UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁ-TICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2022 – MAYO 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA
PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANALISIS SOBRE LOS RIESGOS DE SEGURIDAD EN INTERNET Y REDES SOCIALES EN ADOLSECENTES Y MENORES DE EDAD DE LA PROVINCIA DE LOS RÍOS

ESTUDIANTE:

STEVEEN GABRIEL BELTRÁN JARAMILLO

TUTOR:

WELLINGTON ISAAC MALIZA CRUZ

AÑO 2023

PLANTEAMIENTO DEL PROBLEMA

El uso de internet y aplicaciones de redes sociales se ha vuelto cada vez más común entre niños y adolescentes. Aunque estas herramientas pueden proporcionar una gran cantidad de información y beneficios sociales, también presentan riesgos significativos para la seguridad informática de los jóvenes. Por lo tanto, el problema a analizar es la seguridad informática en internet y aplicaciones de redes sociales en niños y adolescentes.

Herramientas como internet y aplicaciones de redes sociales es un tema cada vez más relevante en la sociedad actual, especialmente en lo que respecta a los adolescentes y los niños. El acceso a internet y las redes sociales puede ser muy útil para los jóvenes, ya que les permite conectarse con amigos, acceder a información y entretenimiento, y desarrollar habilidades digitales. Sin embargo, también puede presentar una serie de riesgos de seguridad que pueden afectar negativamente su bienestar y desarrollo.

La seguridad informática es una preocupación importante para todas las edades, pero los adolescentes y los niños pueden estar particularmente en riesgo debido a su falta de experiencia y conocimientos técnicos.

Los jóvenes pueden estar en riesgo de ciberacoso, fraude en línea, exposición a contenido inapropiado, predadores en línea y malware. Además, la falta de conocimiento técnico de los niños y adolescentes sobre cómo proteger su información personal y mantenerse seguros en línea puede agravar aún más estos riesgos.

Uno de los principales problemas es el acoso cibernético, que puede tener graves consecuencias emocionales y psicológicas para los jóvenes. Además, los adolescentes y los niños también pueden ser víctimas de fraudes en línea, estafas, exposición a

contenido inapropiado y explotación por parte de predadores en línea. Otro problema importante es la pérdida de privacidad, ya que los jóvenes pueden compartir información personal en línea sin darse cuenta de las implicaciones a largo plazo.

La falta de supervisión y orientación adecuada de los padres y cuidadores puede dejar a los jóvenes vulnerables a estos riesgos. Además, las empresas de tecnología y redes sociales pueden no estar haciendo lo suficiente para garantizar la privacidad y la seguridad de los datos de los usuarios más jóvenes.

Por lo cual es especialmente preocupante dado el creciente papel que la tecnología y las redes sociales tienen en la vida cotidiana de los jóvenes. Si no se toman medidas para abordar estos riesgos, puede haber consecuencias negativas a largo plazo para la seguridad y el bienestar de los niños y adolescentes.

Este problema es aún más preocupante debido a la falta de conocimientos de los jóvenes sobre seguridad informática y su falta de experiencia en la toma de decisiones responsables en línea. Los adolescentes y niños son especialmente vulnerables a los riesgos en internet y redes sociales debido a su inexperiencia y falta de conocimiento sobre cómo navegar en línea de manera segura.

Para proteger a los niños y adolescentes de estos riesgos, es importante que los padres y cuidadores supervisen y monitoreen de cerca sus actividades en línea, establezcan reglas claras y límites sobre el uso de Internet y proporcionen educación sobre seguridad en línea. También es importante que aprendan a reconocer y evitar los riesgos de seguridad informática por sí mismos.

JUSTIFICACIÓN

Realizar una investigación sobre los riesgos de seguridad en internet y redes sociales puede ayudar a identificar las vulnerabilidades a las que se están expuestos los usuarios y desarrollar estrategias para protegerlos. Esto puede ser especialmente importante para niños y adolescentes, que a menudo no tienen el conocimiento necesario o la debida experiencia para protegerse adecuadamente en línea.

