 4. Amenazas Magerit asociadas a los activos. Fuente: Autoría Propia.

ID_Activo	Activo	Código Amenaza	Amenaza
Act - 001	Redes Sociales (WhatsApp, Facebook, Instagram, TikTok)	[E.23]	Errores de mantenimiento de equipos
		[E.1]	Errores de los usuarios
		[E.19]	Fugas de información
		[E.15]	Alteración accidental de la información
		[E.20]	Vulnerabilidades de los programas (software)
Act – 002	Software de navegación	[A.8]	Difusión de software dañino
Act – 003		[A.29]	Extorsión

	Identidad digital (perfiles de redes sociales)	[A.5]	Suplantación de la identidad del usuario
Act – 004	Mensajes privados	[A.13]	Repudio
		[A.18]	Destrucción de información
		[A.19]	Divulgación de información
		[A.29]	Extorsión
Act – 005	Dispositivos digitales	[A.23]	Manipulación de los equipos
		[A.11]	Acceso no autorizado
		[E.25]	Pérdida de equipos
		[A.25]	Robo
		[A.26]	Ataque destructivo
Act – 006	Conexiones a Internet	[A.12]	Análisis de tráfico
		[A.14]	Interceptación de información (escucha)
Act - 007	Niños y adolescentes	[A.30]	Ingeniería social
		[A.19]	Divulgación de información
		[A.29]	Extorsión

La matriz permitió determinar las intersecciones amenazas-activos que permiten priorizar la gestión de riesgos, enfocándose en proteger los activos con mayor exposición a múltiples peligros. Se observa que la amenaza de extorsión está vinculada a activos como la identidad digital, mensajes privados y el grupo de niños y adolescentes, destacando así la necesidad de implementar controles rigurosos.

Amenazas como "errores de usuarios" o "ataques de malware" tienen un alcance más amplio y pueden afectar a varios activos esenciales. El activo crucial "Niños y adolescentes" incluye la amenaza denominada "ingeniería social", que abarca técnicas variadas como phishing y hacking, entre otras.

4.4. Análisis de riesgos

El nivel de cada riesgo se calcula combinando el impacto (daño potencial) y la probabilidad (frecuencia esperada) en una escala cuantitativa. Los riesgos críticos e inadmisibles requieren máxima prioridad en mitigación, dado que implican un impacto sumamente alto y probabilidad significativa de ocurrencia.

Las calificaciones tanto del impacto como de la probabilidad se determinan en escalas cuantitativas:

Tabla 5. Escala de valoración para determinar el impacto. Fuente: Autoría Propia.

Impacto	Descripción	Valor
Bajo	El riesgo contiene efectos bajos, es decir que no afecta al activo	**1**
Medio	Cuando se presenta tendría consecuencias mínimas	**2**
Alto	Causa un daño mayor	**3**
Muy alto	La materialización del riesgo causa un daño mayor en la ejecución de procesos y el cumplimiento de los objetivos.	**4**
Crítico	La materialización del riesgo dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos	**5**

Tabla 6. Escala de valoración para determinar la probabilidad de ocurrencia de las amenazas. Fuente: Autoría Propia.

Probabilidad	Frecuencia	Valor
Raro	No se presenta en los últimos cinco años	**1**
Improbable	No se presenta en los últimos dos años	**2**

Posible	Una vez al año	**3**
Probable	Mensualmente	**4**
Casi seguro	A diario	**5**

Así mismo, se ha establecido una escala de valoración para determinar el nivel del riesgo:

Tabla 7. Escala de valoración del riesgo. Fuente: Autoría Propia.

Riesgo	**Descripción**	**Valor**
Bajo	Riesgo aceptable	**1-5**
Medio	Riesgo tolerable	**6-10**
Alto	Riesgo inaceptable	**11-15**
Crítico	Riesgo inadmisible	**16-20**

El análisis de riesgos implica la valoración integral de las amenazas potenciales sobre los activos críticos previamente identificados.

Para cada amenaza detectada se evalúa su probabilidad de ocurrencia en base a factores como: antecedentes, capacidad técnica de los atacantes, controles existentes, vulnerabilidades específicas, entre otros. Asimismo, se estima el impacto o daño que provocaría cada amenaza en caso de materializarse sobre uno o más activos críticos. Este proceso permite orientar la priorización de recursos y esfuerzos hacia los riesgos más altos e intolerables para la privacidad y seguridad de los menores en el ámbito digital. Los controles y salvaguardas se enfocarán en aquellas amenazas que pueden provocar el mayor daño potencial.

Tabla 8. Matriz de riesgos. Fuente: Autoría Propia.

Activo	Código Amenaza	Amenaza	Impacto	Probabilidad	Riesgo
Redes Sociales (WhatsApp, Facebook, Instagram, TikTok)	[E.23]	Errores de mantenimiento de equipos	**3**	**1**	3
	[E.1]	Errores de los usuarios	**4**	**3**	**12**
	[E.19]	Fugas de información	**5**	**3**	**15**
	[E.15]	Alteración accidental de la información	4	2	8
	[E.20]	Vulnerabilidades de los programas (software)	**4**	**2**	**8**
Software de navegación	[A.8]	Difusión de software dañino	**5**	**2**	**10**
Identidad digital (perfiles de redes sociales)	[A.29]	Extorsión	**5**	**4**	**20**
	[A.5]	Suplantación de la identidad del usuario	**4**	**3**	**12**
Mensajes privados	[A.13]	Repudio	**3**	**3**	**9**
	[A.18]	Destrucción de información	**5**	**4**	**20**
	[A.19]	Divulgación de información	**5**	**4**	**20**

	[A.29]	Extorsión	5	3	15
Dispositivos digitales	[A.23]	Manipulación de los equipos	**4**	**2**	**8**
	[A.11]	Acceso no autorizado	**3**	**2**	**6**
	[E.25]	Pérdida de equipos	**4**	**3**	**12**
	[A.25]	Robo	**4**	**3**	**12**
	[A.26]	Ataque destructivo	**5**	**1**	**5**
Conexiones a Internet	[A.12]	Análisis de tráfico	**3**	**2**	**6**
	[A.14]	Interceptación de información (escucha)	**5**	**3**	**15**
Niños y adolescentes	[A.30]	Ingeniería social	5	3	**15**
	[A.29]	Extorsión	5	4	20
	[A.19]	Divulgación de información	5	4	20

4.5. Salvaguardas y contramedidas

Para mitigar los riesgos críticos e inadmisibles identificados, se plantearon salvaguardas y contramedidas de la metodología Magerit, tanto a nivel de procedimientos como de software y hardware. Con el fin de reducir la probabilidad y el impacto potencial de las amenazas más críticas, mitigando los riesgos hasta niveles tolerables para proteger la privacidad, integridad y bienestar de los niños y adolescentes en el ámbito digital. La siguiente matriz excluye a aquellos.

Tabla 9. Matriz de salvaguardas. Fuente: Autoría Propia.

Activo	Código Amenaza	Amenaza	Riesgo	Control Magerit	Control Específicos
Redes Sociales (WhatsApp, Facebook, Instagram, TikTok)	[E.1]	Errores de los usuarios	**12**	Formación y concienciación	Protocolo de Uso Seguro y Capacitación para Redes Sociales
	[E.19]	Fugas de información	**15**	Protección de la Información	Configuraciones de privacidad en las redes sociales y el Internet
	[E.20]	Vulnerabilidades de los programas (software)	**8**	Protección de las Aplicaciones Informáticas	mantener las aplicaciones de redes sociales actualizadas a la última versión en dispositivos móviles y computadoras.
Software de navegación	[A.8]	Difusión de software dañino	**10**	Herramienta contra código dañino	Antivirus

Identidad digital (perfiles de redes sociales)	[A.29]	Extorsión	**15**	Protección de la Información	Sistema de Protección y Verificación de Identidad
	[A.5]	Suplantación de la identidad del usuario	**12**	Identificación y autenticación	Configuraciones de privacidad en las redes sociales y el Internet
	[A.13]	Repudio	**9**	Herramienta de monitorización de contenidos	Software de control parental Educación y conciencia
Mensajes privados	[A.18]	Destrucción de información	**20**	Copias de seguridad de los datos (backup)	Aplicación de restauración de mensajes
	[A.19]	Divulgación de información	**20**	Protección de la Información	Denuncia basada en el artículo 230 del COIP
	[A.29]	Extorsión	15	Formación y concienciación	Software de control parental
	[A.23]	Manipulación de los equipos	**8**	Protección de los Equipos Informáticos	Protección Física y Autenticación de Dispositivos
Dispositivos digitales	[A.11]	Acceso no autorizado	**6**	Control de acceso lógico	Contraseñas seguras

	[E.25]	Pérdida de equipos	**12**	Protección de los Equipos Informáticos	Sistema de Rastreo, Bloqueo y Recuperación de Dispositivos
	[A.25]	Robo	**12**	Copias de seguridad de los datos (backup)	Sistema de Rastreo, Bloqueo y Recuperación de Dispositivos
	[A.12]	Análisis de tráfico	**6**	Seguridad Wireless (WiFi)	Sistema de Cifrado y Anonimización de Tráfico en Red
Conexiones a Internet	[A.14]	Interceptación de información (escucha)	**15**	Seguridad Wireless (WiFi)	Navegación en Redes Confiables
	[A.30]	Ingeniería social	**15**		Capacitaciones en ciberseguridad
Niños y adolescentes	[A.29]	Extorsión	20	Formación y concienciación	Herramientas de control parental
	[A.19]	Divulgación de información	20		Configuraciones de Privacidad

4.5.1. Efectividad del control con el riesgo

La siguiente matriz de efectividad de control de riesgo presenta la eficiencia del control, calificada de forma cuantitativa. Sin embargo es necesario mencionar la aplicación de controles reduce pero no elimina los riesgos; se calcula además el riesgo residual, que representa el nivel remanente luego de implementar las salvaguardas.

