Desarrollo de una Guía de Ciberseguridad para la Protección de Estudiantes Adolescentes en la Institución Educativa San Luis

Elaborado por:

Julieth Andrea Gutiérrez Pineda

Garibaldy Ríos Hernández

Milton Andrés Tovar Bonilla

Leonardo Barreto Florez

Universidad EAN

Especialización Gerencia en Ciberseguridad

Seminario de Investigación de Pregrado

Bogotá

30/11/2024

Tabla de contenido

Lista de figuras

Lista de tablas

Resumen

El mundo digital, que antes representaba un espacio abierto y lleno de fascinantes descubrimientos, se ha transformado en un campo plagado de peligrosos riesgos cibernéticos. En la Institución Educativa San Luis, nuestros alumnos navegan a diario por este territorio incierto e imprevisible, exponiéndose a amenazas que podrían poner en jaque su privacidad, su seguridad personal y su salud emocional. Ha llegado la hora de adoptar medidas proactivas y preventivas para proteger a nuestra comunidad educativa y garantizar un entorno digital seguro y saludable para todos los estudiantes.

Problema de Investigación

En la actualidad, la integración de la tecnología en las instituciones educativas ha cambiado el proceso de enseñanza y aprendizaje, generando facilidad en el acceso a la información y herramientas en línea, sin embargo, este avance tecnológico también ha generado desafíos significativos en términos de seguridad digital.

Las instituciones educativas, al adoptar estas tecnologías, se han enfrentado a un aumento en los riesgos cibernéticos que afectan tanto a estudiantes como al personal educativo. La falta de preparación adecuada para enfrentar estos riesgos y la insuficiente educación en ciberseguridad en las instituciones genera una brecha en la protección de datos y la seguridad en el entorno educativo.

Este planteamiento del problema aborda de manera integral las deficiencias actuales en la educación sobre ciberseguridad y se desglosa en tres elementos clave: antecedentes, descripción del problema y pregunta de investigación, los cuales se abordarán en detalle a continuación.

Causas u orígenes del problema

En Colombia, las causas principales de la vulnerabilidad de los adolescentes frente a los delitos informáticos incluyen:

- **Brecha en la alfabetización digital**: Poca formación en el uso seguro de tecnologías por parte de instituciones educativas y familias.
- **Acceso masivo a dispositivos y redes**: Más del 70% de los hogares colombianos tienen acceso a Internet (DANE), pero sin controles adecuados.
- **Legislación insuficiente o mal implementada**: Aunque existen leyes como la 1273 de 2009, su aplicación no siempre llega a los entornos escolares.
- **Entorno cultural**: Predominancia del uso recreativo sobre el educativo en plataformas digitales.

Síntomas o situaciones anómalas

- Incremento en denuncias por grooming y pornografía infantil, con un 45% de víctimas en el grupo de 11 a 17 años en 2024.
- Alta incidencia de delitos como el phishing y el acceso abusivo a sistemas informáticos en ambientes educativos.
- Dificultades en la identificación temprana de riesgos por falta de protocolos en las instituciones.

Pronóstico

Sin intervención, es probable un aumento en el número de víctimas y la sofisticación de los ataques debido a la rápida evolución tecnológica y la falta de cultura de ciberseguridad en las comunidades escolares.

Control pronóstico

- **Implementación de la guía de ciberseguridad**: Proveer a las instituciones de herramientas prácticas y educativas.
- **Evaluación continua**: Medir la efectividad a través de encuestas y estadísticas.
- **Fortalecimiento legal y operativo**: Promover campañas nacionales que involucren a autoridades, instituciones y familias.

Pregunta de investigación

¿Cómo puede la implementación de una guía de ciberseguridad reducir los riesgos cibernéticos y mejorar la cultura digital entre estudiantes adolescentes en la Institución Educativa San Luis?

Objetivos

Fortalecer la cultura de seguridad digital en la Institución Educativa San Luis mediante la elaboración de una Guía de ciberseguridad que le de herramientas a los estudiantes adolescentes para navegar de manera más segura y consciente el mundo digital.

Objetivos específicos

- Diagnosticar los niveles de conocimiento y las principales amenazas cibernéticas a las que se enfrentan los estudiantes, para realizar una evaluación exhaustiva del nivel de conciencia sobre ciberseguridad en la comunidad estudiantil e identificar las principales vulnerabilidades.
- Diseñar una guía flexible y dinámica que aborde los desafíos cibernéticos actuales, que permita a los estudiantes abordar y desarrollar habilidades básicas en ciberseguridad con contenidos teóricos y prácticos, adaptados a los estudiantes de 12 a 15 años.

- Promover el aprendizaje activo y el pensamiento crítico, utilizando herramientas tecnológicas y estudios de casos reales para hacer que el aprendizaje sobre ciberseguridad.

Justificación

Desde que somos pequeños, la sociedad nos enseña a diferenciar entre lo que es bueno y lo que es malo, entre lo que es seguro y lo que es peligroso. Esas enseñanzas nos acompañan toda la vida, nos dice cómo protegernos ante situaciones de la vida cotidiana y del día a día: cruzar una calle de manera segura, no fiarse de extraños, mantenernos alejados de ciertos peligros, entre otros. Sin embargo, cuando hablamos del medio digital esta línea entre lo que es bueno y lo que es malo se vuelve difusa. La digitalización ha transformado radicalmente la forma en que vivimos, trabajamos y nos relacionamos. Pero también, ha abierto nuevas grietas a peligros desconocidos por la mayoría de las personas. En este escenario, Colombia vive un gran reto: la falta de conocimientos digitales y la creciente vulnerabilidad de los usuarios en el medio digital.

De acuerdo con We Are Social (2024), hay 39 millones de personas que acceden a Internet en Colombia, una situación que denota una alta conectividad en la sociedad. Sin embargo, este crecimiento también ha traído consigo un aumento en los delitos informáticos. De hecho, la “violación de datos personales” es el segundo delito más denunciado por los colombianos (Obando, J., 2024), reflejando lo poco segura que es la seguridad digital, así como el escaso conocimiento que existe acerca de las medidas para protegerse en la red.

Los delitos informáticos son un problema técnico y educativo. Aunque las personas usan Internet a menudo, pocos ciudadanos comprenden el verdadero impacto que tienen al actuar en el ciberespacio. La ignorancia que existe sobre la importancia de la privacidad, el tratamiento seguro de los datos personales y la seguridad en las plataformas digitales es una variable que no ayuda a la disminución de delitos en Colombia. La realidad referida pone de

manifiesto la necesidad urgente de una alfabetización digital que aúne la comprensión de los riesgos involucrados en la actividad online y su correcta prevención.

De acuerdo con las investigaciones encontramos los siguientes datos Estadísticos

1. **Incremento de Incidentes**: En 2022, el Instituto Nacional de Ciberseguridad de España (INCIBE) gestionó 7,980 incidentes de ciberseguridad relacionados con la Red Académica y de Investigación Española (RedIRIS)[1]. Este número representa un aumento significativo en comparación con años anteriores.
2. **Tipos de Ataques**: Los incidentes más comunes en el ámbito educativo incluyen el phishing, con casi 17,000 incidentes, seguido del malware con más de 14,000, y el ransomware con casi 450 incidentes[2].
3. **Frecuencia de Ataques**: Desde principios de 2024 hasta finales de julio, el sector educativo y de investigación en España ha recibido una media de 1,491 ataques por semana por institución[3]

Testimonios de Expertos

1. **Universidad de California, San Francisco (UCSF)**: En 2020, la UCSF sufrió un ataque de ransomware que encriptó datos importantes. Los atacantes exigieron un rescate de 1.14 millones de dólares, que la universidad se vio obligada a pagar para recuperar su información. Este incidente subraya la importancia de fortalecer las medidas de ciberseguridad en las instituciones educativas[4].

[1] https://www.incibe.es/incibe/sala-de-prensa/incibe-gestiono-mas-115000-incidentes-ciberseguridad-durante-2022-9-mas

[2] https://www.incibe.es/incibe/sala-de-prensa/incibe-gestiono-mas-115000-incidentes-ciberseguridad-durante-2022-9-mas

[3] https://www.incibe.es/incibe/sala-de-prensa/incibe-gestiono-mas-115000-incidentes-ciberseguridad-durante-2022-9-mas

[4] https://acerta.net/ciberseguridad/ciberseguridad-la-batalla-por-la-ciberseguridad-en-el-mundo-educativo-proteccion-y-aprendizaje/

2. **Medidas de Protección**: Según expertos de la Universidad Pontificada de Comillas, la implementación de un centro de ciberseguridad y la autenticación de dos factores han sido cruciales para proteger los sistemas internos de la universidad[5].

[5] https://www.vozpopuli.com/espana/sector-educativo-ciberataques.html

Marco teórico

Los delitos informáticos son una problemática creciente a nivel mundial, y Colombia no es la excepción. La rápida evolución de la tecnología y el acceso a Internet han transformado la forma en que los niños, niñas y adolescentes interactúan con el mundo. Sin embargo, este entorno digital también ha dado lugar a nuevas formas de vulnerabilidad, donde los menores pueden ser tanto víctimas como perpetradores de delitos informáticos.

Conceptualización de Delitos Informáticos

Los delitos informáticos, según la Ley 1273 de 2009 en Colombia, se definen como actividades ilegales que utilizan sistemas informáticos, redes o dispositivos electrónicos. Estos pueden incluir:

- Ciberacoso (Cyberbullying): Hostigamiento o acoso a través de plataformas digitales.
- Explotación sexual en línea: Consiste en la producción, distribución o posesión de material sexualmente explícito que involucra a menores.
- Grooming: Interacción en línea donde un adulto se gana la confianza de un menor para abusar de él.
- Fraude y suplantación de identidad: Actividades que buscan obtener beneficios económicos o personales a través de engaños en plataformas digitales.