Esta investigación también puede ayudar a sensibilizar a la población sobre los peligros potenciales asociados con el uso de estas tecnologías. Al concienciar a las personas sobre los riesgos, se pueden tomar las debidas medidas preventivas para reducir el riesgo de ser víctimas de los diferentes delitos en línea. Al mismo tiempo puede proporcionar información útil para la formulación de políticas y regulaciones. Esto puede ayudar a garantizar que los usuarios estén protegidos contra los riesgos al usar el internet o aplicativos como redes sociales, y que se tomen las medidas adecuadas en caso de infracciones.

Los hallazgos de la investigación pueden proporcionar información útil sobre las debilidades de la seguridad en línea y los puntos débiles de las aplicaciones de redes sociales, lo que puede contribuir al desarrollo de tecnologías más seguras en el futuro.

En resumen, la investigación sobre los riesgos de seguridad en internet y aplicaciones de redes sociales es importante para proteger a los usuarios, sensibilizar a la población, mejorar la regulación y política, y contribuir al desarrollo tecnológico. Por lo tanto, es fundamental seguir investigando y desarrollando estrategias para reducir los riesgos de seguridad en línea.

OBJETIVOS

OBJETIVO GENERAL

- Analizar los peligros que se exponen al no tener la información sobre los riesgos de seguridad informática en internet y redes sociales.

OBEJTIVOS ESPECIFICOS

- Identificar los riesgos de seguridad en internet y redes sociales a los que están expuestos los adolescentes y niños.
- Concientizar a los adolescentes y niños al correcto uso de estas tecnologías.
- Proporcionar recomendaciones para mejorar la educación de los adolescentes y niños en seguridad en internet y redes sociales.

LINEA DE INVESTIGACIÓN

El presente caso de estudio está enfocado en la línea de investigación de sistemas de información y comunicación, emprendimiento e innovación que incluyen procesos y procedimientos para la gestión de la información, la seguridad de la información y la gestión del cambio. Esto implica la definición de políticas y normas de seguridad, la gestión de riesgos, la planificación de la continuidad del negocio, la gestión de proyectos y la capacitación de los usuarios finales en el uso de las herramientas y tecnologías de SIC.

La sublinea de redes y tecnologías inteligentes de software y hardware, que son sistemas avanzados que permiten la comunicación y el intercambio de información entre dispositivos y aplicaciones. Estos sistemas utilizan algoritmos y procesos de aprendizaje automático para analizar y procesar grandes cantidades de datos en tiempo real, permitiendo la toma de decisiones más precisas y efectivas. Además, estas tecnologías también tienen un gran potencial para mejorar la eficiencia y la sostenibilidad, al permitir un uso más inteligente y eficaz de los recursos.

Para la realización de esta investigación se aplicó el uso de la investigación cuantitativa que se basa en la recopilación y el análisis de datos numéricos y estadísticos. Esta metodología utiliza técnicas de muestreo para seleccionar una muestra representativa de la población y obtener información sobre variables específicas. En este caso sobre los distintos riesgos de internet y redes sociales existentes que afectan a los usuarios.

Hoy en día, el internet y las redes sociales se han convertido en una parte fundamental de nuestra vida cotidiana. Desde la forma en que nos comunicamos hasta cómo trabajamos y consumimos información, estas herramientas digitales han transformado la forma en que interactuamos con el mundo. Las redes sociales nos permiten conectarnos con amigos y familiares en todo el mundo, compartir nuestros intereses y opiniones, y descubrir nuevas ideas y oportunidades. Además, el internet nos brinda acceso a una amplia variedad de recursos educativos, noticias, entretenimiento y servicios en línea que antes no estaban disponibles. Sin embargo, el uso excesivo de estas herramientas también puede tener consecuencias negativas en nuestra salud mental, física y emocional. Por lo tanto, es importante que utilicemos estas herramientas de manera responsable y equilibrada, manteniendo un equilibrio saludable entre nuestra vida en línea y fuera de línea. En la presente investigación, discutiré algunos de los peligros más comunes del internet y las redes sociales, y cómo podemos protegernos de ellos.