Activo	Cód. Amenaza	Amenaza	Riesgo	Control Magerit	Control Específicos	Eficiencia del Control Bajo = 1 Medio = 2 Óptimo = 3	Riesgo Residual
Redes Sociales (WhatsApp, Facebook, Instagram, TikTok)	[E.1]	Errores de los usuarios	**12**	Formación y concienciación	Protocolo de Uso Seguro y Capacitación para Redes Sociales	2	6
	[E.19]	Fugas de información	**15**	Protección de la Información	Configuraciones de privacidad en las redes sociales y el Internet	3	5
	[E.20]	Vulnerabilidades de los programas (software)	**8**	Protección de las Aplicaciones Informáticas	mantener las aplicaciones de redes sociales actualizadas a la última versión en dispositivos móviles y computadoras.	2	4

Software de navegación	[A.8]	Difusión de software dañino	**10**	Herramienta contra código dañino	Antivirus	3	3
Identidad digital (perfiles de redes sociales)	[A.29]	Extorsión	**15**	Protección de la Información	Sistema de Protección y Verificación de Identidad	2	8
	[A.5]	Suplantación de la identidad del usuario	**12**	Identificación y autenticación	Configuraciones de privacidad en las redes sociales y el Internet	2	6
	[A.13]	Repudio	**9**	Herramienta de monitorización de contenidos	Software de control parental Educación y conciencia	2	4
Mensajes privados	[A.18]	Destrucción de información	**20**	Copias de seguridad de los datos (backup)	Aplicación de restauración de mensajes	2	10
	[A.19]	Divulgación de información	**20**	Protección de la Información	Denuncia basada en el artículo 230 del COIP	3	6
	[A.29]	Extorsión	15	Formación y concienciación	Software de control parental	3	5

	[A.23]	Manipulación de los equipos	**8**	Protección de los Equipos Informáticos	Protección Física y Autenticación de Dispositivos	3	2
Dispositivos digitales	[A.11]	Acceso no autorizado	**6**	Control de acceso lógico	Contraseñas seguras	3	2
	[E.25]	Pérdida de equipos	**12**	Protección de los Equipos Informáticos	Sistema de Rastreo, Bloqueo y Recuperación de Dispositivos	2	6
	[A.25]	Robo	**12**	Copias de seguridad de los datos (backup)	Sistema de Rastreo, Bloqueo y Recuperación de Dispositivos	3	4
	[A.12]	Análisis de tráfico	**6**	Seguridad Wireless (WiFi)	Sistema de Cifrado y Anonimización de Tráfico en Red	2	3

Conexiones a Internet	[A.14]	Interceptación de información (escucha)	**15**	Seguridad Wireless (WiFi)	Navegación en Redes Confiables	1	15
	[A.30]	Ingeniería social	**15**		Capacitaciones en ciberseguridad	2	7
Niños y adolescentes	[A.29]	Extorsión	20	Formación y concienciación	Herramientas de control parental	3	6
	[A.19]	Divulgación de información	20		Configuraciones de Privacidad	2	10

Las salvaguardas propuestas incluyeron contramedidas de tipo técnico, procedimental y legal, siendo medidas como la configuración de privacidad, software de control parental y capacitación en ciberseguridad las más relevantes. El cálculo del riesgo residual evidenció que la implementación de controles reduce el riesgo, pero no lo elimina totalmente, por lo que se requiere un proceso continuo de gestión de riesgos.

4.6. Proceso para la creación de la guía.

Basado en el proceso del análisis de riesgos bajo la metodología Magerit, así como el estudio de vulnerabilidades, amenazas y riesgos de ciberseguridad en niños y adolescentes, se detalla el proceso a seguir para la construcción de una guía de prevención de riesgos de ciberseguridad derivado del uso del Internet y las redes sociales para los niños y adolescentes del cantón Cañar.

- Establecer los objetivos: La guía debe proporcionar lineamientos claros para promover un uso seguro, responsable y ético de las tecnologías digitales y prevenir incidentes de seguridad.
- Basarse en la investigación teórica y el análisis de riesgos realizado para incluir las amenazas y vulnerabilidades más relevantes para el contexto local
- Redactar contenidos claros y concisos, con un lenguaje adaptado al público objetivo. Incluir material gráfico, infografías, listas de verificación, actividades prácticas, etc.
- Integrar medidas técnicas, educativas y procedimentales obtenidas de la literatura, normativa existente y aportes de expertos.

Conclusiones

Como resultado de este trabajo, se realizó una revisión teórica sobre vulnerabilidades, amenazas, riesgos y controles de ciberseguridad de niños y adolescentes en el ámbito legal, técnico y familiar.

Luego de realizar el proceso de análisis y gestión de riesgos a través de la metodología Magerit, se identificó que existen amenazas con un riesgo de ocurrencia muy alto, estas son las relacionadas con las interacciones con desconocidos en línea, extorsión, divulgación de información, supervisión parental deficiente sobre sus actividades digitales. Esto evidencia la necesidad de implementar medidas educativas y técnicas específicas para mitigar estas amenazas en la población joven de la localidad.

Basado en lo anterior, se destaca también la necesidad de mayor supervisión y orientación por parte de padres y tutores sobre las actividades digitales de los niños y adolescentes.

De esta manera, a través de la creación de la guía de riesgos de ciberseguridad proporciona información sobre los riesgos de la ciberseguridad y cómo mantenerse seguros en línea.

Recomendaciones

Se recomienda a la Carrera de Ingeniería de Sistemas de Información de la Universidad Católica de Cuenca extensión Cañar:

- Continuar con proyectos de concientización de riesgos de ciberseguridad a la ciudadanía, a través de talleres prácticos y teóricos.

- Capacitar a los estudiantes de la carrera de Ingeniería de Sistemas de Información sobre seguridad informática.

Referencias

Aguilar, C. A., & Fonseca, I. S. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electrónica Educare (Educare Electronic Journal)*, 1-24.

Alfaro Mairena, A. P., & Paniagua Solís, S. (01 de 01 de 2022). *179.0.219.172.* Obtenido de 179.0.219.172/: http://179.0.219.172/bitstream/handle/20.500.13077/805/AUDITORIA%20DE%20CONTROL%20INTERNO.pdf?sequence=1&isAllowed=y

Alonso, Y. M. (2020). EL CONTROL PARENTAL EN LA REGULACIÓN DEL USO DE LAS REDES SOCIALES EN ADOLESCENTES: INFLUENCIA DE LAS REDES SOCIALES EN LAS RELACIONES ENTRE ESTOS Y ESTAS. *Universidad de La Laguna*, 1-27.

Amigo, B. M., Gutiérrez, J. L., & Ríos, N. G. (2018). *Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, 1-20.

Bartolomé, I. S. (01 de 07 de 2019). *uvadoc.uva.es.* Obtenido de uvadoc.uva.es:

https://uvadoc.uva.es/bitstream/handle/10324/37736/TFG-I-1213.pdf?sequence=1&isAllowed=y

Candau, J. (2021). Ciberseguridad, Evolución y tendencias. *IEEE*, 460-494.

Cardoso, A. T., Falcke, D., & Mosmann, C. P. (2019). Sexting en la adolescencia: percepciones de los padres. *Ciencias Psicológicas*, 19-31.

Claes, F., & Deltell, L. (2019). Museo social en España: redes sociales y webs de los museos estatales. *El profesional de la información*, 1-10.

CÓDIGO ORGÁNICO INTEGRAL PENAL. (17 de 02 de 2021). *www.defensa.gob.ec.* Obtenido de www.defensa.gob.ec: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

CONSEJO NACIONAL PARA LA IGUALDAD INTEGENERACIONAL. (01 de 09 de 2020). *www.igualdad.gob.ec.* Obtenido de www.igualdad.gob.ec: https://www.igualdad.gob.ec/wp-content/uploads/downloads/2020/09/pol%C3%ADtica_publica_internet_segura.pdf

Contreras Olea, G. A. (01 de 01 de 2022). *dspace.utb.edu.ec.* Obtenido de dspace.utb.edu.ec: http://dspace.utb.edu.ec/bitstream/handle/49000/12551/E-UTB-FAFI-SIST-000355.pdf?sequence=1&isAllowed=y

Cordero Ruiz, N. F. (22 de 03 de 2021). *ebuah.uah.es.* Obtenido de ebuah.uah.es: https://ebuah.uah.es/dspace/bitstream/handle/10017/49563/TFM_Cordero_Ruiz_2021.pdf?sequence=1&isAllowed=y

DATAREPORTAL. (11 de 02 de 2023). *datareportal.com*. Obtenido de datareportal.com: https://datareportal.com/reports/digital-2023-ecuador

Departamento de Ciencias e Ingeniería de la Computación. (27 de 08 de 2017). *cs.uns.edu.ar.* Obtenido de cs.uns.edu.ar: https://cs.uns.edu.ar/materias/iocp/downloads/Apuntes/Unidad%203%20-%20Internet.pdf

Díaz, V. M., & Almenara, J. C. (2019). Las redes sociales en educación: desde lai nnovación a la investigación educativa. *Revista Iberoamericana de Educación a Distancia*, 25-33.

FIP. (16 de 08 de 2018). *www.ifj.org.* Obtenido de www.ifj.org: https://www.ifj.org/fileadmin/user_upload/Fake_News_-_FIP_AmLat.pdf

Gallego, F., Malamud, O., & Eleches, C. P. (2020). Parental monitoring and children's internet use: The role of information, control and cuestion. *Journal of Public Economics*, 1-18.

García, A., & Alexey, I. (01 de 01 de 2022). *repositorio.ucv.edu.pe.* Obtenido de repositorio.ucv.edu.pe: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/103847/Abad_GIA-SD.pdf?sequence=1&isAllowed=y

Garcia, C. L. (02 de 24 de 2023). *www.reporteindigo.com*. Obtenido de www.reporteindigo.com: https://www.reporteindigo.com/piensa/sexting-que-hacer-si-tus-fotos-eroticas-se-filtran-y-como-practicarlo-de-forma-segura/

Garitaonandia, C., Iglesias, E. J., Xuarros, I. K., & Larrañaga, N. (2020). Menores conectados y riesgos online: contenidos inadecuados, uso inapropiado de la información y uso excesivo de internet. *Profesional de la información*, 1-10.

Gastelo Fernandez, E. J., & Rodríguez Flores , A. H. (01 de 01 de 2023). *repositorio.uss.edu.pe.* Obtenido de repositorio.uss.edu.pe: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10888/Gastelo%20Fernandez%20Edin%20%26%20Rodr%c3%adguez%20Flores%20Alfredo.pdf?sequence=1&isAllowed=y

González, A. L., & García, N. H. (2019). IMPACTO DE LA TECNOLOGÍA EN LA SOCIEDAD: EL CASO DE ECUADOR. *UNIVERSIDAD Y SOCIEDAD | Revista Científica de la Universidad de Cienfuegos*, 176-182.

Hernández Vera, D. A. (01 de 01 de 2019). *bdigital.uexternado.edu.co.* Obtenido de bdigital.uexternado.edu.co: https://bdigital.uexternado.edu.co/server/api/core/bitstreams/0f36afdf-40eb-4cba-a38f-5827107779a9/content

Hernández, O. (01 de 05 de 2020). *conexo.org.* Obtenido de conexo.org: https://conexo.org/wp-content/uploads/2020/06/Seguridad-Digital-Conceptos-y-Herramientas-B%C3%A1sicas-Mayo-2020.pdf

Hurtado, M. (2018). GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT. *Universidad Piloto de Colombia. Hurtado. Metodología de Análisis de Riesgo. 1*, 1-12.

ICMEC. (01 de 01 de 2018). *www.icmec.org.* Obtenido de www.icmec.org: https://www.icmec.org/wp-content/uploads/2019/12/Material-Sobre-Abuso-Sexual-Infantil-Legislacion-Modelo-y-Revision-Global-9na-Ed.pdf

ISO/IEC . (01 de 10 de 2022). *cdn.standards.iteh.ai.* Obtenido de cdn.standards.iteh.ai: https://cdn.standards.iteh.ai/samples/80585/7bca93ac16fd426a9bc717cadc9284d9/ISO-IEC-27005-2022.pdf

Jain, A. K., Sahoo, ·. S., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review. *Complex & Intelligent Systems* , 1-21.