Marco Legal en Colombia

Colombia ha desarrollado un marco legal para combatir los delitos informáticos, destacando la Ley 1273 de 2009, que tipifica varios delitos relacionados con la informática y establece penas para quienes cometan estas infracciones. Además, la Ley 1620 de 2013, que promueve la convivencia escolar y la prevención del acoso escolar, aborda aspectos de ciberacoso y su impacto en el bienestar de los estudiantes.

Vulnerabilidades de Niños, Niñas y Adolescentes

Los menores de edad son particularmente vulnerables en el entorno digital debido a:

- Inmadurez emocional: Pueden no tener la capacidad para entender las consecuencias de sus acciones en línea.
- Falta de conocimiento: Muchos menores carecen de educación sobre el uso seguro y responsable de Internet.
- Exposición a contenido inapropiado: La facilidad de acceso a contenido violento, sexual o dañino puede tener efectos adversos en su desarrollo.

Efectos Psicológicos y Sociales

Los delitos informáticos pueden tener consecuencias graves en la salud mental y emocional de los menores. El ciberacoso, por ejemplo, está relacionado con altos niveles de ansiedad, depresión y, en casos extremos, suicidio. Además, el miedo a la exposición y la estigmatización pueden llevar a los menores a aislarse socialmente.

Prevención y Educación

La educación es fundamental para prevenir delitos informáticos. Se requieren programas que enseñen a los menores sobre el uso seguro de Internet, la importancia de la privacidad y el respeto en las interacciones digitales. Iniciativas de concientización dirigidas a padres y educadores también son esenciales para crear un entorno seguro.

Contexto Sociocultural

Acceso y Uso de Tecnología

El acceso a Internet en Colombia ha aumentado significativamente en los últimos años, impulsado por la penetración de dispositivos móviles. Según datos del DANE (Departamento Administrativo Nacional de Estadística), más del 70% de los hogares colombianos cuentan con acceso a Internet, lo que permite a niños y adolescentes interactuar con el mundo digital desde una edad temprana. Sin embargo, este acceso también expone a los menores a riesgos significativos.

Cultura Digital

La cultura digital en Colombia está marcada por un uso intensivo de redes sociales y plataformas de mensajería. Estas herramientas son atractivas para los jóvenes, pero también crean un ambiente propenso al ciberacoso y la difusión de contenido inapropiado. La normalización de ciertos comportamientos en línea puede desensibilizar a los menores frente a la gravedad de sus acciones.

Tipologías de Delitos Informáticos

Ciberacoso El ciberacoso se presenta como uno de los delitos más comunes entre menores. Este fenómeno incluye la difusión de rumores, amenazas y humillaciones a través de mensajes, imágenes o videos. Los estudios muestran que una gran parte de los adolescentes ha sido testigo o ha sufrido ciberacoso, lo que resalta la necesidad de programas de intervención en las escuelas.

Grooming El grooming es una forma de abuso en la que un adulto establece una relación de confianza con un menor a través de la tecnología. Este proceso puede llevar a la explotación sexual, y aunque las leyes colombianas buscan sancionar estas conductas, la detección temprana y la educación sobre este riesgo son cruciales para su prevención.

Fraude Electrónico, Los adolescentes pueden ser víctimas de fraudes en línea, como la suplantación de identidad o el robo de datos personales. La falta de información sobre cómo proteger su información puede llevar a consecuencias financieras y emocionales.

Rol de las Instituciones Educativas

Las escuelas tienen un papel vital en la prevención de delitos informáticos. Es esencial implementar programas de alfabetización digital que enseñen a los estudiantes sobre la ética en línea, la seguridad y el manejo de situaciones de riesgo. La capacitación a docentes también es fundamental para detectar y manejar casos de ciberacoso.

Acción del Estado

El gobierno colombiano ha establecido iniciativas para combatir los delitos informáticos, como la creación de la Dirección de Ciberpolicía. Sin embargo, es necesario fortalecer estos esfuerzos a través de campañas de concientización y la colaboración entre diferentes entidades, incluyendo organizaciones no gubernamentales y la comunidad.

Responsabilidad de los Padres

Los padres juegan un papel crucial en la protección de sus hijos en el entorno digital. Fomentar una comunicación abierta sobre el uso de la tecnología y establecer límites claros puede ayudar a mitigar los riesgos.

Metodología

Este estudio resulta relevante, ya que examina una problemática en constante crecimiento y actualidad y que afecta a nuestros jóvenes. A través del uso de encuestas, relatos auténticos, información reciente y un análisis integral desde la perspectiva educativa, y técnica, se podrá expandir el panorama de la ciberseguridad y establecer referentes para desarrollar estrategias que aborden las deficiencias conductuales, formativas o de acceso, con el fin de enfrentar los riesgos a los que se exponen nuestros jóvenes todos los días en el ambiente digital.

Entre tanto, este estudio pretende aportar habilidades y herramientas a los jóvenes de los primeros cursos de la educación básica (Bachillerato) para que les permitan prevenir y entender el alcance de la huella digital que como usuarios de la red generamos, así como su trascendencia a la percepción física para un mejor entendimiento y prevención en el manejo, gestión y divulgación de datos. Además de evitar que sean víctimas de Delitos informáticos a través de internet a través de una guía de Ciberseguridad.

Tipo de investigación

Se utilizaron los datos proporcionados para realizar un análisis descriptivo, incluyendo tablas de frecuencia, porcentajes y análisis de tendencias. Se complementó la información con búsquedas en internet para contextualizar y validar los hallazgos.

Para obtener información y estadísticas relacionadas con lo indicado se realizó la búsqueda de esta a través de datos abiertos y de estudios relacionadas con la problemática, además se pudo a través de encuestas información relevante para la investigación.

Tipo de estudio

El tipo de estudio para la presente investigación es descriptivo y exploratorio. Se busca proporcionar un análisis detallado de la problemática de los delitos informáticos y los riesgos asociados al uso de Internet, con el objetivo de identificar patrones, conductas y factores clave. Además, se emplearán enfoques cualitativos y cuantitativos, utilizando testimonios, datos estadísticos actualizados y análisis de fuentes relevantes para abordar la situación desde diversas perspectivas, como la social, legislativa y técnica. Este estudio tiene como finalidad explorar la situación actual, así como proporcionar una comprensión más profunda de las falencias en la ciberseguridad y las posibles soluciones para mitigar los riesgos en los usuarios de la red.

Población y muestra

La población muestra que se tomó para esta investigación fue un grupo de estudiantes del colegio San Luis, donde estudia uno de los hijos de uno de los integrantes del grupo de investigación, y que a través de él se pudo gestionar la realización de la misma con permisos de los padres por protección de los jóvenes, que son menores de edad, no se pidió nombre ni ningún tipo de identificación.

Recolección y análisis de datos

Los instrumentos para recabar información son principalmente las encuestas realizadas y la recolección de datos de fuentes abiertas, aplicable dentro alcance del estudio de caso. (Hernández, Fernández, & Baptista, 2010).

Tratamiento de los datos

Según las definiciones planteadas por Hernández et al. (2014), el análisis de datos cuantitativos se realiza una vez que se ha completado el proceso de recolección de los datos,

lo que implica que los investigadores deben reunir una cantidad suficiente de información numérica y estructurada antes de proceder con su análisis. Este tipo de análisis generalmente se enfoca en la cuantificación de variables y busca identificar patrones, tendencias y relaciones estadísticas entre los datos obtenidos. Para ello, se utilizan herramientas matemáticas y estadísticas que permiten organizar, clasificar y analizar los datos de manera objetiva y precisa.

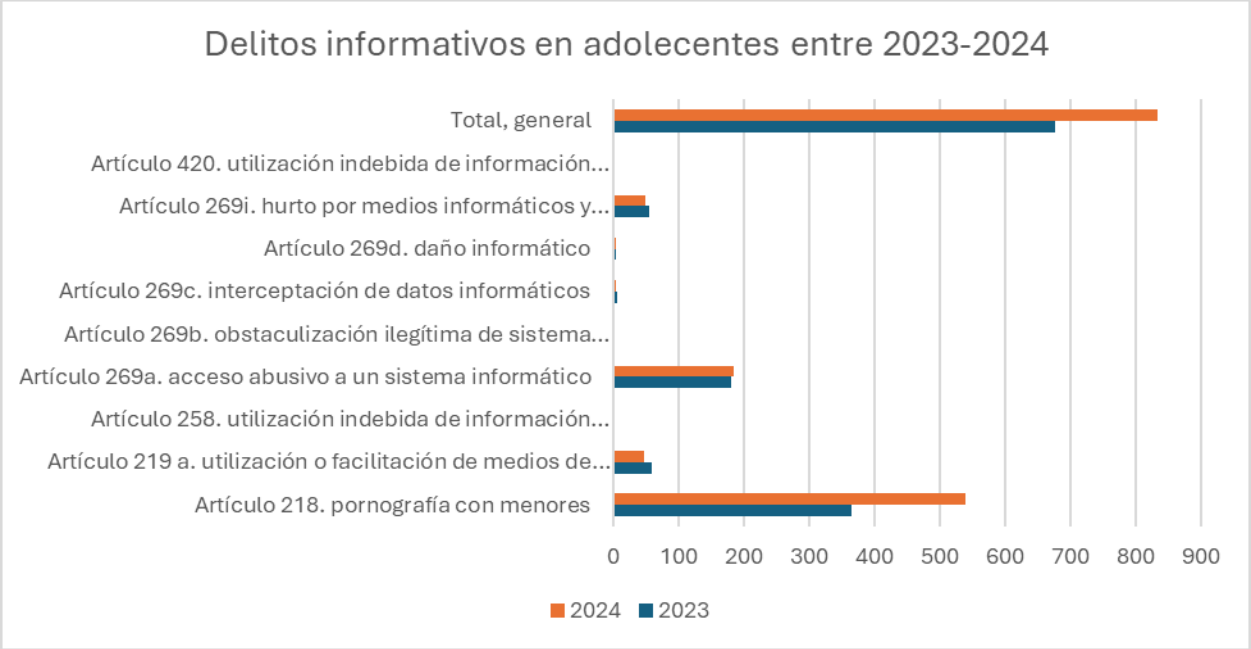
Análisis de datos

Los delitos informáticos representan uno de los retos más importantes en el ámbito de la seguridad digital en Colombia. Este análisis explora la creciente incidencia de estos delitos entre adolescentes, identificando patrones, factores contribuyentes y su impacto en la sociedad. Según datos recientes, los delitos cibernéticos en general han aumentado significativamente, con un foco particular en el comportamiento de menores de edad.