RIESGOS DE LAS REDES SOCIALES

Las redes sociales, como Facebook, Twitter, Instagram y Snapchat, forman parte de nuestro día a día ya que estamos conectados a estas redes sociales todo el día en su gran mayoría de casos. Sin embargo, estas plataformas pueden presentar riesgos importantes para la privacidad, la seguridad y la salud mental de los usuarios. Las redes sociales son una herramienta poderosa para conectarnos con amigos y familiares, pero también presentan peligros importantes. Uno de los mayores riesgos es la exposición a información personal y privada. (Etecé, 2021)

Las redes sociales han revolucionado la forma en que nos comunicamos, compartimos información y nos conectamos con el mundo que nos rodea. Sin embargo, también presentan riesgos significativos para la seguridad, la privacidad y la salud mental de los usuarios. A continuación, se presentan algunos de los peligros más comunes de las

redes sociales, junto con citas de investigaciones y estudios que los respaldan. (Etecé, 2021)

Exposición a contenido inapropiado: Las redes sociales pueden exponer a los usuarios a contenido inapropiado, violento o sexualmente explícito. Según un estudio de la Academia Estadounidense de Pediatría, el 42% de los adolescentes informaron haber sido expuestos a contenido sexualmente explícito en línea. (Kraus, 2019).

ACOSO EN LÍNEA

El acoso en línea, también conocido como ciberacoso, es un problema creciente en la sociedad actual. Se refiere al acoso, la intimidación, la difamación y otras formas de abuso que ocurren a través de plataformas en línea como redes sociales, mensajes de texto y correo electrónico. El acoso en línea puede tener un impacto significativo en la salud mental y emocional de las víctimas, incluyendo la ansiedad, la depresión y el aislamiento social. (Duggan, 2019)

Además, el acoso en línea puede tener consecuencias graves y duraderas, como el acoso en el lugar de trabajo o la disminución de las oportunidades educativas y laborales. Es importante que las víctimas de acoso en línea reciban apoyo y asistencia para hacer frente a las consecuencias emocionales y legales del acoso en línea. También se deben tomar medidas para prevenir el acoso en línea, la aplicación de leyes y políticas que aborden el acoso en línea. (Duggan, 2019)

El acoso en línea es un problema común en las redes sociales y puede tener consecuencias graves a los usuarios. Según una encuesta de Pew Research Center, el 41% de los adultos estadounidenses informó haber experimentado algún tipo de acoso en línea (Duggan, 2019).

RIESGO DE PRIVACIDAD

La privacidad en internet y las redes sociales es un tema importante, especialmente para los jóvenes. Las redes sociales y otras plataformas en línea a menudo recopilan información personal de los usuarios, incluyendo su nombre, dirección, edad y otros datos sensibles. Esta información puede ser utilizada por anunciantes y otras empresas para dirigirse a los usuarios con publicidad personalizada y, en algunos casos, vender su información a terceros.

Es importante que los jóvenes entiendan los riesgos de privacidad en línea y tomen medidas para proteger su información personal. Esto incluye ajustar la configuración de privacidad en las redes sociales y evitar compartir información personal innecesaria. Los jóvenes también deben tener cuidado al momento de ingresar a links de procedencia sospechosa o no verificada o descargar programas gratuitos en la red, ya que esto puede poner en peligro su seguridad en línea. (Moreno, 2021)

Los padres y otros adultos responsables también pueden desempeñar un papel importante en la protección de la privacidad de los jóvenes en línea. Esto puede incluir educar a los jóvenes sobre la importancia de la privacidad en línea y supervisar su actividad en línea para detectar posibles amenazas. En general, la protección de la privacidad en línea debe ser una preocupación importante para todos los usuarios de internet. (Moreno, 2021)

Las redes sociales pueden comprometer la privacidad de los usuarios al compartir información personal o exponerla a personas no autorizadas. Según un estudio de la Universidad de Pensilvania, el 13% de los adolescentes informó haber recibido solicitudes de amistad de extraños en línea (Moreno, 2021).