Jain, G., & Rani, N. (2019). Awareness Learning Analysis of Malware and Ransomware in Bitcoin. En P. P. Singh, & T. S. W., *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)* (págs. 765-776). Springer Nature Singapore Pte Ltd.

Kahimise, J., & Shava, F. B. (2020). An Analysis of Social Networking Threats . *ProQuest*, 576-583.

Kaspersky. (13 de 06 de 2023). *latam.kaspersky.com*. Obtenido de latam.kaspersky.com: https://latam.kaspersky.com/safe-kids

Kaur, D., Uslu, S., & Durresi, A. (2021). Trust-Based Security Mechanism for Detecting Clusters of Fake Users in Social Networks. *Web, inteligencia artificial y aplicaciones de red: actas de los talleres de la 33.ª Conferencia internacional sobre redes y aplicaciones de información avanzada (WAINA-2019) 33 . Publicaciones internacionales de Springer, 2019.*, 641-650.

Keles, B., McCrae, N., & Grealish, A. (2019). A systematic review: the influence of social media on depression, anxiety and psychological distress in adolescents. *Internacional Journal of Adolescence and Youth*, 79-93.

Koohang, A., Nord, J. H., Floyd, K., & Paliszkiewiz, J. (2022). Social media privacy and security concerns: Trust and awareness. *Issues in Information Systems*, 253-264.

Llauce Valdera, L. (01 de 01 de 2022). *repositorio.unprg.edu.pe.* Obtenido de repositorio.unprg.edu.pe: https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/10411/Llauce_Valdera_Luciano.pdf?sequence=1&isAllowed=y

Lozano, D. C., Mendoza, D. V., & Vega, C. R. (2020). Adicción a redes sociales y ciberbullying en los adolescentes . *Muro de la Investigación*, 34-44.

Luzuriaga, R. F., & Santiago, I. R. (2022). Grooming e inteligencia emocional en adolescentes. ¿Puede el desarrollo emocional en la escuela prevenir este tipo de acoso cibernético? *Revista Latinoamrecina de Tecnología Educativa*, 45-58}.

Méndez, A. G. (01 de 01 de 2022). *uvadoc.uva.es.* Obtenido de uvadoc.uva.es: https://uvadoc.uva.es/bitstream/handle/10324/54724/TFG-B.%201871.pdf?sequence=1&isAllowed=y

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (18 de 04 de 2020). *www.gobiernoelectronico.gob.ec.* Obtenido de www.gobiernoelectronico.gob.ec: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (18 de 04 de 2020). *www.gobiernoelectronico.gob.ec.* Obtenido de www.gobiernoelectronico.gob.ec: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Montes Vozmediano, M., Pastor Ruiz , Y., Martín Nieto, R., & Atuesta Reyes, J. (2020). Smartphone y redes sociales: una aproximación a los usos, vulnerabilidades y riesgos durante la adolescencia en España y Colombia. *Revista ESPACIOS*, 44-59.

Moreira, M. A., & Rodríguez, J. R. (01 de 01 de 2022). *riull.ull.es.* Obtenido de riull.ull.es: https://riull.ull.es/xmlui/handle/915/31096

Moretti, C., & Herkovits, D. (2021). De víctimas, perpetradores y espectadores: una meta-etnografía de los roles en el ciberbullying. *Cad. Saúde Pública*, 1-18.

Mullo Mullo, E. (01 de 01 de 2022). *dspace.utb.edu.ec.* Obtenido de dspace.utb.edu.ec: http://dspace.utb.edu.ec/bitstream/handle/49000/14239/E-UTB-FAFI-SIST.INF-000129.pdf?sequence=1&isAllowed=y

Muñoz Aguilar, J. H. (01 de 10 de 2022). *repositorio.pucesa.edu.ec.* Obtenido de repositorio.pucesa.edu.ec: https://repositorio.pucesa.edu.ec/bitstream/123456789/3839/1/78273.pdf

Noguera, M., Edotti, L., Galofre, A., Martínez, L., & Gonzales, P. G. (2023). La pornografía infantil en entornos digitales en Colombia. *Tejidos Sociales*, 1-11.

OEA. (11 de 11 de 2021). *www.oas.org.* Obtenido de www.oas.org: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Paschke, K., Austermann, M. I., Simon-Kutscher, K., & Thomasius, R. (2021). Adolescent gaming and social media usage before and during the COVID-19 pandemic. *Sucht*, 13-22.

Pedriatía Salud . (08 de 04 de 2018). *www.pediatriasalud.com*. Obtenido de www.pediatriasalud.com: https://www.pediatriasalud.com/grooming/

Pineda, A. C., & Torres, C. J. (2020). *Sexting: signo de identidad juvenil en la sociedad digital.* España: ecoedicion.

Prieto, A. T. (2019). Ciberadicciones. Adicción a las nuevas tecnologías (NTIC). *Comisión de Formación Continuada*, 131-141.

Realpe, M. E., & Cano, J. (2020). Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia. *Urosario*, 105-113.

Russell M Viner, A. A.-G.-L. (2019). Roles of cyberbullying, sleep, and physical activity in mediating the effects of social media use on mental health and wellbeing among young people in England: a secondary analysis of longitudinal data. *The Lancet Salud de niños y adolescentes*, 1-12.

Sandoval, M. A., & Rodríguez, D. M. (24 de 11 de 2022). *repository.libertadores.edu.co.* Obtenido de repository.libertadores.edu.co: https://repository.libertadores.edu.co/bitstream/handle/11371/5402/Pe%c3%b1a_Sanchez_2022.pdf?sequence=1&isAllowed=y

SARANGO, W. X. (01 de 06 de 2021). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/20665/1/UPS%20-%20TTS416.pdf

Slavko, A. S., Zavhorodnia, V. M., & Shevchenko, N. A. (2020). Protection of One's Honor, Dignity, and Business Reputation on Social Networks: Issues and Ways to Resolve Them. *International Journal of Media and Information Literacy*, 205-216.

Thakur, K., Tseng, J., & Hayajneh, T. (2019). Cyber Security in Social Media: Challenges and the Way Forward. *Cyber Security in Social Media*, 41-49.

Thilini B. G. Herath, P. K., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *MDPI*, 1-18.

Tusa, F., & Durán, M. B. (2019). La era de la DESINFORMACIÓN y de las noticias falsas en el ambiente político ecuatoriano de transición: un análkisis de caso. *USFQ Press*, 18-41.

Villavicencio, J. C., Álava, V. P., & Loor, M. P. (2019). LA CIBERADICCIÓN EN LA CONDUCTA DE LOS ESTUDIANTES. . *ATLANTE*, 1-13.

Villota García S, S. C., Zamora López, G. G., & Llanga Vargas, E. F. (2019). USO DEL INTERNET COMO BASE PARA EL APRENDIZAJE. *Atlante.*, 1-7.

Wartberg, L., Thomasius, R., & Paschke, K. (2021). The relevance of emotion regulation, procrastination, and perceived stress for problematic social media use in a representative sample of children and adolescents. *Computer in Human Behavior*, 1-7.

Xylogiannopoulos, K. F., Karampelas, P., & Alhajj, R. (2020). A password creation and validation system for social media platforms bases on big data analytics. *Journal of Ambient Intelligence and Humanized Computing* , 53-73.

Zafar, A. B., Javed, X. L., & Kifayat, Z. J. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, 139-154.

ANEXO 1

A. TÍTULO
Guía de prevención de riesgos de ciberseguridad derivado del uso del internet y las redes sociales en niños y adolescentes del cantón Cañar

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Inteligencia de Negocios	
		Sistemas de Información	
		Gobierno y administración de tecnologías de información	
		Auditoría Informática	
		Seguridad Informática	x
		Redes y comunicación	
		Arquitectura de Hardware	
		Arquitectura de desarrollo de software	
		Ingeniería de Software	
		Gestión y gobierno de proyectos de tecnología informática	
		Ingeniería de requerimientos	
		Algoritmos y programación	
		Ciencias exactas y naturales (Matemáticas, Física, Química, Biología, etc.)	
		Modelaje y simulación	

C. PLANTEAMIENTO DEL PROBLEMA

Desde hace algunos años, el uso del internet así como las redes sociales se ha vuelto cada vez más común entre niños y adolescentes del cantón Cañar. Sin embargo, el acceso a la tecnología también conlleva riesgos en términos de seguridad y privacidad en línea. Es por ello, que resulta importante diseñar una guía de prevención de riesgos de ciberseguridad para estos grupos.

A pesar de que existen diferentes iniciativas que buscan educar sobre la seguridad en línea, en el cantón Cañar en las instituciones, no se cuenta con una guía específica que brinde información sobre los peligros y riesgos asociados con el uso de internet y las redes sociales por parte de niños y adolescentes. De acuerdo con Calderas (2022) manifiesta que esta falta de orientación puede resultar en situaciones como la exposición a contenidos inapropiados, acoso cibernético, robo de identidad o incluso ser víctimas de fraudes en línea. En consecuencia, es necesario abordar este problema a través de la elaboración de una guía de prevención de riesgos de ciberseguridad dirigida a niños y adolescentes del cantón Cañar, que contenga información relevante y actualizada sobre cómo utilizar las herramientas tecnológicas de manera segura y responsable. Esta guía no solo ayudará prevenir problemas relacionados con la seguridad en línea, sino que también fomentaría el uso consciente y responsable de la tecnología en la población joven del cantón, beneficiando a las diferentes unidades educativas.

D. OBJETIVO GENERAL

Generar una guía de prevención de riesgos de ciberseguridad derivado del uso del internet y las redes sociales en niños y adolescentes del cantón Cañar

E. OBJETIVOS ESPECÍFICOS

1. *Realizar un estudio teórico sobre las amenazas y vulnerabilidades más comunes de las redes sociales y su impacto en los niños y adolescentes*
2. *Realizar un tratamiento de gestión de riesgos de ciberseguridad sobre el uso del internet y redes sociales en los niños y adolescentes utilizando un marco de referencia reconocido.*
3. *Crear una guía estratégica para prevenir y mitigar las amenazas y vulnerabilidades en los adolescentes del cantón Cañar*

F. JUSTIFICACIÓN

Los nativos digitales, tienden a confiar demasiado en la tecnología, y es por eso que publican información personal que podría ser usada sin su consentimiento. Siendo un grupo vulnerable ante varios riesgos, ya que a menudo carecen de la experiencia y la educación necesaria para protegerse adecuadamente en línea. Además, los padres y tutores pueden o no estar al tanto de todos los peligros cibernéticos que sus hijos enfrentan a diario y cómo prevenirlos.