Delitos informáticos en adolescentes entre 2023 – 2024

También se logró obtener información de relacionada con víctimas de delitos informáticos con uso de tecnologías a niños, niñas y adolescentes entre el año 2023 y lo corrido del 2024, donde se extrajo la siguiente estadística:

Figura 1 – Delitos informáticos en adolescentes entre 2023 – 2024



Elaboración Propia

Tabla 1: Delitos informáticos en adolescentes entre 2023-2024

Delitos informáticos en adolescentes entre 2023-2024	2023	2024
Artículo 218. pornografía con menores	364	539
Artículo 219 a. utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores	59	48
Artículo 258. utilización indebida de información privilegiada	3	0
Artículo 269a. acceso abusivo a un sistema informático	180	184
Artículo 269b. obstaculización ilegítima de sistema informático o red de telecomunicación	3	3
Artículo 269c. interceptación de datos informáticos	7	4
Artículo 269d. daño informático	5	5
Artículo 269i. hurto por medios informáticos y semejantes	56	49
Artículo 420. utilización indebida de información oficial privilegiada	0	1
Total, general	**677**	**833**

Elaboración Propia

De acuerdo con lo anterior se puede realizar el siguiente análisis:

Tendencias Generales:

Aumento en la cantidad de delitos informáticos: Entre 2023 y 2024, se observa un aumento general de 156 casos, pasando de 677 a 833 delitos reportados. Este incremento puede reflejar una mayor conciencia y denuncia de estos delitos, así como una posible expansión de las actividades ilícitas relacionadas con el uso indebido de tecnologías.

Análisis de Delitos Específicos:

Pornografía con menores (Artículo 218): Este es, con mucho, el delito más común tanto en 2023 como en 2024. El número de casos aumenta de 364 en 2023 a 539 en 2024, lo que representa un 47.9% de incremento. Este aumento es alarmante y sugiere que, a pesar de los esfuerzos en la prevención, los menores siguen siendo víctimas vulnerables en el entorno digital.

Utilización o facilitación de medios para ofrecer servicios sexuales de menores (Artículo 219a): Aunque en 2023 se reportaron 59 casos, en 2024 esta cifra ha disminuido a 48. Esta reducción podría ser un indicio positivo de que las políticas de prevención, como las campañas de sensibilización y la intervención temprana, están teniendo algún impacto.

Acceso abusivo a sistemas informáticos (Artículo 269a): Este delito muestra un leve aumento de 180 casos en 2023 a 184 en 2024, lo que indica que, a pesar de los esfuerzos para mejorar la ciberseguridad, los adolescentes siguen siendo víctimas de estos ataques cibernéticos.

Hurto por medios informáticos (Artículo 269i): Este delito ha experimentado una pequeña disminución, de 56 casos en 2023 a 49 en 2024, lo que podría reflejar el impacto de mayores medidas de protección en plataformas de pago y servicios electrónicos.

Implicaciones y Recomendaciones:

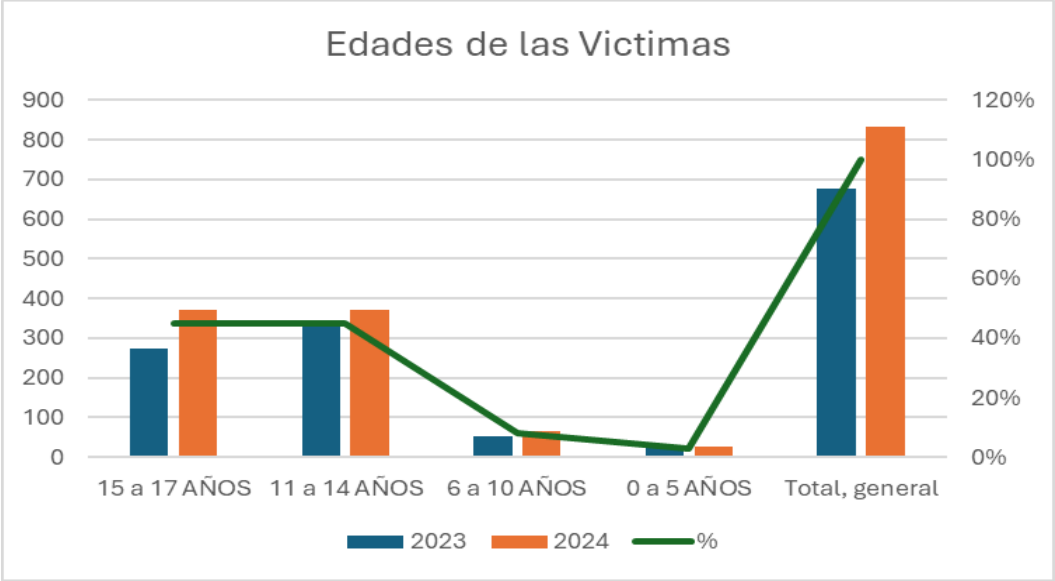
El aumento en delitos graves como la pornografía infantil subraya la necesidad urgente de mejorar las estrategias de monitoreo en línea y aumentar la colaboración internacional para rastrear estos delitos. Las plataformas digitales y redes sociales deben implementar mejores mecanismos de detección de contenido ilícito.

La disminución en algunos tipos de delitos, como la facilitación de servicios sexuales, podría estar relacionada con los esfuerzos preventivos, lo que sugiere que continuar con la educación y sensibilización, especialmente en jóvenes, es clave para seguir reduciendo estos casos.

La necesidad de fortalecer la ciberseguridad es evidente en el caso de delitos como el acceso abusivo a sistemas. Es necesario implementar programas de educación digital tanto para estudiantes como para padres, a fin de prevenir estos ataques.

Edades victimas

Figura 2 – Edades Victimas



Elaboración Propia

Tabla 2: Edades Victimas

Edad de las víctimas de delitos informáticos	2023	2024	%
15 a 17 AÑOS	275	371	45%
11 a 14 AÑOS	328	371	45%
6 a 10 AÑOS	52	64	8%
0 a 5 AÑOS	22	27	3%
Total, general	**677**	**833**	**100%**

Elaboración Propia

Incremento General en el Número de Víctimas:

En el período analizado, el número total de víctimas aumentó en 156 casos (de 677 en 2023 a 833 en 2024). Este incremento representa un 23% más de víctimas en 2024, sin contar los meses restantes del año.

Grupos de Edad Más Vulnerables:

Los adolescentes de 11 a 17 años constituyen el 90% del total de víctimas en 2024, dividiéndose equitativamente entre los rangos de 11-14 años y 15-17 años (45% cada uno).

Estos datos reflejan que los adolescentes en etapa escolar son el grupo más propenso a ser objetivo de delitos informáticos, probablemente debido a su alta interacción con tecnologías digitales y redes sociales.

Menor Riesgo en Grupos Más Jóvenes:

Los niños de 0 a 10 años representan solo el 11% del total de víctimas en 2024, lo cual es significativamente menor que en los adolescentes. Esto podría explicarse por una menor exposición a dispositivos conectados y la supervisión parental.

Tasa de Crecimiento en Grupos Específicos:

El aumento porcentual más significativo se observa en los niños de 6 a 10 años, con un incremento del 23% (de 52 casos en 2023 a 64 en 2024).

El grupo de 0 a 5 años también presenta un crecimiento del 23%, aunque en valores absolutos sigue siendo el grupo con menos víctimas.

Análisis Cualitativo:

Factores Contributivos para los Adolescentes (11 a 17 años):

Alta exposición digital: Este rango de edad es el que más interactúa con redes sociales, videojuegos en línea y otras plataformas, lo que aumenta su vulnerabilidad a delitos como grooming, ciberacoso y exposición a contenidos inapropiados.

Falta de educación cibernética: Muchos adolescentes no poseen una adecuada formación en ciberseguridad, lo que los hace más propensos a caer en estafas y ser víctimas de delitos informáticos.

Uso sin supervisión: La libertad en el uso de dispositivos electrónicos sin control parental puede facilitar el acceso a contenido inapropiado y contactos con personas peligrosas.

Protección en Grupos Más Jóvenes (0 a 10 años):

En este rango, los menores suelen estar más protegidos debido a la supervisión parental y al acceso limitado a internet. Sin embargo, los incrementos reportados sugieren que los menores pueden estar siendo expuestos a riesgos mediante dispositivos compartidos o falta de controles parentales adecuados.

Impacto Psicológico y Social:

Las víctimas adolescentes pueden enfrentar problemas emocionales como ansiedad, depresión y baja autoestima debido a delitos como el ciberacoso o la exposición no consensuada de información privada.

Recomendaciones Basadas en los Datos:

Educación Digital:

Implementar programas educativos en colegios para enseñar a los adolescentes sobre el uso responsable de internet, cómo detectar riesgos y cómo reportar actividades sospechosas.

Fortalecimiento de Controles Parentales:

Promover herramientas de control parental para limitar el acceso a contenidos y plataformas inapropiadas para niños menores de 10 años.