COMUNIDAD VULNERABLE (NIÑOS Y ADOLESCENTES)

Los adolescentes y niños son la comunidad más vulnerable a riesgos en Internet y redes sociales debido a su falta de experiencia y madurez en línea. Los riesgos pueden incluir el acoso en línea, el ciberacoso, el grooming, la exposición a contenido inapropiado o violento, la adicción a los juegos en línea y la pérdida de privacidad y seguridad. Los niños y adolescentes son particularmente susceptibles a la manipulación y el engaño en línea, lo que puede resultar en el robo de información personal o el acceso a sitios web maliciosos. (Malckiff, 2021)

Además, pueden ser víctimas de depredadores en línea que buscan explotar su vulnerabilidad y falta de conocimiento. Es importante que los padres y tutores tomen medidas para proteger a sus hijos en línea, como supervisar su actividad en línea, establecer límites de tiempo para el uso de Internet y enseñarles las mejores prácticas de seguridad en línea y así poder evitar cualquier tipo de vulnerabilidad que ponga en peligro su integridad y así a concientizar a la protección en internet y redes sociales. (Malckiff, 2021)

Los peligros a los que están expuestos incluyen el ciberacoso, el acoso en línea, la exposición a contenido inapropiado, la adicción a los juegos en línea, el grooming y el contacto con desconocidos. La falta de experiencia en línea de los niños y adolescentes puede resultar en una mayor susceptibilidad a la manipulación y el engaño. Los depredadores en línea pueden aprovecharse de la ingenuidad de los jóvenes y utilizar la red para fines maliciosos, como el robo de información personal o el acceso a sitios web maliciosos. (Malckiff, 2021)

ADICCIÓN A LAS REDES SOCIALES

La adicción a las redes sociales es un problema común en la sociedad actual. El fácil acceso y la constante disponibilidad de las redes sociales a través de dispositivos móviles y computadoras ha llevado a un aumento en el tiempo que las personas pasan en

estas plataformas. La adicción a las redes sociales puede afectar negativamente la salud mental, ya que puede aumentar la ansiedad, el aislamiento social y la depresión. Además, puede afectar el rendimiento laboral y académico, y limitar el tiempo que las personas pasan interactuando cara a cara con amigos y familiares (Rodriguez, 2021).

Las redes sociales pueden ser adictivas y consumir gran parte del tiempo y la atención de los usuarios. Según un estudio del Pew Research Center, el 69% de los adultos estadounidenses utilizan las redes sociales, y el 51% de ellos informó que utilizan las redes sociales varias veces al día (Rodriguez, 2021).

La adicción a las redes sociales puede tener un impacto significativo en la sociedad juvenil. Los jóvenes son particularmente vulnerables a los efectos negativos de las redes sociales, ya que suelen pasar más tiempo en línea y tener menos experiencia en la gestión de su tiempo. La adicción a las redes sociales puede afectar su capacidad para desarrollar relaciones significativas fuera de la pantalla y limitar su tiempo dedicado a actividades importantes, como el trabajo escolar o los deportes. (Rodriguez, 2021)

Además, la adicción a las redes sociales puede aumentar el riesgo de acoso en línea y la exposición a contenidos inapropiados. Es importante que los jóvenes reciban educación sobre el uso saludable de las redes sociales y aprendan a equilibrar su tiempo en línea y fuera de línea. Los padres, educadores y otros adultos responsables también tienen la responsabilidad de supervisar y guiar a los jóvenes en su uso de las redes sociales. (Rodriguez, 2021)

DESINFORMACIÓN Y PROPAGANDA

La desinformación en internet y la propaganda engañosa son un problema común en la actualidad. La facilidad para difundir información en línea ha llevado a la creación y propagación de noticias falsas y rumores sin fundamento, que pueden ser perjudiciales para las personas y la sociedad en general. Además, los anunciantes y los políticos pueden utilizar técnicas de propaganda engañosa para influir en la opinión pública y obtener

ganancias o poder. Para combatir esta situación, es importante que los usuarios de internet verifiquen la fuente de la información y analicen la validez de los datos antes de compartirla. También se recomienda la educación en alfabetización mediática y crítica para ayudar a las personas a identificar y evitar la desinformación en línea.

Las redes sociales pueden ser utilizadas para la difusión de información errónea o propaganda, lo que puede afectar negativamente la percepción del usuario sobre temas importantes. Según un estudio del Pew Research Center, el 64% de los adultos estadounidenses cree que las redes sociales tienen un impacto mayormente negativo en la forma en que las noticias se distribuyen en nuestro país (Galán, 2021).

EXPOSICIÓN A CIBERDÉLITOS

El internet y redes sociales pueden exponer a los usuarios a ciberdelitos, como el phishing y la suplantación de identidad. Según un estudio de la empresa de seguridad informática NortonLifeLock, el 21% de los jóvenes/adultos estadounidenses informó haber sido víctima de un ciberdelito en línea.