Por lo tanto, es importante proporcionar una guía de prevención de riesgos de ciberseguridad específica para los niños y adolescentes del cantón Cañar, que ayude a los jóvenes a entender los peligros en línea y a tomar medidas para protegerse de ellos. Esta guía incluirá información sobre la privacidad en línea, el acoso cibernético, la suplantación de identidad en línea, el grooming, la exposición a contenidos inapropiados, entre otros.

En definitiva, será de gran utilidad para los jóvenes, padres, tutores y educadores del cantón Cañar, al proporcionar información clara y práctica para protegerse en línea y disfrutar de internet y las redes sociales de manera segura y responsable.

G. ALCANCE

El alcance de la presente investigación, va a permitir generar una propuesta de guía de prevención de riesgos de ciberseguridad enfocada a los niños y adolescentes del cantón Cañar, misma que proporcione métodos de seguridad para reducir los riesgos y vulnerabilidades de ellos, analizando el uso de las redes sociales como Facebook, Tiktok e Instagram y las páginas web a las que ellos acceden. Para lo que se trabajará con una muestra de estudiantes de algunas instituciones educativas del cantón Cañar.

H. CONCEPTOS RELACIONADOS

Seguridad Digital

Este concepto hace referencia a un grupo de métodos y/o estrategias que tienen la finalidad de proteger y controlar los datos, la forma en la que se comunican y la información que se maneja actualmente en los diferentes medios sociales. Volviéndose cada vez más importante garantizando además la continuidad de los negocios y de sus clientes, sin embargo es necesario

que se tenga en cuenta que para lograr una seguridad digital efectiva, es importante efectuar medidas de seguridad (Hernández, 2020).

Redes Sociales

De acuerdo con Marín & Cabero (2019), las redes sociales son herramientas utilizadas a nivel mundial, de manera especial en los jóvenes. Cambiando la forma en que la sociedad interactúa, convirtiéndose en una parte integral del diario vivir de muchas personas; han alcanzado un gran impacto tanto en marketing como en la publicidad. Sin embargo, es fundamental tener en cuenta los riesgos asociados con el uso de las redes sociales, como la exposición a contenidos inapropiados, el acoso cibernético, la suplantación de identidad y otros peligros en línea (págs. 26-28)

Factores de riesgo de las redes sociales

Social media ofrece una gran cantidad de beneficios así como también riesgos. Algunos de ellos enfocados en los adolescentes son la adicción es decir que se vuelven adictivas afectando a los niños y adolescentes ya que les afecta en el sueño, la productividad; el ciberacoso; la suplantación de la identidad; la privacidad y seguridad; contenido inapropiado, entre otros (Amigo, Gutiérrez, & Ríos, 2018).

Ciberseguridad

"Telecomunicaciones [UIT] la define como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías." (Flores Cantos, Pozo Curo, Flores Conislla, & Adauto Medina, 2021)

Sexting

Este concepto es definido por Ojeda et al. (2020) como una práctica en la cual se comparten imágenes o videos sexualmente explícitos mediante dispositivos electrónicos, puede ser consensuado entre dos personas que comparten una relación íntima y deciden enviar imágenes o videos sexualmente explícitos para excitarse o mantener la intimidad a distancia. Sin embargo, también puede ocurrir de manera no consensuada cuando una persona comparte imágenes o videos de otra persona sin su consentimiento.

Ciberacoso

Cortés (2020) define al ciberacoso, como acoso en línea o acoso digital, se refiere al comportamiento agresivo, intencional y repetitivo realizado a través de medios digitales, como las redes sociales, el correo electrónico, los mensajes de texto, los foros en línea, los juegos en línea, entre otros.

El ciberacoso puede tomar muchas formas, como el envío de mensajes ofensivos, la difusión de rumores, la creación de perfiles falsos, la publicación de fotos o videos humillantes, el hackeo de cuentas personales, la exclusión de grupos en línea, entre otros. El impacto del ciberacoso puede ser devastador para las víctimas, que pueden experimentar problemas emocionales, psicológicos y físicos, como depresión, ansiedad, aislamiento social, e incluso puede llevar al suicidio (pág. 3)

Adolescentes

La palabra adolescencia hace mención a una nueva etapa de la vida en la que cambian cualidades tanto del cuerpo como de la mente (Pàmpols, 2020). “Esta etapa se encuentra entre la niñez y la edad adulta, en el rango de 10 a 14 años la adolescencia temprana y la tardía de 15 a 19 años” (Pérez & Santiago, 2002, pág. 16)

I. TRABAJOS RELACIONADOS

El analizar el impacto negativo del internet y las diferentes redes sociales en niños y adolescentes es fundamental, ya que de esta manera se puede identificar vulnerabilidades y amenazas. Siendo así un factor social que afecta a nivel mundial; es por ello que varios autores han desarrollado investigaciones que van en beneficio de los jóvenes en vista de que se abordan problemáticas de seguridad informática.

Claes & Deltell en el año (2019), realizan un análisis de la comunicación digital en museos, determinando el uso de las diferentes redes sociales y páginas webs en estudiantes, en donde definen que el Internet debe ser usado por los estudiantes para fines académicos y se debe limitar el acceso a las redes sociales en establecimientos y museos. Tomando esta investigación como referencia para el análisis de indicadores que los autores utilizan para analizar las páginas web.

Así mismo, un artículo realizado por Luque & Herrero (2019), analizan el impacto de la tecnología en adolescentes en Ecuador, realizando el estudio de manera cualitativa, mediante una prueba de test-retest. Los autores efectúan 6 preguntas referentes al uso de los dispositivos móviles, las redes sociales, la conectividad y la comunicación, considerando también la afectación de las redes sociales, en donde ultiman que si en las diferentes escuelas, colegios e incluso universidades no se hace hincapié del buen

manejo de la tecnología, no se puede asegurar un buena productividad de los jóvenes. Siendo este artículo una línea base para analizar la encuesta y sobre todo sus indicadores.

Por otro lado Torres (2021) analiza y evalúa el impacto de los ciberataques en adolescentes en el rango de 12 a 17 años de edad en la ciudad de Quito, a través de la metodología descriptiva utilizando la técnica cuantitativa para realizar una encuesta, utilizando también herramientas para la generación de ciberataques. El autor analiza los artículos del COIP relacionados a la ciberseguridad, además obtiene como resultado que los ataques que se dan con mayor frecuencia en un 42% de los adolescentes son los enlaces enviados por correo electrónico para el robo de información. El documento antes mencionado permite identificar los artículos del Código Orgánico Integral Penal que se enfocan en los delitos informáticos, mismos que se tomará como valor de referencia para la construcción de la guía.

Un documento elaborado por Area et al. en el año (2022), permite visualizar una guía de buenas prácticas, misma que posee estrategias para el buen uso de las TIC dirigida no solamente a los niños, sino también a los padres de familia, así como a los docentes. De esta manera este trabajo, permite considerar los puntos abordados así como las imágenes que presentan para la elaboración de la guía.

En cuanto a investigaciones nacionales, Peña & Sánchez en el año (2022), elaboran una guía de buenas prácticas con el objetivo de mitigar los riesgos a los adolescentes entre el rango de 13 a 15 años, utilizando una metodología cualitativa, que permite identificar en primera instancia la manera en la que los jóvenes utilizan el internet. Sin embargo, con la aplicación de la guía se pudo ultimar el cambio en cuanto al manejo de las redes sociales, siendo este favorable.

El documento antes mencionado, sirve como referencia de cómo estructurar la guía de buenas prácticas enfocada a los adolescentes.

J. METODOLOGÍA

La metodología a utilizar en el presente trabajo de investigación será de carácter mixto, realizando un análisis del uso de las redes sociales para la construcción de una guía de buenas prácticas a través de una encuesta enfocada a los niños y adolescentes relacionadas al uso de las redes sociales (Facebook, Instagram, Tiktok, Snapchat). Así como una entrevista dirigida a los docentes de las unidades educativas de bachillerato del cantón Cañar.

K. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	MES						
		I	II	III	IV	V	VI	MEDIOS DE VERIFICACIÓN
1.	Realizar un estudio teórico sobre las amenazas y vulnerabilidades más comunes de las redes sociales y su impacto en los niños y adolescentes							

1.1.	Bases Teóricas sobre los riesgos de las redes sociales, ciberdelitos, entre otros.	x						Lista de documentos almacenados en la herramienta Mendeley
1.2.	Estado del arte de documentos relacionados al tema de investigación		x					Matriz de Excel
2.	Investigar las políticas y regulaciones relacionadas a la ciberseguridad							
2.1.	Determinar las políticas del COIP relacionadas a la ciberseguridad			x				Fuentes de información de páginas web oficiales
2.2.	Selección de un marco de referencia			x	x			Matriz comparativa
2.3.	Selección de una metodología para el análisis de riesgos de las redes sociales en los niños y adolescentes del cantón Cañar							Matriz comparativa
3.	Crear una guía estratégica para prevenir y mitigar las amenazas y vulnerabilidades en los adolescentes del cantón Cañar							
3.1.	Definir la estructura de la guía					x		Documento pdf
3.2.	Generar la guía de buenas prácticas					x	x	Documento pdf

L. DECLARACIÓN FINAL

Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES

DIRECTOR:	Ing. Cristhian Flores Urgilés
ESTUDIANTE 1	Fernanda Michaelle Narváez Ochoa

N. FIRMAS DE RESPONSABILIDAD

Lugar:	
Fecha:	

Firmas:

Nombre: Cristhian Humberto Flores Urgilés	Nombre: Fernanda Michaelle Narváez Ochoa

CC: **Director del Proyecto**	C.C.: 0302358601 **Estudiante / Egresado**

O. APROBACIÓN	
Firmas:	
Nombre: CC: **Primer Par Revisor**	Nombre: C.C.: **Segundo Par Revisor**

P. REFERENCIAS

Referencias

Alfaro, A. C. (2020). Acoso escolar, ciberacoso y las nuevas tecnologías de la información y la comunicación. *Revista Cubana de Medicina General Integral.*, 1-9.

Amigo, B. M., Gutiérrez, J. L., & Ríos, N. G. (2018). *Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, 1-20.

Claes, F., & Deltell, L. (2019). Museo social en España: redes sociales y webs de los museos estatales. *El profesional de la información*, 1-10.

Díaz, V. M., & Almenara, J. C. (2019). Las redes sociales en educación: desde lai nnovación a la investigación educativa. *Revista Iberoamericana de Educación a Distancia*, 25-33.

González, A. L., & García, N. H. (2019). IMPACTO DE LA TECNOLOGÍA EN LA SOCIEDAD: EL CASO DE ECUADOR. *UNIVERSIDAD Y SOCIEDAD | Revista Científica de la Universidad de Cienfuegos*, 176-182.