Campañas de Sensibilización:

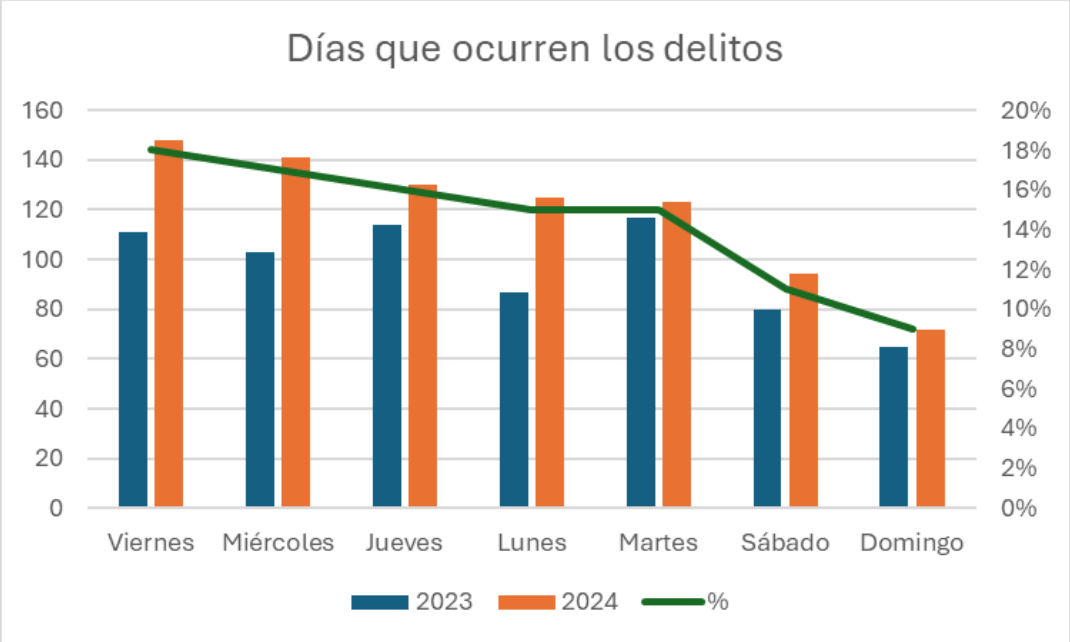
Realizar campañas nacionales para informar a padres, profesores y estudiantes sobre los peligros en línea, con un enfoque especial en la prevención del grooming y la pornografía infantil.

Colaboración entre Entidades:

Las autoridades educativas, tecnológicas y judiciales deben trabajar conjuntamente para identificar patrones de delitos informáticos y mejorar las herramientas de monitoreo.

Días que ocurren los delitos

Figura 3 – Días que ocurren los delitos



Elaboración Propia

Tabla 3: Días que ocurren los delitos

Días que se ejecutan los de delitos informáticos	2023	2024	%
Viernes	111	148	18%

Miércoles	103	141	17%
Jueves	114	130	16%
Lunes	87	125	15%
Martes	117	123	15%
Sábado	80	94	11%
Domingo	65	72	9%
Total, general	**677**	**833**	**100%**

Elaboración Propia

Tendencias generales:

Incremento en la actividad delictiva: Se observa un aumento general en la cantidad de delitos informáticos cometidos en 2024 en comparación con 2023. Esto se evidencia en el total general, que pasa de 677 a 833.

Días de mayor incidencia: Los días con mayor número de delitos informáticos tanto en 2023 como en 2024 son: viernes, miércoles y jueves.

Fin de semana con menor actividad: El sábado y el domingo presentan la menor cantidad de delitos informáticos, lo que podría indicar que los delincuentes aprovechan los días laborables cuando las personas están más activas en línea.

Análisis por día:

Viernes: Es el día con mayor número de delitos informáticos en ambos años, mostrando un aumento significativo de 111 a 148 casos.

Miércoles: También muestra un aumento considerable en 2024, pasando de 103 a 141 casos.

Jueves: Aunque sigue siendo uno de los días con mayor incidencia, el aumento en 2024 es menos pronunciado en comparación con el viernes y el miércoles.

Lunes a viernes: En general, los días laborables concentran la mayor parte de la actividad delictiva.

Sábado y domingo: Muestran un aumento en 2024, pero siguen siendo los días con menor incidencia.

Posibles explicaciones:

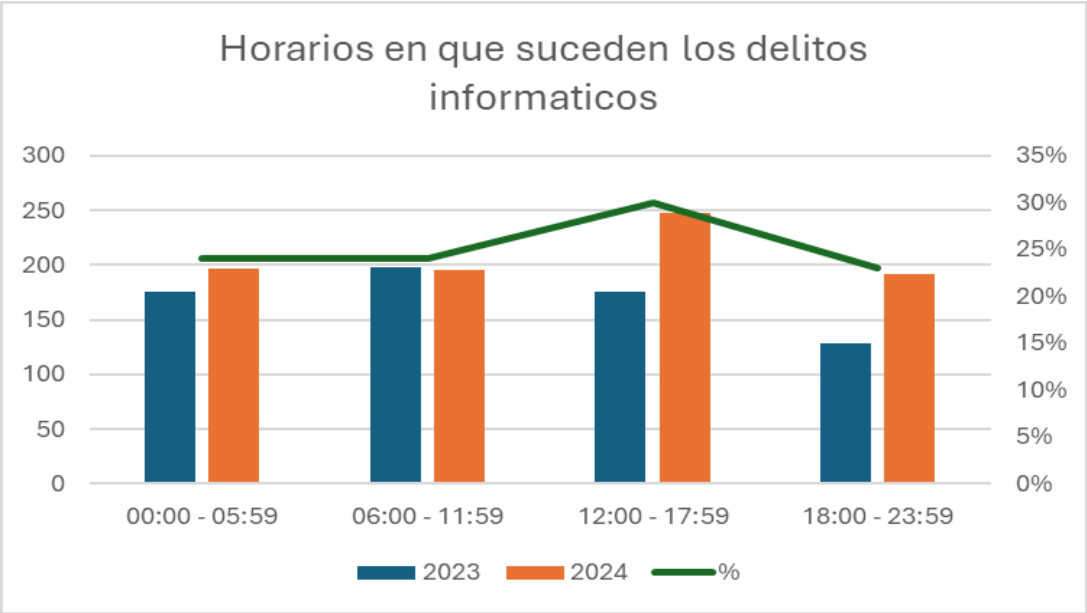
Actividad en línea: El aumento de delitos informáticos entre semana podría estar relacionado con la mayor actividad de las personas en línea durante las jornadas laborales, ya sea por motivos de trabajo, estudio o gestiones personales.

Vulnerabilidades en sistemas: Los delincuentes podrían aprovechar las horas de trabajo para atacar sistemas informáticos de empresas o instituciones que pueden estar más vulnerables durante ese periodo.

Patrones de comportamiento: El análisis de los días de la semana podría revelar patrones de comportamiento de los delincuentes informáticos, lo que podría ser útil para la prevención y la investigación de estos delitos.

Horarios en que suceden los delitos

Figura 4 – Horarios en que suceden los delitos



Elaboración Propia

Tabla 4: Horarios en que suceden los delitos

Horarios que se ejecutan los de delitos informáticos	2023	2024	%
00:00 - 05:59	175	197	24%
06:00 - 11:59	198	196	24%
12:00 - 17:59	176	248	30%
18:00 - 23:59	128	192	23%
Total general	**677**	**833**	**100%**

Elaboración Propia

Incremento de delitos: Al igual que en la tabla anterior, se observa un aumento general en la cantidad de delitos informáticos en 2024 respecto a 2023 (de 677 a 833).

Franja horaria de mayor incidencia: La franja horaria con mayor número de delitos en 2024 es la que va desde el mediodía hasta las 17:59, con un aumento considerable respecto a 2023.

Madrugada con actividad significativa: Aunque con menor incidencia que la franja diurna, la madrugada (00:00 - 05:59) registra un número importante de delitos, mostrando un aumento en 2024.

Análisis por franja horaria:

00:00 - 05:59: A pesar de ser un horario de menor actividad en general, se observa un aumento en 2024, lo que podría indicar que los delincuentes aprovechan la menor vigilancia durante la madrugada.

06:00 - 11:59: Esta franja mantiene una cantidad similar de delitos en ambos años, con una ligera disminución en 2024.

12:00 - 17:59: Es la franja con mayor incremento en 2024, pasando de 176 a 248 delitos. Esto podría estar relacionado con una mayor actividad en línea durante la tarde, tanto por motivos laborales como personales.

18:00 - 23:59: Muestra un aumento en 2024, aunque sigue siendo menor que la franja diurna de mayor incidencia.

Posibles explicaciones:

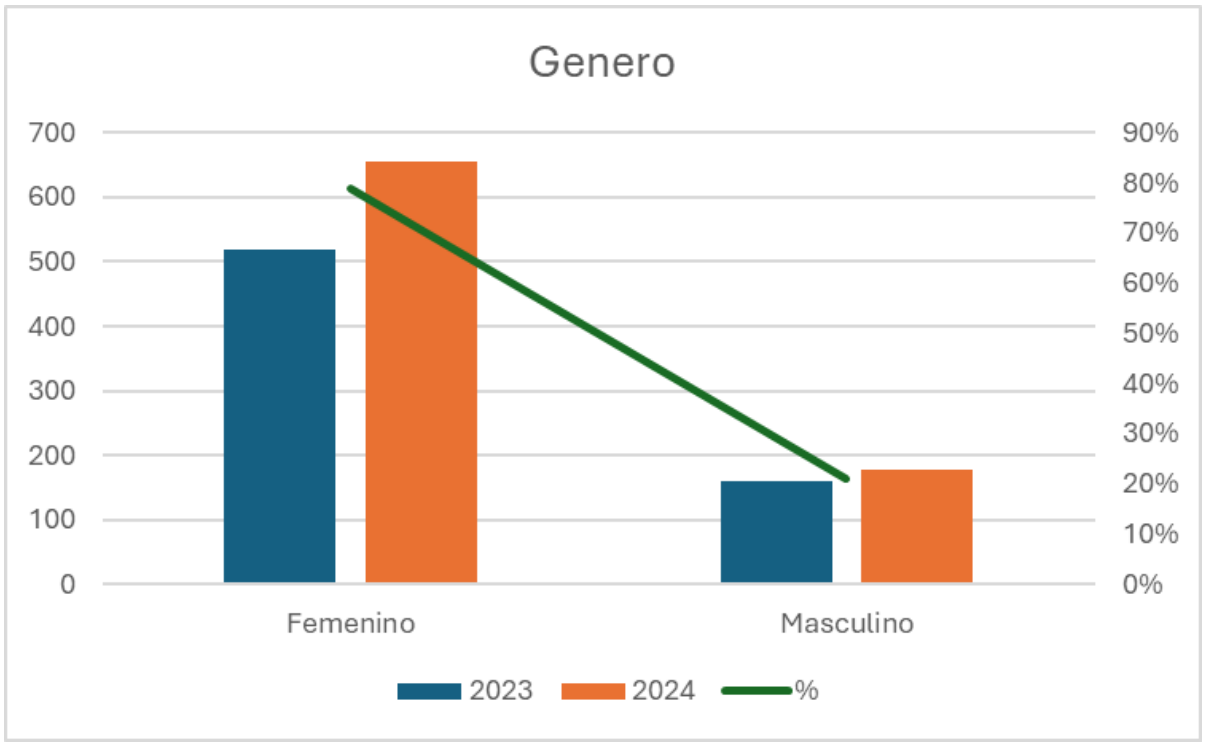
Patrones de actividad online: El aumento en la franja de 12:00 a 17:59 podría deberse a que muchas personas realizan actividades online durante la tarde, como compras, gestiones bancarias o uso de redes sociales, lo que podría ser aprovechado por los delincuentes.