La exposición a ciberdelitos es una preocupación creciente en la era digital. Los ciberdelincuentes pueden utilizar una variedad de técnicas para acceder a información personal, financiera y empresarial a través de dispositivos conectados a internet. Estos delitos incluyen phishing, ransomware, malware y ataques de hacking. La exposición a estos riesgos puede tener consecuencias graves, como la pérdida de datos importantes, la pérdida de dinero y el robo de identidad. (NortonLife, 2021)

Para protegerse contra estos riesgos, es importante que los usuarios tomen medidas adecuadas, como ajustar las opciones de privacidad en las redes sociales, utilizar contraseñas seguras, limitar el tiempo dedicado a las redes sociales y educarse sobre los peligros asociados. Al tomar medidas de precaución adecuadas, los usuarios pueden disfrutar de los beneficios de las redes sociales mientras minimizan los riesgos asociados. (NortonLife, 2021)

RIESGOS DEL INTERNET

El uso del internet conlleva ciertos riesgos que deben ser considerados. La exposición a contenidos inapropiados, la suplantación de identidad, el acoso en línea y la exposición a virus y malware son solo algunos de los peligros que pueden afectar a los usuarios de internet. Es importante que las personas tomen medidas para protegerse, como usar contraseñas seguras, mantener el software actualizado y ser conscientes de los riesgos asociados con la navegación en línea. (Etecé, 2023)

Hay que tener en cuenta que los riesgos al momento de navegar en internet son demasiado grandes y mucho más cuando tienes escasos o nulos conocimientos de como resguardar tu información en línea o en aplicaciones, ya que estás muchas veces son echas con propósitos no legales y pueden perjudicar de grandes formas tu vida. Principalmente teniendo en cuenta que la gran mayoría de la población no conoce de estos riesgos o simplemente no les interesa conocer para poder resguardar sus datos en la red. (Etecé, 2023)

Dentro de este grupo de vulnerabilidades en la red tenemos las siguientes:

- Riesgos de privacidad y manejo de la información confidencial.

Los riesgos de privacidad y manejo de la información confidencial son cada vez más significativos en el mundo digital actual. Con la creciente cantidad de datos que se generan y comparten en línea, la protección de la privacidad y la seguridad de la información se ha convertido en un desafío crítico. Las amenazas a la privacidad y la seguridad pueden incluir la recopilación no autorizada de datos personales, la filtración de información confidencial, el robo de identidad, el ransomware y otros tipos de ataques cibernéticos.

- Riesgos propios de la interacción con terceros

La interacción con terceros en la Internet puede ser riesgosa y potencialmente peligrosa debido a la falta de control sobre los datos que se comparten y la confiabilidad de los otros usuarios. Los riesgos pueden incluir la divulgación de información personal, el acoso en línea, la propagación de virus y malware, el phishing y el fraude en línea.

- Riesgos de acceso a información falsa o sensible.

El acceso a información falsa o sensible puede ser riesgoso debido a la posibilidad de que la información sea utilizada de manera inapropiada. La información falsa puede llevar a decisiones equivocadas o dañar la reputación de una persona o una organización. Por otro lado, la información sensible, como datos financieros o de identidad personal, puede ser utilizada por ciberdelincuentes para cometer fraude o robo de identidad.

- Riesgos derivados del mal uso de internet.

El mal uso de Internet puede tener consecuencias graves para la privacidad, la seguridad y la reputación de los usuarios. Los riesgos pueden incluir el acoso en línea, el ciberacoso, la exposición a contenido inapropiado o violento, el acceso a sitios web maliciosos y la descarga de malware. Además, el mal uso de Internet también puede incluir el uso inadecuado de las redes sociales, como compartir información personal o confidencial o publicar contenido inapropiado que puede afectar la reputación personal o profesional.

CÓMO PROTEGERSE

Aunque existen muchos riesgos asociados con el internet y las redes sociales, hay medidas que los usuarios pueden tomar para protegerse a sí mismos y a sus datos.

En primer lugar, es importante configurar adecuadamente las opciones de privacidad en las redes sociales para limitar la exposición de información personal.