Hernández, O. (01 de 05 de 2020). *conexo.org.* Obtenido de conexo.org: https://conexo.org/wp-content/uploads/2020/06/Seguridad-Digital-Conceptos-y-Herramientas-B%C3%A1sicas-Mayo-2020.pdf

Mirabal, J. W. (01 de 08 de 2022). *prcrepository.org.* Obtenido de prcrepository.org: https://prcrepository.org/xmlui/bitstream/handle/20.500.12475/1680/An%C3%A1lisis%20del%20caso%20USA%20v.%20Steve%20Waithe.pdf?sequence=1

Moreira, M. A., & Rodríguez, J. R. (01 de 01 de 2022). *riull.ull.es.* Obtenido de riull.ull.es: https://riull.ull.es/xmlui/handle/915/31096

Ojeda, M., Rey, R. d., Walrave, M., & Vandebosch, H. (2020). Sexting en adolescentes: Prevalencia y comportamientos. *Revista Científica de Educomunicación*, 9-19.

Pàmpols, C. F. (2020). Identidad, Juventud y Crisis: el concepto de crisis en las teorías. *Revista Española de Sociología (RES)*, 11-26.

Pérez, S. P., & Santiago, M. A. (23 de 10 de 2002). *ccp.ucr.ac.cr.* Obtenido de ccp.ucr.ac.cr: https://ccp.ucr.ac.cr/bvp/pdf/adolescencia/Capitulo%20I.pdf

Sandoval, M. A., & Rodríguez, D. M. (24 de 11 de 2022). *repository.libertadores.edu.co.* Obtenido de repository.libertadores.edu.co: https://repository.libertadores.edu.co/bitstream/handle/11371/5402/Pe%c3%b1a_Sanchez_2022.pdf?sequence=1&isAllowed=y

SARANGO, W. X. (01 de 06 de 2021). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/20665/1/UPS%20-%20TTS416.pdf

ANEXO 2

GUÍA
DE PREVENCIÓN
DE RIESGOS DE CIBERSEGURIDAD

DEL USO DEL INTERNET Y LAS REDES SOCIALES

Universidad Católica de Cuenca

CCPD-C
CONSEJO CANTONAL DE PROTECCIÓN DE DERECHOS CAÑAR

Prólogo

En una era en la que el flujo de información es constante y la digitalización se ha convertido en un pilar fundamental de nuestra cotidianidad, la ciberseguridad emerge como uno de los desafíos más prominentes del siglo XXI. Las amenazas virtuales no solo ponen en riesgo la integridad de sistemas y redes, sino que, lo que es más preocupante, comprometen la seguridad y privacidad de las personas en su vida diaria.

La presente guía está dirigida a toda la comunidad del cantón Cañar, desde estudiantes, docentes, padres de familia y funcionarios públicos, hasta ciudadanos en general. Su objetivo es proporcionar información y recomendaciones sobre cómo proteger su privacidad, seguridad e integridad personal al utilizar Internet y las redes sociales.

La Universidad Católica de Cuenca extensión Cañar, comprometida con la formación integral de sus estudiantes, promueve la cultura de la ciberseguridad a través de esta guía. Con esta iniciativa, la Universidad busca contribuir a la protección de sus estudiantes, docentes y colaboradores de los riesgos de ciberseguridad.

Asímismo, el Consejo Cantonal de Protección de Derechos del cantón Cañar, responsable de garantizar el ejercicio de los derechos de los niños, niñas y adolescentes, se suma a esta iniciativa para promover la seguridad de los menores de edad en el mundo digital. Con esta guía, el Consejo busca sensibilizar a padres de familia y docentes sobre la importancia de la prevención del ciberacoso y el sexting.

Esta guía es el fruto de esa alianza. Aquí, se abordan de manera integral los riesgos asociados con el uso del internet y las redes sociales, proporcionando consejos prácticos, ejemplos concretos y medidas preventivas que permitirán a los usuarios reconocer amenazas y actuar de manera adecuada.

Alentamos a cada lector a que se sumerja en estas páginas no solo con la mente abierta al aprendizaje, sino también con el compromiso de ser multiplicador de esta información vital. Juntos, como comunidad, podemos construir un espacio digital más seguro para todos.

Autor: Fernanda Michaelle Narváez Ochoa

CIBERSEGURIDAD

¿Qué es la Ciberseguridad?

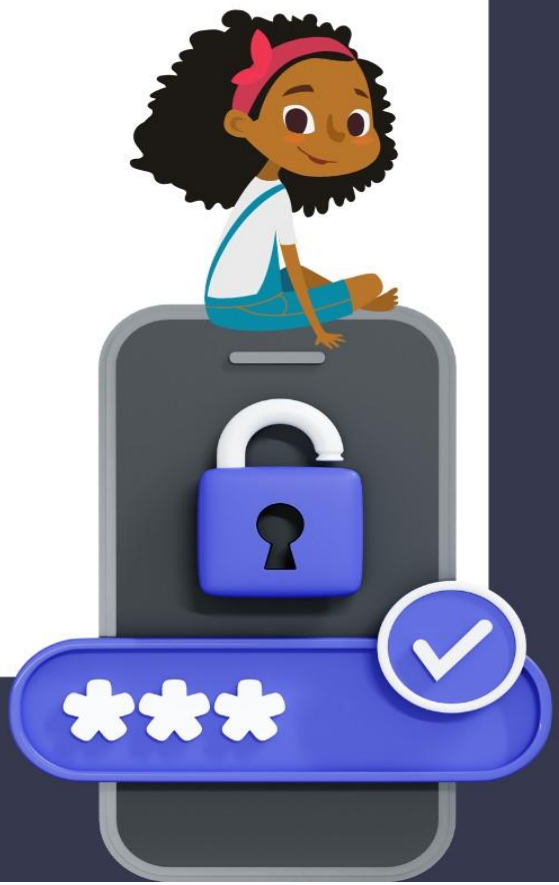
La ciberseguridad es la práctica de proteger la información digital, los sistemas y las redes de los ataques cibernéticos. Los ataques cibernéticos son intentos de robar, dañar o interrumpir los sistemas informáticos que pueden causar daños económicos, pérdida de datos y privacidad, e incluso daños físicos.
La ciberseguridad es importante para todos, desde individuos hasta empresas y gobiernos.

Las personas necesitan proteger su información personal y financiera. Las empresas necesitan proteger sus datos comerciales y sistemas informáticos. y los gobiernos necesitan proteger su infraestructura crítica, como las redes eléctricas y los sistemas de defensa.

Seguridad en redes sociales y el Internet

En la actualidad, las redes sociales y el Internet forman parte integral de nuestra vida cotidiana. Nos permiten comunicarnos con amigos y familiares, compartir información, aprender cosas nuevas y realizar muchas otras actividades. Sin embargo, estas plataformas también pueden ser un riesgo para nuestra seguridad.
La seguridad en redes sociales y el Internet es el proceso de proteger la información personal y financiera de los usuarios. Los ciberdelincuentes pueden aprovechar las redes sociales y el Internet para cometer delitos, como el robo de identidad, el fraude el ciberacoso, entre otros.

La seguridad en línea ayuda a proteger a los usuarios de contenido dañino, como malware, phishing y spam. Además de proteger la privacidad de los usuarios de las diferentes redes sociales.



LA PRIVACIDAD EN LÍNEA

La privacidad en línea es el derecho de controlar la información personal que se comparte en línea. Esto incluye información como el nombre, la dirección, el número de teléfono, el correo electrónico, las fotos y los videos.
La privacidad en línea es importante por varias razones. En primer lugar, ayuda a proteger a las personas de los ciberdelincuentes, que pueden utilizar la información personal para cometer fraude, robo de identidad u otros delitos.

En segundo lugar, ayuda a proteger la privacidad de las personas, ya que no quieren que todos sepan todo sobre ellas. En tercer lugar, ayuda a proteger la libertad de expresión, ya que las personas pueden estar menos dispuestas a expresarse si temen que su información personal pueda ser utilizada en su contra.

¿Cómo proteger la privacidad en línea?

- **No compartas información personal con personas que no conoces.**
- **Evita hacer clic en enlaces o abrir archivos adjuntos de correos electrónicos o mensajes de texto de fuentes desconocidas.**
-
- **Utiliza contraseñas seguras y únicas para todas tus cuentas.**
- **Activa la verificación en dos pasos para tus cuentas importantes.**
- **Mantén tu software actualizado.**
- **Selecciona cuidadosamente las configuraciones de privacidad en tus cuentas en línea.**
- **Sé consciente de los riesgos de la privacidad en línea.**

Privacidad en redes sociales

Las redes sociales recopilan una gran cantidad de información sobre sus usuarios, incluyendo nombres, direcciones, números de teléfono, números de tarjetas de crédito, etc. Esta información puede ser utilizada para fines comerciales, como la publicidad dirigida, o para fines fraudulentos, como el robo de identidad.

CONTRASEÑAS SEGURAS

Una contraseña es una combinación de letras, números y símbolos que se utiliza para autenticar la identidad de un usuario. Las contraseñas se utilizan en una variedad de aplicaciones, incluyendo sitios web, cuentas de correo electrónico, redes inalámbricas y computadoras.

Una contraseña segura es una combinación de letras, números y símbolos que es difícil de adivinar. Ayudan a proteger tu información personal y financiera de los ciberdelincuentes.

¿Cómo crear contraseñas seguras?

- **Utiliza una combinación de letras, números y símbolos.** Las contraseñas que solo utilizan letras o números son más fáciles de adivinar.
- **Elige una contraseña que sea larga, al menos 12 caracteres.** Las contraseñas más largas son más difíciles de adivinar.
- **No utilices palabras comunes o fáciles de adivinar, como tu nombre, tu fecha de nacimiento o el nombre de tu mascota**.
- **No uses la misma contraseña para todas tus cuentas**. Si una de tus contraseñas se ve comprometida, todas tus cuentas se verán en riesgo.