Vulnerabilidad de sistemas: La madrugada podría ser un horario atractivo para los delincuentes debido a una menor supervisión de los sistemas de seguridad en empresas e instituciones.

Diferencias horarias: Es posible que los delincuentes operen desde diferentes zonas horarias, lo que podría influir en la distribución de los delitos a lo largo del día.

Genero de victimas

Figura 5 – Genero de victimas



Elaboración Propia

Tabla 5: Genero de victimas

Género afectado por los delitos informáticos	2023	2024	%
Femenino	518	655	79%
Masculino	159	178	21%
Total general	**677**	**833**	**100%**

Elaboración Propia

Esta tabla nos muestra la distribución de las víctimas de delitos informáticos por género en los años 2023 y 2024. Veamos un análisis:

Incremento de delitos: Se observa un aumento general en la cantidad de víctimas de delitos informáticos en 2024 en comparación con 2023, pasando de 677 a 833.

Género más afectado: En ambos años, el género femenino es el más afectado por los delitos informáticos, representando un porcentaje significativamente mayor que el masculino.

Análisis por género:

Femenino: El número de víctimas mujeres aumentó de 518 en 2023 a 655 en 2024, manteniendo un porcentaje cercano al 79%.

Masculino: También se observa un aumento en el número de víctimas hombres, pasando de 159 a 178, aunque el porcentaje se mantiene alrededor del 21%.

Posibles explicaciones:

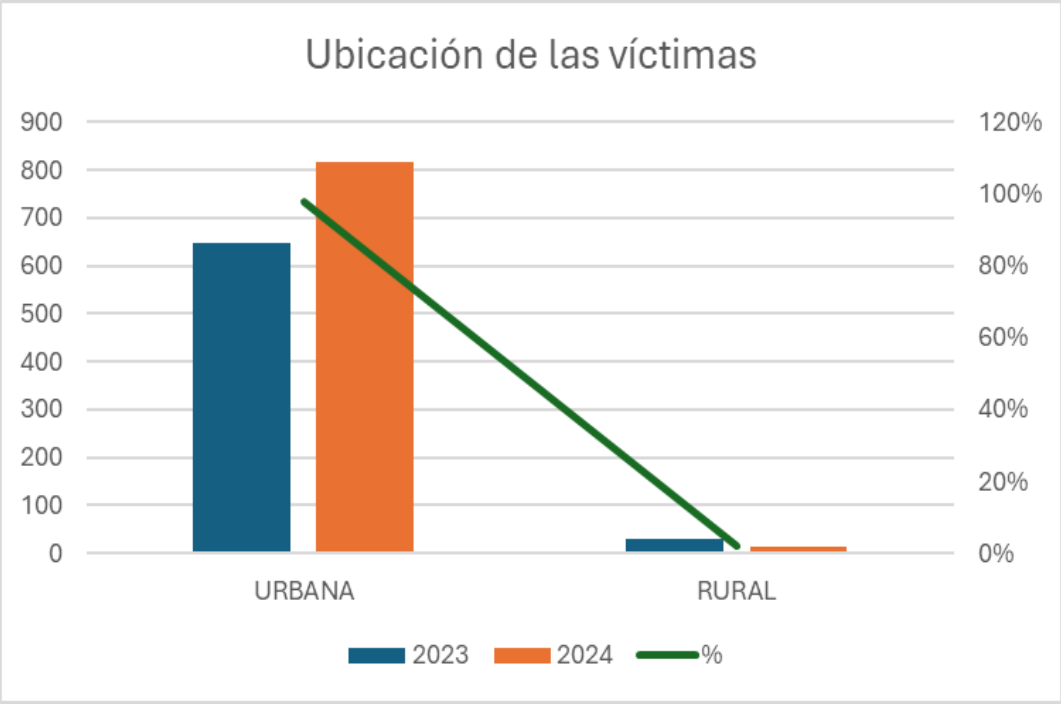
Mayor exposición online: Es posible que las mujeres estén más expuestas a ciertos tipos de delitos informáticos debido a una mayor participación en redes sociales, plataformas de compra online o actividades que requieren compartir información personal.

Ciberacoso y violencia de género: Las mujeres son más propensas a ser víctimas de ciberacoso, sextorsión y otros delitos relacionados con la violencia de género, lo que podría explicar la diferencia en las cifras.

Sesgos en la denuncia: Es posible que exista un sesgo en la denuncia de delitos informáticos, donde las mujeres se sientan más inclinadas a reportar estos incidentes que los hombres.

Ubicación de las victimas

Figura 6 – Ubicación de victimas



Elaboración Propia

Tabla 6: Ubicación de victimas

Ubicación de las víctimas de delitos informáticos	2023	2024	%
URBANA	648	818	98%
RURAL	29	15	2%
Total general	677	833	100%

Elaboración Propia

Esta tabla muestra la ubicación de las víctimas de delitos informáticos, diferenciando entre zonas urbanas y rurales, durante los años 2023 y 2024. Analicemos la información:

Incremento de delitos: Se observa, nuevamente, un aumento general en la cantidad de víctimas de delitos informáticos en 2024 en comparación con 2023 (de 677 a 833).

Mayor concentración en zonas urbanas: La gran mayoría de las víctimas de delitos informáticos se encuentran en zonas urbanas, tanto en 2023 como en 2024.

Disminución en zonas rurales: Sorprendentemente, se observa una disminución en el número de víctimas en zonas rurales en 2024.

Análisis por ubicación:

URBANA: El número de víctimas en zonas urbanas aumentó de 648 en 2023 a 818 en 2024, representando un 98% del total.

RURAL: En contraste, el número de víctimas en zonas rurales disminuyó de 29 en 2023 a 15 en 2024, representando solo un 2% del total.

Posibles explicaciones:

Acceso a internet y tecnología: Las zonas urbanas tienen mayor acceso a internet y tecnología, lo que aumenta la exposición a los delitos informáticos.

Concentración de la población: La mayor densidad de población en zonas urbanas facilita la propagación de malware y la realización de ataques informáticos.

Infraestructura crítica: Las zonas urbanas concentran infraestructuras críticas, como bancos, empresas y organismos gubernamentales, que pueden ser objetivo de ciberataques.

Mayor concienciación en zonas rurales: Es posible que la disminución de víctimas en zonas rurales se deba a una mayor concienciación sobre los riesgos en línea y la adopción de medidas de seguridad.

Migración a zonas urbanas: La migración de zonas rurales a urbanas podría influir en la distribución de las víctimas.

Conclusiones del análisis de datos

Las recomendaciones se centran en la necesidad de fortalecer la ciberseguridad y la prevención de delitos informáticos, con especial atención a las poblaciones más vulnerables como mujeres, adolescentes y residentes de zonas rurales.

Puntos clave:

Investigación: Se destaca la importancia de la investigación para comprender las causas de los delitos informáticos, especialmente la victimización de mujeres y la disminución de casos en zonas rurales. Esto permitirá desarrollar estrategias de prevención más efectivas.

Concienciación y educación: Se enfatiza la necesidad de concienciar a los usuarios sobre los riesgos en línea y las medidas de seguridad, con un enfoque particular en mujeres, adolescentes y residentes de zonas rurales.

Fortalecimiento de la seguridad: Se recomienda reforzar la seguridad informática en todo momento, con especial atención a las franjas horarias y los días de mayor incidencia. Esto incluye la adaptación de las medidas de seguridad a los patrones de actividad de los delincuentes.

Atención a grupos vulnerables: Se subraya la importancia de brindar atención especializada a las víctimas de delitos informáticos, considerando las necesidades específicas de cada género.

Prevención en adolescentes: Se hace hincapié en la necesidad de enfocar las políticas de prevención en los adolescentes, especialmente en aquellos de 11 a 17 años, mediante una combinación de educación, supervisión y regulación tecnológica.

Lucha contra la pornografía infantil: Se insta a las autoridades colombianas a reforzar las políticas de prevención, vigilancia y sanción en el ciberespacio para combatir la pornografía infantil, con un enfoque especial en los adolescentes y las plataformas que utilizan.

En resumen:

El resumen general de las recomendaciones destaca la necesidad de una estrategia integral para combatir los delitos informáticos, que combine la investigación, la concienciación, el fortalecimiento de la seguridad, la atención a grupos vulnerables y la cooperación entre autoridades, empresas y usuarios.