Además, los usuarios deben tener precaución al aceptar solicitudes de amistad o mensajes de personas desconocidas. Es importante educar a los niños y adolescentes sobre los riesgos del internet y supervisar su uso. Los padres también deben considerar utilizar software de control parental para limitar el acceso a contenido inapropiado. (Confianza, 2020)

Los usuarios deben tener precaución al hacer clic en enlaces o descargar software. Es importante utilizar software antivirus y mantener los dispositivos actualizados para protegerse contra virus y malware. El internet ha cambiado radicalmente la forma en que nos comunicamos, trabajamos y nos entretenemos. Sin embargo, también ha creado riesgos significativos para nuestra seguridad, privacidad y salud mental. (Confianza, 2020)

Una de las mayores preocupaciones relacionadas con el internet es la exposición a contenido inapropiado. Los niños y adolescentes pueden ser especialmente vulnerables a este riesgo, ya que pueden ser expuestos a contenido violento, sexualmente explícito o inapropiado para su edad. En un estudio de la Academia Estadounidense de Pediatría, se encontró que el 42% de los adolescentes había sido expuesto a contenido sexualmente explícito en línea (Confianza, 2020).

AQUÍ TIENES ALGUNOS CONSEJOS DE SEGURIDAD EN INTERNET Y REDES SOCIALES

Utiliza autenticación de dos factores

La autenticación de dos factores (2FA) es un método de seguridad informática que requiere dos formas diferentes de verificación para permitir el acceso a una cuenta o sistema. Esto proporciona una capa adicional de seguridad, ya que incluso si un atacante logra obtener la contraseña de un usuario, aún necesitaría otro factor de autenticación, como un código generado por una aplicación o un mensaje de texto enviado a un teléfono móvil, para acceder a la cuenta. (Evans, 2019)

Usa una VPN

Utilizar una red privada virtual (VPN) es una forma cada vez más popular de protegerse en línea. Una VPN enmascara la dirección IP del usuario y cifra su conexión a Internet, lo que significa que los datos que se envían y reciben están protegidos y no pueden ser interceptados por terceros. Esto es particularmente importante en situaciones en las que el usuario está utilizando una red Wi-Fi pública, que es más vulnerable a los ataques de hackers. (Evans, 2019)

Además de proteger la privacidad y seguridad del usuario en línea, una VPN también puede permitir el acceso a contenido restringido geográficamente, lo que la convierte en una herramienta útil para quienes desean acceder a sitios web y servicios que de otra manera estarían bloqueados en su ubicación actual o no contienen los permisos suficientes para establecer un funcionamiento correcto debido a las políticas de tu país de origen. (Evans, 2019)

Protege la red wifi de tu casa

Proteger la red Wi-Fi de una casa es importante para prevenir ciberdelitos. Una de las primeras medidas de seguridad que se deben tomar es cambiar el nombre y la contraseña predeterminados del router para evitar que los atacantes accedan a la red utilizando credenciales por defecto. También se debe configurar una contraseña segura y robusta que no sea fácilmente adivinable. Otra medida es utilizar un cifrado Wi-Fi, como WPA2 o WPA3, para asegurar que los datos transmitidos a través de la red estén protegidos. (Kaspersky, 2023)

Por último, se debe mantener el firmware del router actualizado para asegurarse de que se estén parcheando las vulnerabilidades conocidas y que el router esté funcionando con el mejor nivel de seguridad posible. Es recomendable también habilitar un firewall en el router para filtrar el tráfico de la red y bloquear los intentos de acceso no autorizados. (Kaspersky, 2023)

Es importante tener conocimientos sobre cómo proteger una red doméstica para prevenir delitos cibernéticos, ya que el uso de dispositivos conectados a Internet está aumentando cada vez más en los hogares. Sin una adecuada protección, los atacantes pueden acceder a la red doméstica y comprometer la privacidad y seguridad de los dispositivos conectados, lo que puede resultar en la pérdida de datos personales, financieros o de otro tipo. (Kaspersky, 2023)

Además, los ciberdelincuentes pueden utilizar una red doméstica comprometida para realizar actividades ilegales, como el envío de correo basura o ataques de denegación de servicio. Por lo tanto, conocer y aplicar medidas de seguridad en la red doméstica es esencial para protegerse contra los delitos cibernéticos y mantener la privacidad y seguridad en línea. (Evans, 2019)