GEOLOCALIZACIÓN EN REDES SOCIALES

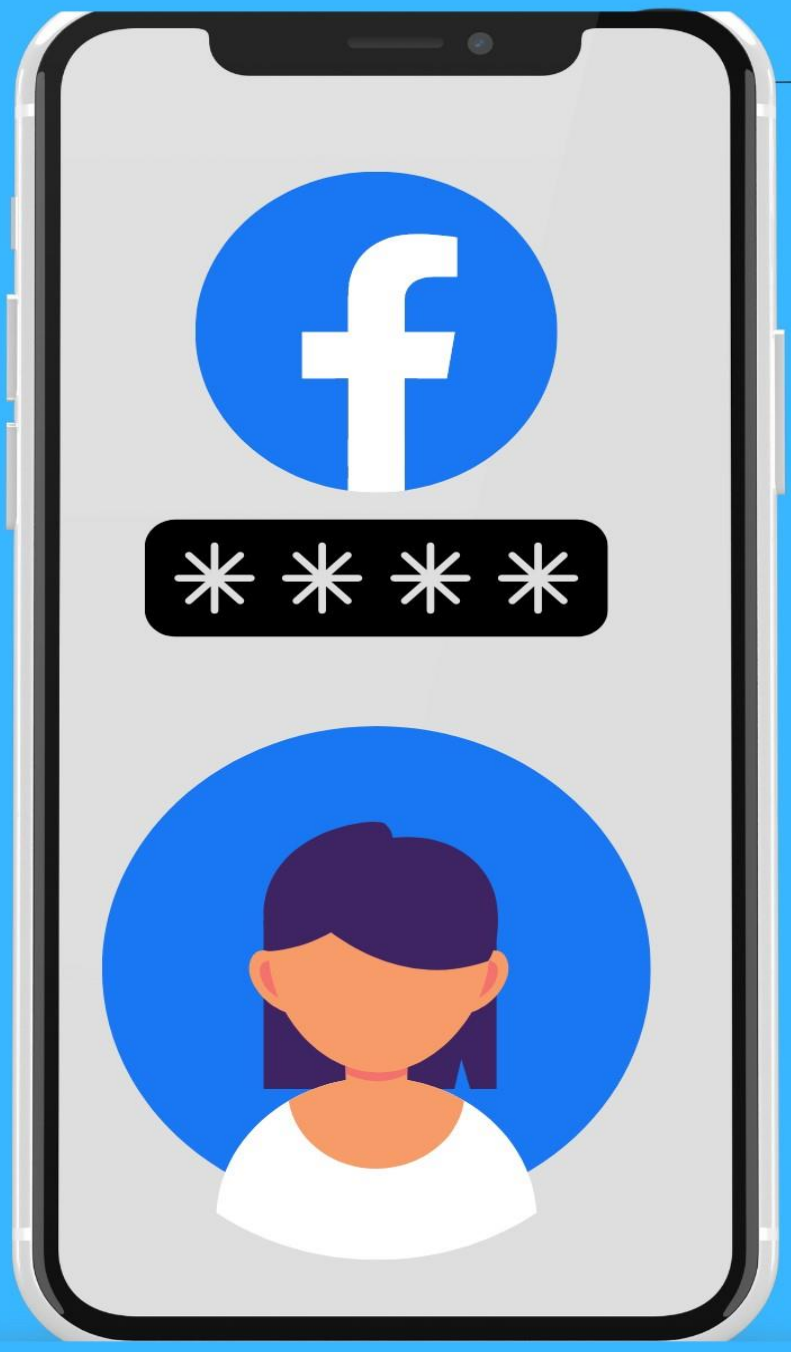
La geolocalización en redes sociales es una tecnología que permite a los usuarios compartir su ubicación geográfica con otros usuarios. Esto se puede hacer de forma explícita, al indicar la ubicación en una publicación o comentario, o de forma implícita, al permitir que la aplicación de redes sociales acceda a los datos de geolocalización del dispositivo.

Al compartir su ubicación con otros usuarios, estos están revelando información personal sobre sus movimientos y actividades. Esto puede ser utilizado por personas malintencionadas para rastrearlos, acosarlos o incluso robarles.

Un ciberdelincuente puede rastrear a un usuario que ha compartido su ubicación en las redes sociales. Esto puede ser utilizado para robarle su información personal o para atacarlo físicamente

Amenazas más comunes de las redes sociales para los niños y adolescentes

ROBO DE INFORMACIÓN



¿Qué es el robo de información?

El robo de información en línea es el acto de obtener información personal o confidencial de forma ilícita. Esta información puede incluir nombres, direcciones, números de teléfono, números de tarjetas de crédito, contraseñas, datos bancarios y otros datos sensibles.
El robo de información se refiere a cuando alguien, sin permiso, toma datos o información personal de otro. Imagina que tienes una caja secreta con cosas valiosas dentro, y alguien la abre y se lleva lo que hay dentro sin que tú lo sepas. En el mundo digital, esa "caja" podría ser tu computadora, tu teléfono o incluso tu perfil en un juego en línea, y las "cosas valiosas" podrían ser tus fotos, mensajes, o información sobre quién eres.

Tipos de información que suelen ser robados

Información Personal: Como tu nombre completo, dirección, fecha de nacimiento, o el nombre de tu escuela. Es como si alguien conociera detalles sobre ti sin que tú se los hayas contado.

Información Financiera: Aunque los niños no suelen tener tarjetas de crédito, pueden saber detalles de las tarjetas de sus padres si alguna vez han comprado algo en línea. Esta información es como el dinero en una alcancía; no querrías que alguien la tomara sin permiso

Información Corporativa: Es como el "secreto" de una empresa. Si los padres tienen un negocio o los docentes trabajan en una escuela, hay datos e información que sería un problema si alguien más los tuviera.

Es vital educar a los niños sobre la importancia de mantener segura su información y ser cautelosos sobre con quién y cómo la comparten, tanto en el mundo real como en el digital. Por otro lado, es esencial estar informados y ser proactivos para proteger la información de la familia y la institución educativa.

Consecuencias del Robo de información

Consecuencias Financieras

En el mundo digital, si alguien toma la información de las tarjetas de los padres, se puede gastar su dinero sin permiso. Si se sustrae la información bancaria o de tarjetas de crédito, pueden realizarse compras no autorizadas, dejándonos con pérdidas monetarias.

Daño a la Reputación

Si la información personal es expuesta, puede ser utilizada de manera malintencionada, afectando la imagen y la confianza que otros depositan en nosotros.

Violación de la Privacidad

La información robada puede revelar detalles íntimos de nuestra vida, exponiendo aspectos que preferiríamos mantener privados. Esto puede generar una sensación de vulnerabilidad y estrés.

¿Qué hacer en caso de ser víctima de robo de información?

1. **Cambiar las contraseñas**. Esto incluye sus contraseñas para sus cuentas bancarias, correo electrónico, redes sociales y cualquier otra cuenta en línea que utilice. Asegúrese de usar contraseñas seguras y únicas para cada cuenta.
2. **Revisión de Configuraciones de Seguridad:** Modificar las configuraciones de privacidad y seguridad en todas las cuentas, y asegúrese de que la información personal esté protegida.
3. **Comunicación y monitoreo de cuentas bancarias** Si la información rabada se ha divulgada o utilizado públicamente, es necesario informar a quienes pueden verse afectados. También es importante que los padres de familia revisen las cuentas bancarias o tarjetas de crédito.

Prevención y Buenas prácticas

La mejor manera de enfrentar el robo de información es evitar que suceda en primer lugar.

Uso de Software Antivirus y Firewall

El software antivirus es un programa que busca y elimina virus, malware y otras amenazas a la seguridad de su computadora. El software antivirus funciona escaneando los archivos de su computadora en busca de código malicioso. Si el software antivirus encuentra código malicioso, lo eliminará o lo pondrá en cuarentena.

Configuraciones de Seguridad y Privacidad en Aplicaciones y Redes Sociales

- Configure quién puede ver sus publicaciones. Puede elegir compartir sus publicaciones con todos, solo con sus amigos, o con una lista personalizada de personas.
- Evite compartir información personal en sus publicaciones. Esto incluye su dirección, número de teléfono o información de contacto de emergencia.
- Sea cuidadoso con lo que acepta de otros usuarios. No acepte solicitudes de amistad de personas que no conoce personalmente.
- Reporte cualquier actividad sospechosa. Si ve algo que le preocupa, comuníquese con el administrador de la red social.

PHISHING

¿Qué es el Phishing?

El phishing es una técnica de engaño utilizada por cibercriminales para hacer que las personas revelen información personal, como contraseñas, datos de tarjetas de crédito y otros detalles sensibles, al hacerles creer que están interactuando con una entidad confiable, como un banco, una red social o un proveedor de servicios.

Técnicas comunes de phishing

- Correos electrónicos falsificados: Estos imitan a organizaciones legítimas y solicitan al destinatario que actualice su información o haga clic en un enlace.
- Sitios web falsos: Páginas que imitan el aspecto de sitios web legítimos, diseñados para que los usuarios ingresen sus datos.
- Mensajes de texto o llamadas falsas: Solicitudes de información a través de SMS o llamadas telefónicas que pretenden ser de organizaciones confiables

¿Cómo Reconocer un Intento de Phishing?

- Direcciones de correo electrónico sospechosas o no coincidentes con la entidad que supuestamente lo envía.
- Saludos genéricos, como "Estimado cliente" en lugar de tu nombre real.
- Solicitudes urgentes o amenazantes para que actúes rápidamente.
- Enlaces que, al pasar el mouse por encima, muestran una URL diferente a la de la supuesta entidad.

URLs engañosas

Los piratas informáticos utilizan URL engañosas para engañar a las personas de varias maneras. Una forma común es enviar correos electrónicos o mensajes de texto que contienen un enlace a una URL engañosa. Cuando la persona hace clic en el enlace, es redirigida a un sitio web falso que se parece al sitio web legítimo. El sitio web falso puede pedirle a la persona que ingrese su información personal, como su nombre, dirección de correo electrónico o número de tarjeta de crédito

MALWARE

¿Qué es el malware?

El malware, término que proviene de la fusión de las palabras "malicious" (malicioso en inglés) y "software", se refiere a cualquier programa o archivo que está diseñado para dañar o explotar cualquier dispositivo, red o servicio, ya sea por razones maliciosas o por simple lucro.

Métodos de Propagación

Descargas de fuentes no confiables: Descargar software de sitios web no verificados o de terceros puede resultar en la instalación de malware.
Correos electrónicos y enlaces phishing: Archivos adjuntos maliciosos o enlaces que dirigen a sitios web infectados.
Dispositivos USB y otros medios extraíbles: Si contienen malware, pueden infectar cualquier sistema con el que entren en contacto.
Exploit kits y vulnerabilidades no parchadas: Atacan y explotan vulnerabilidades en software no actualizado.

Síntomas de una Infección de Malware

Rendimiento lento del dispositivo: Un dispositivo infectado a menudo funciona más lentamente debido a procesos maliciosos en segundo plano.
Publicidad no deseada o ventanas emergentes: Presencia constante de anuncios que no se originan de sitios web visitados.
Archivos o programas que actúan de manera inusual: Ejecuciones automáticas, cierres inesperados o comportamientos extraños.
Sistemas que se bloquean o reinician sin motivo aparente: Frecuentes pantallazos azules o reinicios espontáneos.

Prevención y Buenas Prácticas

Uso de soluciones antivirus y antimalware: Es vital mantener estos programas actualizados y realizar escaneos regulares.
Mantener sistemas y software actualizados: Las actualizaciones a menudo contienen parches para vulnerabilidades conocidas.
Evitar descargar archivos de fuentes desconocidas o no confiables: Siempre es mejor confiar en fuentes oficiales o sitios web reconocidos.