Análisis de datos de las encuestas estudiantes Colegio San Luis

A continuación, se muestra el análisis que se realizo a las encuestas realizadas a los estudiantes de grado sexto de bachillerato del Colegio San Luis:

Los datos contienen los resultados de una encuesta sobre ciberseguridad con 20 participantes. La encuesta incluye 10 preguntas sobre varios temas relacionados con la ciberseguridad, incluyendo:

Tabla 7: Preguntas encuesta

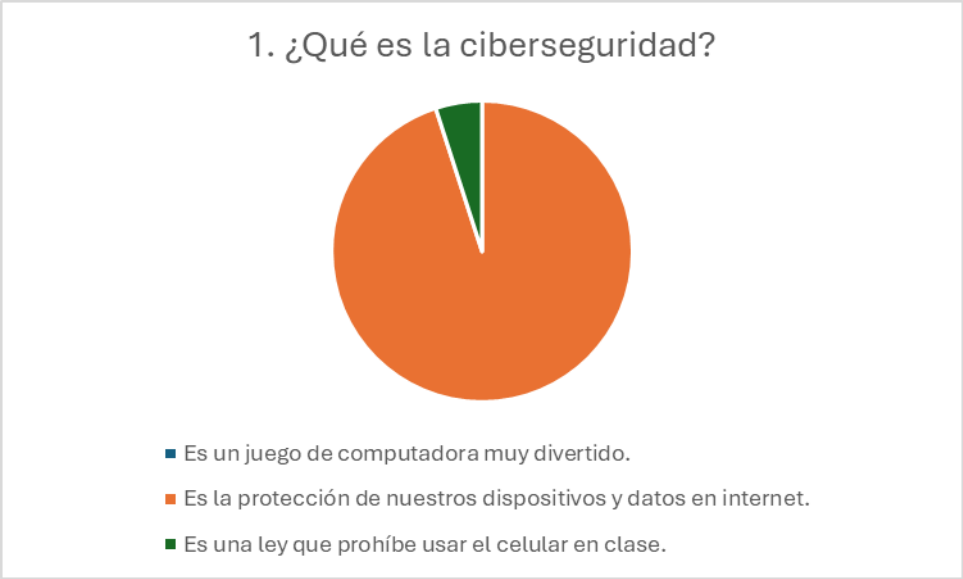
	Preguntas realizadas a los estudiantes
1	¿Qué es la ciberseguridad?
2	¿Cuál de estas acciones puede poner en riesgo tu seguridad en línea?
3	¿Qué información NO deberías compartir en las redes sociales?
4	¿Qué es el phishing?
5	¿Qué debes hacer si crees que alguien ha hackeado tu cuenta?
6	¿Conoces algún ejemplo de malware?
7	¿Cuál es la importancia de tener una contraseña segura?
8	¿Qué harías si recibes un mensaje de alguien que no conoces pidiéndote dinero?
9	¿Has aprendido sobre ciberseguridad en la escuela?
10	¿Te gustaría aprender más sobre cómo protegerte en internet?

Elaboración Propia

Respuestas:

1. Conocimiento general de ciberseguridad

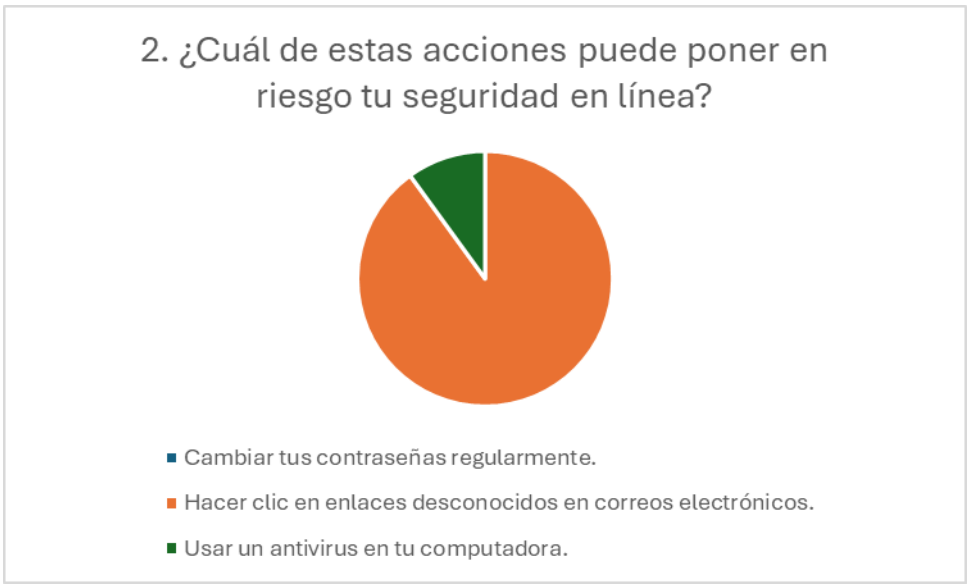
Figura 7 – ¿Qué es la ciberseguridad?



Elaboración Propia

2. Comportamientos de riesgo en línea

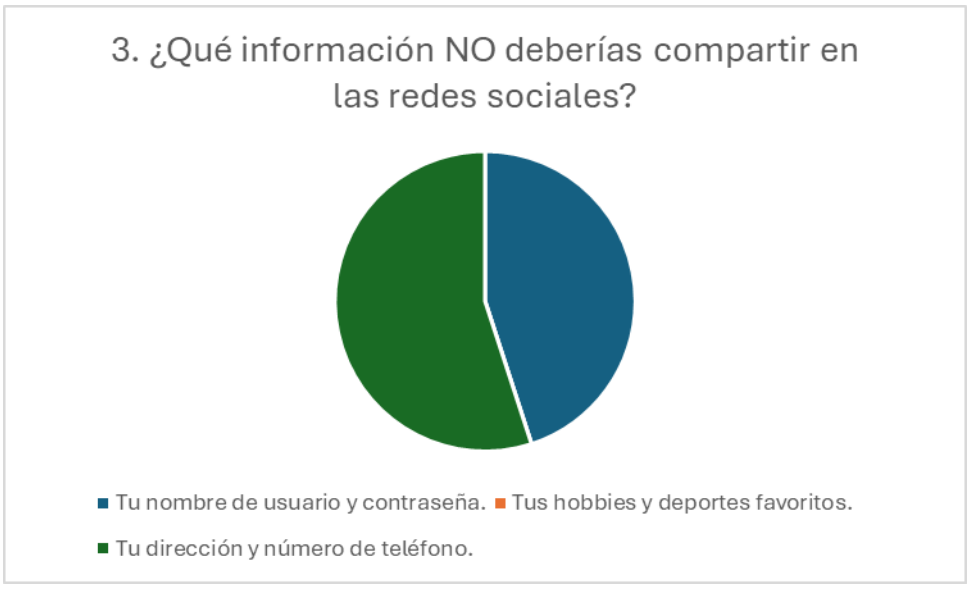
Figura 8 – ¿Cuál de estas acciones puede poner en riesgo tu seguridad en línea?



Elaboración Propia

3. Compartir información en redes sociales

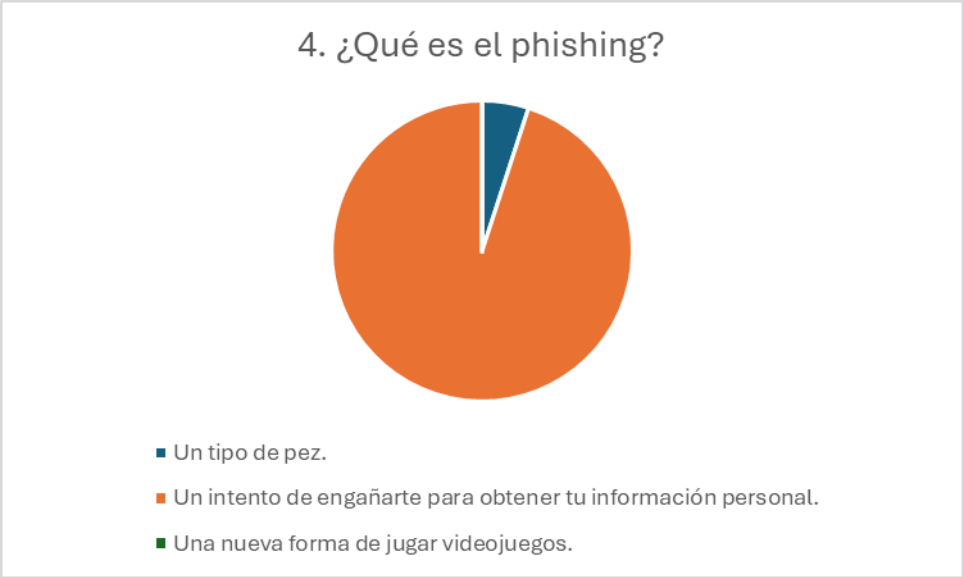
Figura 9 – ¿Qué información NO deberías compartir en las redes sociales?



Elaboración Propia

4. Phishing

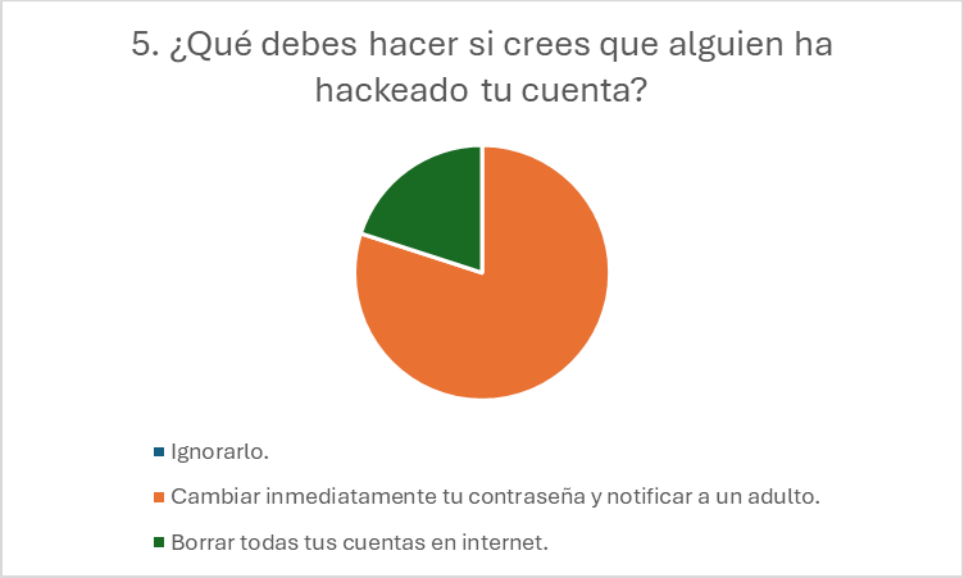
Figura 10 – ¿Qué es el phishing?



Elaboración Propia

5. Hackeo de cuentas

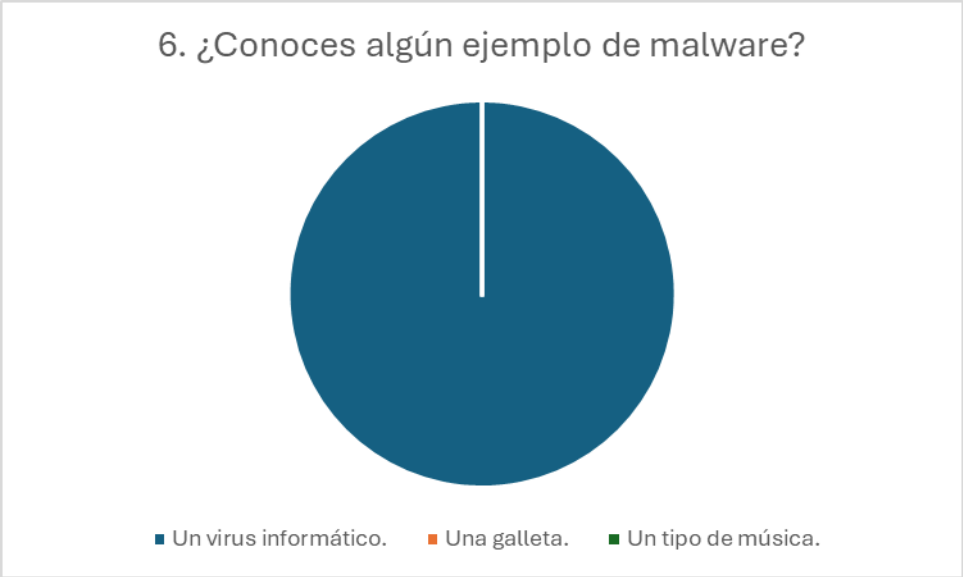
Figura 11 – ¿Qué debes hacer si crees que alguien ha hackeado tu cuenta?



Elaboración Propia

6. Malware

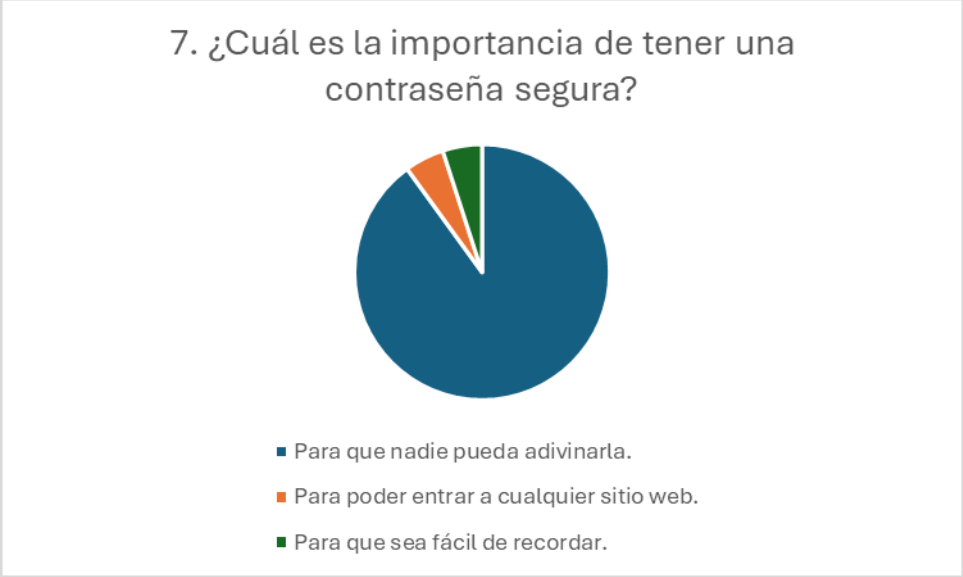
Figura 12 – ¿Conoces algún ejemplo de malware?



Elaboración Propia

7. Contraseñas seguras

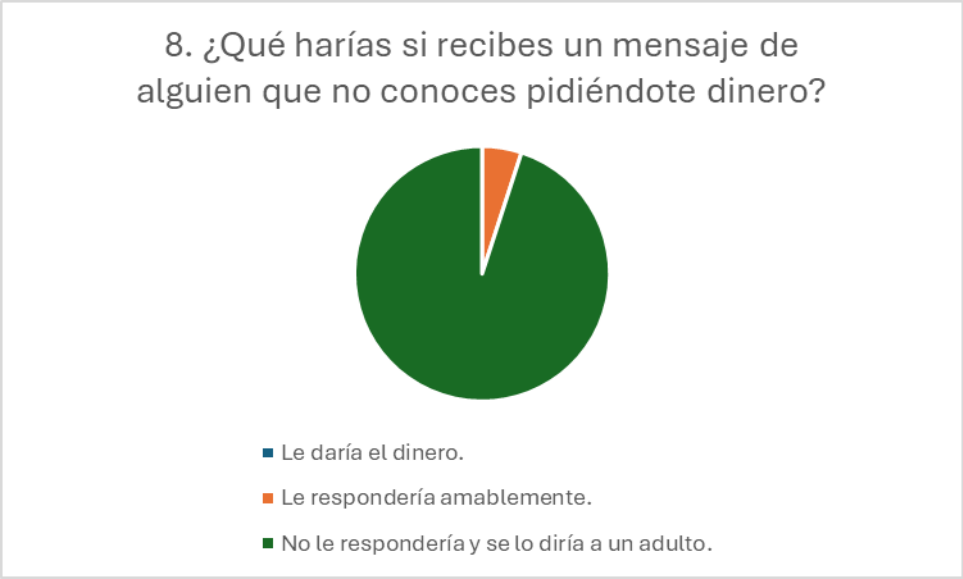
Figura 13 – ¿Cuál es la importancia de tener una contraseña segura?



Elaboración Propia

8. Estafas en línea

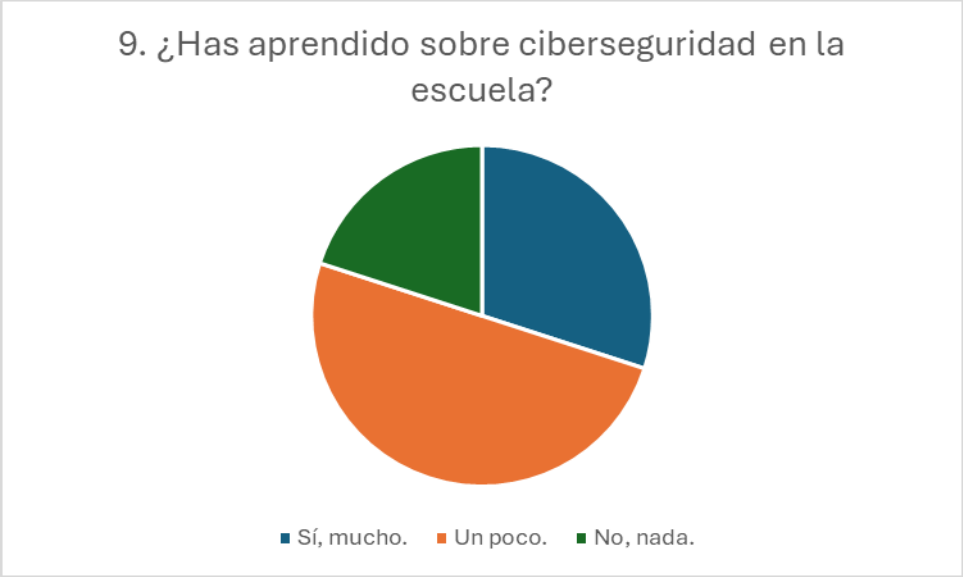
Figura 14 – ¿Qué harías si recibes un mensaje de alguien que no conoces pidiéndote dinero?



Elaboración Propia

9. Educación sobre ciberseguridad

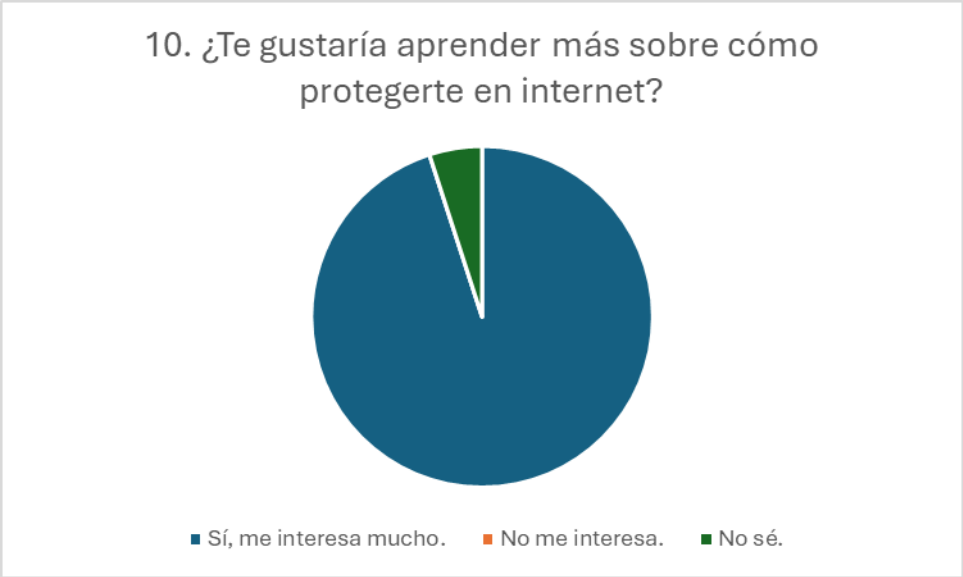
Figura 15 – ¿Has aprendido sobre ciberseguridad en la escuela?