Tendencias y Amenazas Emergentes

En este mundo digital en constante evolución, es esencial estar al tanto de las nuevas formas de malware y las técnicas que los cibercriminales emplean

a. Juegos y Aplicaciones:
Es común que los niños descarguen y prueben nuevos juegos o aplicaciones en sus dispositivos.
Desafortunadamente, algunos de estos pueden contener malware disfrazado. Asegúrese de que sólo se descarguen aplicaciones de tiendas oficiales y de revisar las valoraciones y comentarios antes de hacerlo.

b. Juguetes Conectados:
Los juguetes que pueden conectarse a internet (como muñecos, relojes y otros dispositivos) pueden ser vulnerables a ataques si no se configuran adecuadamente. Es esencial cambiar las contraseñas predeterminadas y mantener el software de estos juguetes actualizado.

c. Phishing a través de Plataformas de Juegos:
En las plataformas de juegos online, es posible que los niños reciban mensajes con enlaces a "recompensas" o "bonificaciones". Estos pueden ser intentos de phishing. Es crucial enseñar a los niños a **no hacer clic en enlaces sospechosos** y a **no compartir información personal.**

d. Aplicaciones de Chat y Redes Sociales:
Con la creciente popularidad de las plataformas de comunicación en línea, los niños pueden ser blanco de mensajes maliciosos o enlaces que contienen malware. Es vital que configuren sus cuentas en modo privado y que sólo acepten mensajes de contactos conocidos.

PSYWARE

¿Qué es el spyware?

El spyware es un tipo de software malicioso diseñado específicamente para infiltrarse en dispositivos sin el consentimiento del usuario, con el propósito principal de recopilar y transmitir información personal, hábitos de navegación, y otros datos sin el conocimiento o permiso del usuario

Síntomas de una Infección de Spyware

- **Lentitud del sistema o conexión a internet:** El spyware, al operar en segundo plano, consume recursos del sistema, lo que puede resultar en un rendimiento notablemente más lento.
- **Publicidad emergente no deseada:** Aunque es más típico del adware, algunos spyware también pueden mostrar anuncios emergentes basados en la información recopilada de tus hábitos de navegación.
- **Cambios no autorizados en la configuración del sistema o del navegador:** Si tu página de inicio cambia sin tu intervención, o aparecen barras de herramientas desconocidas, podrías estar ante un caso de infección.
- **Redireccionamientos no deseados del navegador:** Si al navegar te encuentras con que constantemente te redirigen a sitios que no solicitaste, es probable que hay

Consecuencias del Spyware

Robo de Información Personal o Financiera: Una de las principales amenazas del spyware es la capacidad de recopilar datos personales, como contraseñas, números de tarjetas de crédito y otra información confidencial. Esta información puede ser utilizada para cometer fraudes o robo de identidad.

Monitoreo de Actividades en Línea: El spyware puede registrar las páginas que visitas, tus búsquedas en línea y otros hábitos de navegación. Esta información puede ser vendida a terceros, a menudo para fines publicitarios.

Prevención y Buenas Prácticas

Uso de Soluciones Antivirus y Antispyware Actualizadas: Asegúrate de tener instalado un software de seguridad de confianza y de mantenerlo actualizado. Estos programas detectan y eliminan la mayoría de las amenazas de spyware.

Evitar Descargar Software de Fuentes No Confiables: Siempre descarga software de sitios oficiales o de tiendas de aplicaciones reconocidas. Las descargas de sitios no confiables o de terceros tienen un mayor riesgo de contener spyware.

GROOMING

¿Qué es el grooming?

El grooming se refiere a una serie de acciones deliberadas y manipuladoras llevadas a cabo por un adulto, con el objetivo de establecer un lazo emocional con un menor, frecuentemente a través de internet. Esta relación puede ser construida por medio de la seducción, la manipulación, la amenaza o el engaño, con la finalidad de obtener un beneficio sexual, ya sea directamente con el menor o mediante la producción de material pornográfico infantil.

Síntomas y Señales de Alerta

Cambios de comportamiento en el menor: Un niño o adolescente que está siendo víctima de grooming podría mostrarse más retraído, ansioso o temeroso.

Actividad online a horas inusuales: Si un menor está conectándose a altas horas de la noche o en momentos que no son comunes para él, podría ser una señal de que está en contacto con alguien que lo está manipulando.

Secreto o protección excesiva sobre sus actividades en línea: Si de repente se muestra más reservado sobre lo que hace en la red, cierra rápidamente ventanas cuando alguien se acerca o se niega a compartir detalles sobre con quién está interactuando, son indicativos de que algo puede estar sucediendo.

Mecanismos y Estrategias del Groomer

El groomer suele presentarse como un amigo comprensivo y atento, buscando áreas de interés común con el menor para crear una conexión. Es común que pretendan ser otro joven para parecer menos amenazantes y más afines.

El agresor a menudo insta al menor a mantener su relación en secreto, afirmando que nadie más comprendería o que se trataría de "nuestro pequeño secreto". Esta táctica aísla al menor y lo hace más vulnerable.

Actuación ante Sospechas o Evidencias

Si se sospecha o se tiene evidencia de grooming, es fundamental mantener la calma y no borrar ninguna evidencia. Asegurarse de que el menor esté seguro y animarlo a hablar sobre lo sucedido, mostrando apoyo y comprensión.

Recopilar pruebas:

Guarda cualquier comunicación, fotografía o video relacionado con el presunto groomer, ya que podría ser crucial para una investigación posterior.

Acudir a las autoridades:

Es esencial denunciar el caso ante las autoridades competentes para iniciar una investigación y proteger al menor y a otros posibles objetivos.

Prevención y Protección

Configuración de medidas de seguridad en dispositivos y plataformas en línea:
Los padres y educadores deben familiarizarse con las configuraciones de privacidad y seguridad de las plataformas que los menores utilizan, asegurándose de que sus cuentas estén adecuadamente protegidas.

Promoción de la comunicación abierta:
Es fundamental crear un entorno en el que los niños y adolescentes se sientan cómodos compartiendo sus experiencias en línea, sin temor a represalias o malentendidos.

El grooming, como se mencionó anteriormente, a menudo tiene como objetivo final obtener material sexualmente explícito del menor, que puede variar desde fotos y videos en situaciones comprometedoras hasta material claramente pornográfico. Una vez que el groomer tiene en su poder ese material, puede usarlo para varios propósitos, incluyendo su propio disfrute, para compartirlo en comunidades clandestinas en línea o para chantajear al menor y obtener aún más material o favores sexuales.
La producción, distribución, posesión y consumo de pornografía infantil están prohibidos y son delitos graves en la gran mayoría de países del mundo. Las penas para estos delitos son generalmente severas, dada la naturaleza atroz del crimen y el daño irreversible que causa a las víctimas.

CYBERBULLYING

¿Qué es el ciberbullying?

El ciberacoso, también conocido como acoso cibernético o cyberbullying, se refiere a actos repetidos de acoso llevados a cabo a través de medios electrónicos, principalmente a través de Internet. Estos actos pueden incluir, pero no se limitan a, mensajes amenazantes, difusión de rumores, publicación de información privada o difamatoria, y creación de perfiles o sitios web falsos con el propósito de humillar a una persona. El ciberacoso puede ocurrir en diversas plataformas, como redes sociales, correos electrónicos, mensajes de texto y sitios web.

El ciberacoso puede tener consecuencias graves para las víctimas, que pueden experimentar ansiedad, depresión, aislamiento social, problemas de autoestima y, en casos extremos, pueden llevar a pensamientos suicidas.

Redes sociales como Facebook, TikTok o Instagram, son las más populares entre los niños y adolescentes en donde prevalece el ciberacoso de varias maneras, como:

- **Mensajes de texto o imágenes amenazantes o humillantes**
- **Difusión de rumores o información falsa**
- **Intimidación o amenazas**
- **Exclusión social**
- **Comentarios humillantes o degradantes.**

Eventualmente,los patios de recreo, los pasillos de las escuelas y las esquinas de las calles alguna vez fueron los principales escenarios de confrontaciones entre niños, hoy en día, las redes sociales han ampliado este escenario al mundo virtual, donde las palabras y las imágenes tienen el poder de perpetuarse y multiplicarse con una rapidez sin precedentes.

En este espacio digital, los jóvenes no sólo interactúan con sus amigos cercanos, sino también con una audiencia global, amplificando así el potencial de daño. Las barreras tradicionales de la empatía se difuminan, permitiendo que las burlas, los insultos y las humillaciones se propaguen con facilidad.

Es vital que comprendamos el impacto del cyberbullying en redes sociales en niños y adolescentes, no sólo porque afecta su bienestar presente, sino porque puede tener repercusiones duraderas en su salud mental, autoestima y desarrollo personal.

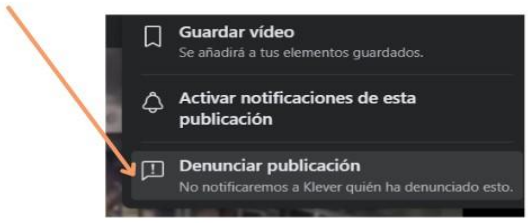
Manifestaciones del Cyberbullying

El cyberbullying en redes sociales adopta diversas formas, muchas de las cuales son únicas para el entorno digital. Los comportamientos de acoso pueden ser directos o indirectos, y, a menudo, son magnificados por la naturaleza viral de las redes sociales.
Los comportamientos del cyberbullying se ven reflejados en comentarios deliberamente ofensivos o provocativos. Revelación personal sobre alguien sin su consentimiento; discusiones en línea que se vuelven hostiles.
Los adolescentes especialmente utilizan las redes sociales para erparcir rumores o mentiras sobre alguién para dañar su reputación o también para compartir o amenazar con compartir contenido comprometedor sin el consentimiento de la persona involucruda

¿Cómo actuar cuando se detecta un caso de cyberbullying?

Detectar un caso de cyberbullying es solo el primer paso; es crucial saber cómo actuar de manera rápida y efectiva para proteger a la víctima y evitar mayores daños
Para ello, es necesario:

- Brindar apoyo a la víctima
- Documentar el acoso, es decir realizar capturas de pantalla, con la finalidad de guardar pruebas de cyberbullying, mensajes, videos, llamadas.
- Reportar en la plataforma, Facebook por ejemplo permite denunciar comentarios, publicaciones, etc



- Bloquear al ciberatacante
- Informar a las autoridades de la escuela si en caso el cyberbullying involucra a estudiantes de la misma institución.
- Informar a la policía dependiendo de la gravedad y naturaleza del acoso, especialmente cuando se trata de amenazas directas.

.

Herramientas de seguridad y privacidad

Software de monitoreo: Estas herramientas permiten a los padres supervisar la actividad en línea de sus hijos, detectando posibles signos de acoso.
Los padres pueden controlar el uso de Internet de sus hijos configurando herramientas de control parental o activando el modo niños en los dispositivos. Esto ayuda a proteger a los niños de contenido dañino y a promover un uso responsable de Internet. Además, las herramientas de control parental pueden ayudar a los padres a establecer límites de tiempo de pantalla y a rastrear la ubicación de sus hijos en línea.

Configuraciones de privacidad: Las redes sociales y otras plataformas ofrecen configuraciones de privacidad para proteger la información personal y limitar quién puede interactuar con el usuario.
Al configurar su privacidad de forma adecuada, puede controlar quién puede ver su información y contenido en línea.
Esto puede ayudar a protegerlo de ser acosado por personas que no lo conocen o que no conoce bien.
Es importante mantener el perfil en privado, es decir, que solo los amigos podrán ver su información personal.
Controlar quién puede ver las publicaciones, fotos y videos.