Elaboración Propia

10. Interés en aprender más sobre ciberseguridad

Figura 16 – ¿Te gustaría aprender más sobre cómo protegerte en internet?



Elaboración Propia

Análisis de las respuestas

La mayoría de los participantes demostraron un buen conocimiento general de ciberseguridad, reconociéndola como la protección de dispositivos y datos en internet (95%).

El 90% de los participantes identificó correctamente hacer clic en enlaces desconocidos en correos electrónicos como un comportamiento de riesgo en línea.

Sin embargo, hubo una división en cuanto a la información que no se debe compartir en redes sociales, con un 55% que indicó la dirección y el número de teléfono, y un 45% que indicó el nombre de usuario y la contraseña.

La mayoría de los participantes (95%) entendió el concepto de phishing como un intento de engaño para obtener información personal.

El 80% de los participantes supo qué hacer en caso de que su cuenta sea hackeada: cambiar la contraseña y notificar a un adulto.

Todos los participantes identificaron correctamente un virus informático como un ejemplo de malware.

El 90% de los participantes reconoció la importancia de tener una contraseña segura para evitar que otros la adivinen.

La mayoría de los participantes (95%) supo cómo responder a un mensaje de un desconocido pidiendo dinero: no responder y decírselo a un adulto.

La mitad de los participantes ha recibido algo de educación sobre ciberseguridad en la escuela, mientras que el 30% ha recibido mucha y el 20% no ha recibido ninguna.

La gran mayoría de los participantes (95%) expresó interés en aprender más sobre cómo protegerse en internet.

Conclusión

En general, los resultados de la encuesta sugieren que los participantes tienen un conocimiento básico de ciberseguridad y son conscientes de algunos de los riesgos en línea. Sin embargo, todavía hay áreas donde la educación y la concienciación podrían mejorarse, como compartir información en redes sociales y la importancia de las contraseñas seguras. El alto interés en aprender más sobre ciberseguridad indica una disposición a mejorar sus conocimientos y habilidades en esta área.

Matriz de riesgo identificados

Tabla 8: Matriz de riesgos

Riesgo	Causa	Consecuencia	Probabilidad	Impacto
Posibilidad de afectación a la privacidad y exposición de información sensible de menores y adolescentes - Sharenting	Publicación de contenido, fotografías, videos de los menores y adolescentes sin autorización	Violación de la privacidad de los menores y adolescentes, implicaciones legales, suplantación, robo de identidad	Alto	Medio
Posibilidad de robo de	Publicación de	Acceso no	Media	Alto

Riesgo	Causa	Consecuencia	Probabilidad	Impacto
información por publicación de datos e información personal y de contacto, pérdida o robo de identidad digital por secuestro de perfiles en redes sociales, información personal y financiera – Phishing/Ingeniería social	información de contacto, perfiles de usuario sin configuraciones de seguridad y restricción de acceso	consentido a datos privados, robo de información personal, suplantación de identidad. Distorsión de la realidad por posible adoctrinamiento o fanatismos orientados a la afectación personal o de terceros		
	Publicación de información confidencial y privada, ubicación y posesiones que puede ser utilizada por atacantes que, mediante técnicas engañosas generan un ambiente de confianza y familiaridad con la víctima, lo que les permite acceder a información sensible y realizar acciones fraudulentas.	Robo y estafa físico y virtual. Suplantación de identidad física y virtual. Fraudes financieros. Afectación a terceros debido a la suplantación	Medio	Alto
Posibilidad de daño físico y emocional por acoso - Ciberbulling	Publicación de contenido mal intencionado con el fin de dañar o denigrar a uno o varios individuos relacionado con su etnia, credo, clase social, afinidad política.	Daño emocional, aislamiento social, impacto en la autoestima y salud mental de la víctima.	Alto	Alto
Posibilidad de afectación a la integridad física y mental por acoso sexual – Grooming/Sextorsión	Perfiles de redes sociales abiertos, sin ningún tipo de restricción de contacto o por contacto directo de las victimas con sus	Violación a la intimidad de los menores y adolescentes debido al contacto con extraños o	Bajo	Alto

Riesgo	Causa	Consecuencia	Probabilidad	Impacto
	atacantes en el entorno digital, lo cual les permite generar un ambiente de confianza que puede repercutir en violaciones y ataques físicos	personas del grupo social que les permite realizar acoso sexual físico y digital		
Posibilidad de afectación a la imagen y reputación física y digital debido al intercambio de contenido digital explicito – Sexting/Sextorsión	Falta de conciencia en los menores y adolescentes debido a la realización de prácticas de intercambio de mensajes, fotografías y videos con contenido sexual explicito.	Situaciones de chantaje, ciberacoso, vulneración de la privacidad y reputación en entornos físicos y digitales	Media	Alto
Posibilidad de difamación y manipulación debido a la generación o divulgación de información no verificada - Fake News	Distribución o generación de contenido difuso o de difamación de las personas, la información compartida no es verificada o cuenta con un alto grado de sensacionalismo para conseguir seguidores o interacciones “clickbait”.	Afectación a la integridad de las personas, impacto en la toma de decisiones debido a sesgos en la información, desinformación deliberada, polarización y división social, aislamiento del individuo afectado	Alto	Medio
Posibilidad de afectación física y mental ocasionada por la práctica de actividades propuestas por otros individuos en la red	Promoción y divulgación deliberada que promueven la realización de actividades riesgosos que pueden afectar la integridad física y emocional de quienes participan.	Afectación física y emocional que puede generar un alto impacto negativo en la condición física de los individuos, además de los daños sicológicos del ser	Medio	Alto

Elaboración Propia

Formulación de propuesta

De acuerdo a todo el análisis realizados a los datos encontrados acerca los delitos informáticos en Colombia entre 2023 y 2024, y los resultados de las encuestas diligenciadas por 20 estudiantes del grado 6 del colegio San Luis, se propone la creación de una guía en ciberseguridad para esta audiencia que refuerce la concienciación y educación enfatizada en la necesidad de concienciar a los usuarios sobre los riesgos en línea y las medidas de seguridad, con un enfoque particular en mujeres, adolescentes y residentes de zonas rurales. Además todavía hay áreas donde la educación y la concienciación podrían mejorarse, como compartir información en redes sociales y la importancia de las contraseñas seguras. El alto interés en aprender más sobre ciberseguridad indica una disposición a mejorar sus conocimientos y habilidades en esta área.

La creación de una guía de ciberseguridad dirigida a jóvenes en Colombia se justifica por la creciente exposición de este grupo poblacional a los riesgos del mundo digital. Los jóvenes colombianos, al igual que en el resto del mundo, son usuarios activos de internet y las redes sociales, donde interactúan, se informan y se entretienen. Sin embargo, esta participación los hace vulnerables a diversas amenazas como el ciberacoso, la sextorsión, el grooming, la suplantación de identidad y el acceso a contenido inapropiado. Una guía de ciberseguridad les brindaría las herramientas necesarias para navegar de forma segura y responsable, reconociendo los riesgos, aprendiendo a proteger su información personal y desarrollando una conciencia crítica frente al contenido que consumen y comparten en línea.

Además, la guía contribuiría a cerrar la brecha de conocimiento en ciberseguridad que existe en la población joven. A pesar de ser nativos digitales, muchos jóvenes desconocen las medidas básicas de seguridad online, como la creación de contraseñas robustas, la identificación de sitios web fraudulentos y la protección de su privacidad en redes sociales. Esta

falta de conocimiento los convierte en blancos fáciles para los ciberdelincuentes. Una guía de ciberseguridad adaptada a su lenguaje y contexto, con ejemplos claros y consejos prácticos, les permitiría adquirir las habilidades necesarias para protegerse y tomar decisiones informadas en el mundo digital.

Finalmente, la guía de ciberseguridad promovería la construcción de una cultura de ciberseguridad en Colombia. Al educar a los jóvenes sobre los riesgos y las mejores prácticas en línea, se fomenta un uso responsable y ético de las tecnologías. Esto no solo los beneficia individualmente, sino que también contribuye a crear un entorno digital más seguro para toda la sociedad colombiana. Además, al empoderar a los jóvenes en materia de ciberseguridad, se les brinda la oportunidad de convertirse en agentes de cambio, promoviendo la ciberseguridad en sus comunidades y contribuyendo a la construcción de un país más ciberseguro.

Referencias

Khan, S. (2019). Integrating Cybersecurity into the Curriculum: Challenges and Solutions. Computers & Education. https://doi.org/10.1016/j.compedu.2019.103670

McLaughlin, M., & O'Connor, C. (2020). Digital Safety and Security in Schools. Journal of Educational Technology. https://doi.org/10.1016/j.jedtech.2020.100045

Jones, T., Miller, R., & Patel, A. (2021). Creating a Culture of Cybersecurity in Schools. Journal of School Health. https://doi.org/10.1111/josh.12959

Smith, J., & Williams, L. (2022). Developing Effective Cybersecurity Programs for Students. International Journal of Cyber Education. https://doi.org/10.1016/j.ijcyberedu.2022.100037

Yadav, A. (2021). Cybersecurity in Education: An Overview. Educational Technology Research and Development. https://doi.org/10.1007/s11423-021-09987-4

We Are Social. (2024). Digital 2024: Colombia. Recuperado de https://datareportal.com/reports/digital-2024-colombia