La importancia de la intervención temprana y el apoyo psicológico.

La prevención del cyberbullying en redes sociales es una tarea multidimensional que involucra a individuos, familias, escuelas y comunidades. Una respuesta efectiva requiere una combinación de educación, conciencia y el uso de herramientas y recursos adecuados.
El cyberbullying puede dañar la autoimagen y la confianza de la víctima. El apoyo psicológico puede ayudar a reconstruir estos aspectos esenciales del bienestar.

CIBERADICCIÓN

¿Qué es la ciberadicción?

La ciberadicción se refiere a la dependencia compulsiva y excesiva de internet o de dispositivos electrónicos, hasta el punto en que esta dependencia interfiere con la vida diaria, las relaciones personales, la educación y la salud. Es una forma de comportamiento adictivo, similar a otras adicciones no relacionadas con sustancias.

Síntomas y Señales de Alerta

Cambios en patrones de sueño: Las personas afectadas a menudo sacrifican horas de sueño para pasar más tiempo en línea, lo que puede llevar a trastornos del sueño.

Negligencia de responsabilidades diarias: Tareas escolares, laborales o domésticas pueden ser descuidadas o ignoradas en favor del tiempo pasado en línea.

Pérdida de interés en otras actividades: Actividades que antes se disfrutaban, como deportes o hobbies, pueden ser dejadas de lado.

Irritabilidad cuando no se puede acceder a la tecnología: La persona puede mostrar signos de agitación, frustración o incluso enfado cuando se le niega el acceso a sus dispositivos o a internet.

Tipos de Ciberadicciones

Adicción a juegos en línea: Esta adicción se manifiesta cuando los niños pasan la mayoría de su tiempo libre jugando videojuegos en línea.

Adicción a redes sociales: Aquí, el adolescente siente la necesidad constante de revisar y actualizar sus perfiles en redes sociales, interactuar con otros, o simplemente pasar horas navegando por estas plataformas.

Causas y Factores de Riesgo

- **Factores psicológicos y emocionales:** La búsqueda de aprobación en línea, el deseo de escapar de problemas personales o la necesidad de una gratificación instantánea pueden llevar a un uso excesivo de la tecnología. Además, personas con ciertas predisposiciones o trastornos, como la ansiedad, la depresión o trastornos de la personalidad, pueden ser más susceptibles.
- **Ambiente y entorno social:** La presión de grupo o la sensación de pertenecer a una comunidad en línea puede intensificar la necesidad de estar conectado. En algunos casos, el entorno familiar puede no ofrecer un espacio de comunicación abierto, empujando a los jóvenes a buscar refugio en el mundo virtual.
- **Fácil acceso y disponibilidad de dispositivos:** Vivimos en una era donde el acceso a dispositivos conectados es constante. Tablets, smartphones y computadoras están al alcance de la mano la mayoría del tiempo, lo que puede facilitar el desarrollo de comportamientos adictivos.

Recompensas intermitentes: Las plataformas en línea a menudo se diseñan para ofrecer gratificaciones intermitentes, como "likes", comentarios o recompensas en juegos. Estas pequeñas dosis de gratificación pueden incentivar a los usuarios a volver una y otra vez.

Prevención y Buenas Prácticas

- **Establecer límites de tiempo:** Es vital definir y adherirse a un tiempo específico para el uso de dispositivos. Por ejemplo, establecer reglas como no usar dispositivos durante las comidas o antes de dormir puede ayudar a mantener un equilibrio.
- **Descansos regulares:** Animar a niños y adolescentes a tomar descansos frecuentes cuando estén en línea. Estos descansos pueden incluir actividades físicas, estiramientos o simplemente desconectar la vista de las pantallas.
- **Participación en actividades fuera de línea:** Fomentar hobbies y actividades que no involucren el uso de tecnología, como leer, practicar deportes, arte o música.

SEXTING

¿Qué es el sexting?

El sexting es el envío de mensajes, fotos o vídeos de contenido sexual a través de dispositivos tecnológicos, como teléfonos móviles, aplicaciones de mensajería instantánea, redes sociales, correo electrónico u otra herramienta de comunicación.

El sexting puede ser una forma segura y divertida de explorar la sexualidad, siempre y cuando se haga de forma responsable. Sin embargo, también puede tener consecuencias negativas, como el acoso, el chantaje o la difusión de imágenes íntimas sin consentimiento.

También es importante recordar que el sexting no es un juego. Es una actividad que puede tener consecuencias negativas, como la difusión de las imágenes sin el consentimiento de la persona que las envió, el acoso o chantaje, y problemas legales.

Consecuencias Negativas

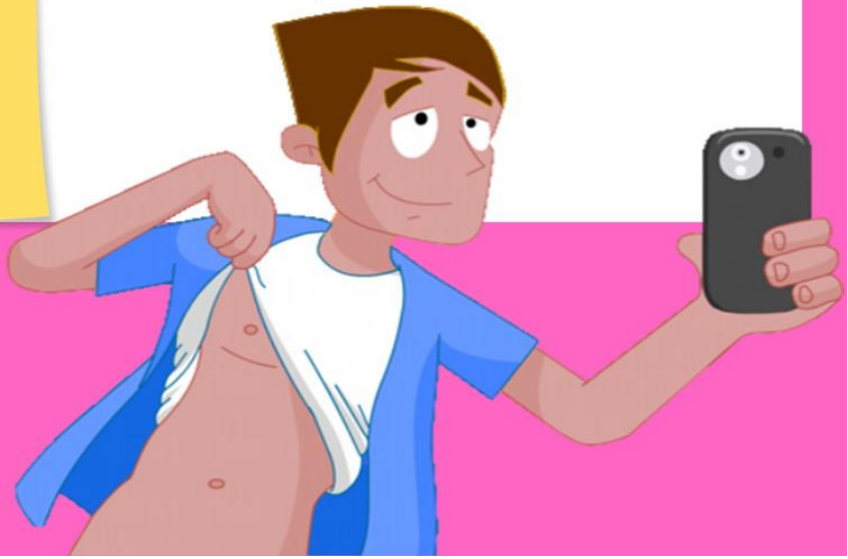
- Circulación de las imágenes sin el consentimiento de la persona que las envió.
- Acoso o chantaje.
- Problemas legales.

Consideraciones en torno al sexting

1. **Consentimiento:** Ambas partes involucradas deben estar de acuerdo y entender las implicaciones de compartir ese tipo de contenido.
2. **Legalidad:** En muchos lugares, compartir imágenes o videos íntimos de menores de edad, incluso si uno mismo es menor y se comparte su propio contenido, es ilegal y puede ser considerado como distribución de pornografía.

Riesgos asociados al sexting

- Difusión accidental : Es posible enviar por error una imagen o mensaje íntimo a la persona equivocada oa un grupo.
- Reenvío sin consentimiento : Una vez que se envía una imagen o mensaje, el remitente pierde el control sobre dónde puede terminar. La persona receptora podría reenviarlo a otras personas, ya sea por malicia, presión de terceros o incluso accidentalmente.
- Dispositivos perdidos o robados : Los smartphones o computadoras que contienen imágenes o mensajes íntimos pueden caer en manos equivocadas.



Consejos para evitar el sexting

- **Piensa antes de actuar.** Antes de enviar un mensaje o foto de contenido sexual, piensa en las posibles consecuencias. ¿Qué pasaría si la imagen o el mensaje se difundiera sin tu consentimiento?
- **No envíes mensajes o fotos de contenido sexual a personas que no conoces bien**. Si no estás seguro de la persona con la que estás hablando, no envíes ningún contenido sexual.
- **No te dejes presionar por nadie para que envíes contenido sexual**. Si alguien te presiona para que envíes contenido sexual, no lo hagas.
- **Si recibes un mensaje o foto de contenido sexual de alguien que no conoces, no lo reenvíes**. Borra el mensaje o la foto y bloquea al remitente.
- **Si te sientes avergonzado o culpable por enviar contenido sexual, habla con un adulto de confianza**. Un adulto puede ayudarte a entender los riesgos del sexting y a tomar medidas para protegerte

¿QUÉ HACER EN CASO DE QUE DIVULGEN MIS FOTOS?

1. **Reunir pruebas**
2. **Bloquear al remitente**
3. **Reporta a las autoridades**

RECUERDA QUE ECUADOR CUENTA CON LEYES PARA SANCIONAR ESTE DELITO.

Art. 103, 104, 173,178

MARCO LEGAL

Código Orgánico Integral Penal

El marco legal del Ecuador para el **robo de información** se encuentra en el Código Orgánico Integral Penal (COIP), en los artículos 298 al 304. Las penas por el robo de información varían dependiendo de la gravedad del delito. El robo de información simple se castiga con prisión de uno a tres años. El robo de información agravado se castiga con prisión de tres a cinco años.

La **interceptación ilegal de datos** es un delito que consiste en la obtención de información personal o confidencial, sin el consentimiento del titular de los datos. Este delito puede cometerse de diversas formas, como mediante el acceso no autorizado a un sistema informático, la instalación de software espía o la interceptación de comunicaciones.El marco legal del Ecuador para la intercepción ilegal de datos se contempla en los artículos del 230 al 234

El marco legal del Ecuador para el **malware** se encuentra en el Código Orgánico Integral Penal (COIP), en los artículos 305 al 309. La creación de malware se castiga con prisión de uno a tres años. La distribución de malware se castiga con prisión de tres a cinco años.

La **violación a la intimidad** es también considerada como un delito en Ecuador, en el que el artículo 178 establece sanciones con pena privativa.

La pornografía infantil que se encuentra dentró del **grooming**, es un delito grave que puede acarrear severas consecuencias legales, por ello el artículo 103, 104, 173,174, estipulan sanciones severas para quienes realicen este tipo de actos.

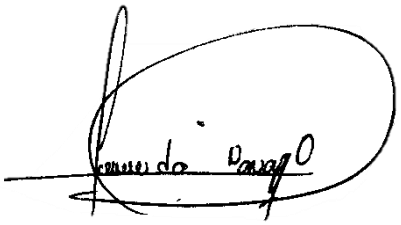
En Ecuador, la **suplantación de identidad** puede ser sancionada con una pena de prisión de seis meses a tres años. La pena puede ser mayor si el delito se comete con fines de lucro o para causar daño a la víctima. Este delito está contemplado en el artículo 212 del COIP.

DISFRUTA DE LA INTERNET CON SEGURIDAD

Universidad Católica de Cuenca	**AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL**

Fernanda Michaelle Narváez Ochoa portador(a) de la cédula de ciudadanía Nº **0302358601** En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"GUÍA DE PREVENCIÓN DE RIESGOS DE CIBERSEGURIDAD DERIVADO DEL USO DEL INTERNET Y LAS REDES SOCIALES EN NIÑOS Y ADOLESCENTES DEL CANTÓN CAÑAR"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca**,** para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, **11 de octubre de 2023**

F: 

……..

Fernanda Michaelle Narváez Ochoa

C.I. **0302358601**