El internet también puede ser utilizado para el robo de identidad. Los delincuentes pueden obtener información personal, como números de seguro social y fechas de nacimiento, y utilizarla para abrir cuentas de crédito y realizar compras en línea. El robo de identidad puede tener consecuencias graves para la vida financiera de la víctima, y puede ser difícil de resolver una vez que se ha producido. (Evans, 2019)

Finalmente, el internet puede ser utilizado para la propagación de virus y malware. Los usuarios pueden descargar software malicioso sin saberlo, lo que puede comprometer la seguridad de sus dispositivos y su información personal. Según un estudio de la empresa de seguridad informática NortonLifeLock, se produjeron más de 10,2 millones de intentos de ataques de malware en 2020. Es importante utilizar software antivirus y mantener los dispositivos actualizados para protegerse contra estos tipos de ataques. (NortonLife, 2021)

Para protegerse contra estos riesgos, los usuarios deben ser conscientes de los peligros y tomar medidas para proteger su información personal y financiera. Es importante utilizar contraseñas seguras y cambiarlas regularmente, así como configurar

opciones de privacidad adecuadas en las redes sociales y otras plataformas en línea. Los usuarios también deben tener precaución al hacer clic en enlaces o descargar software, y utilizar software antivirus para protegerse contra virus y malware. (NortonLife, 2021)

El internet presenta una serie de riesgos para la seguridad, privacidad y salud mental de los usuarios. Sin embargo, al tomar medidas adecuadas para protegerse y educarse sobre los peligros, los usuarios pueden disfrutar de los beneficios del internet mientras minimizan los riesgos asociados. (NortonLife, 2021) La población más vulnerable a los delitos cibernéticos puede variar según el tipo de delito en cuestión. Sin embargo, se puede señalar a ciertos grupos como especialmente vulnerables:

Los niños y adolescentes: los menores de edad son particularmente vulnerables a la exposición a contenido inapropiado y a ser víctimas de acoso en línea. Un estudio de la ONG Childnet International encontró que el 34% de los niños y jóvenes encuestados en Europa reportaron haber visto imágenes inapropiadas en línea, y el 11% había sido objeto de ciberacoso (Childnet International, 2021).

Los ciber delitos hoy en día están siendo más frecuentes que años posteriores debido a la propagación de la tecnología y la implementación de la misma en nuestras vidas, básicamente son delitos que se realizan en la red y al igual que los demás delitos existentes es recomendable estar al tanto sobre ellos . Es importante tener en cuenta que cualquier persona puede ser víctima de delitos cibernéticos y que la vulnerabilidad no se limita a los grupos mencionados anteriormente (Paredes, 2021)

En Ecuador, algunos de los delitos cibernéticos más frecuentes son:

Fraudes en línea: Estafas a través de internet en las que los delincuentes solicitan información personal y financiera de las víctimas para utilizarla en actividades ilegales.

Phishing: Delito en el que se suplanta la identidad de una entidad financiera o gubernamental para obtener información confidencial de las víctimas.

Robo de identidad: Consiste en el uso no autorizado de la información personal de alguien para cometer fraude.

Ciberacoso: Se trata de un tipo de acoso que se realiza a través de internet y que puede incluir amenazas, intimidación y difamación.

Pornografía infantil: Delito en el que se producen, distribuyen o se accede a contenidos pornográficos que involucran a menores de edad.

Según datos del Ministerio del Interior de Ecuador, los casos de fraude en línea y phishing han aumentado en los últimos años. En 2019, se registraron más de 3.500 denuncias por delitos cibernéticos en el país, lo que representa un aumento del 28% en comparación con el año anterior, es importante destacar que la lista de delitos cibernéticos puede variar en función del país y de la realidad social y tecnológica de cada lugar. (Interior, 2020)

Uno de los mayores delitos cibernéticos conocidos en Ecuador ocurrió en el año 2019, cuando se descubrió una brecha de seguridad en un servidor de la empresa Novaestrat que expuso datos personales de casi toda la población ecuatoriana. La información filtrada incluía nombres completos, fechas de nacimiento, números de identificación, direcciones de correo electrónico, números de teléfono y registros de votantes. (Interior, 2020)

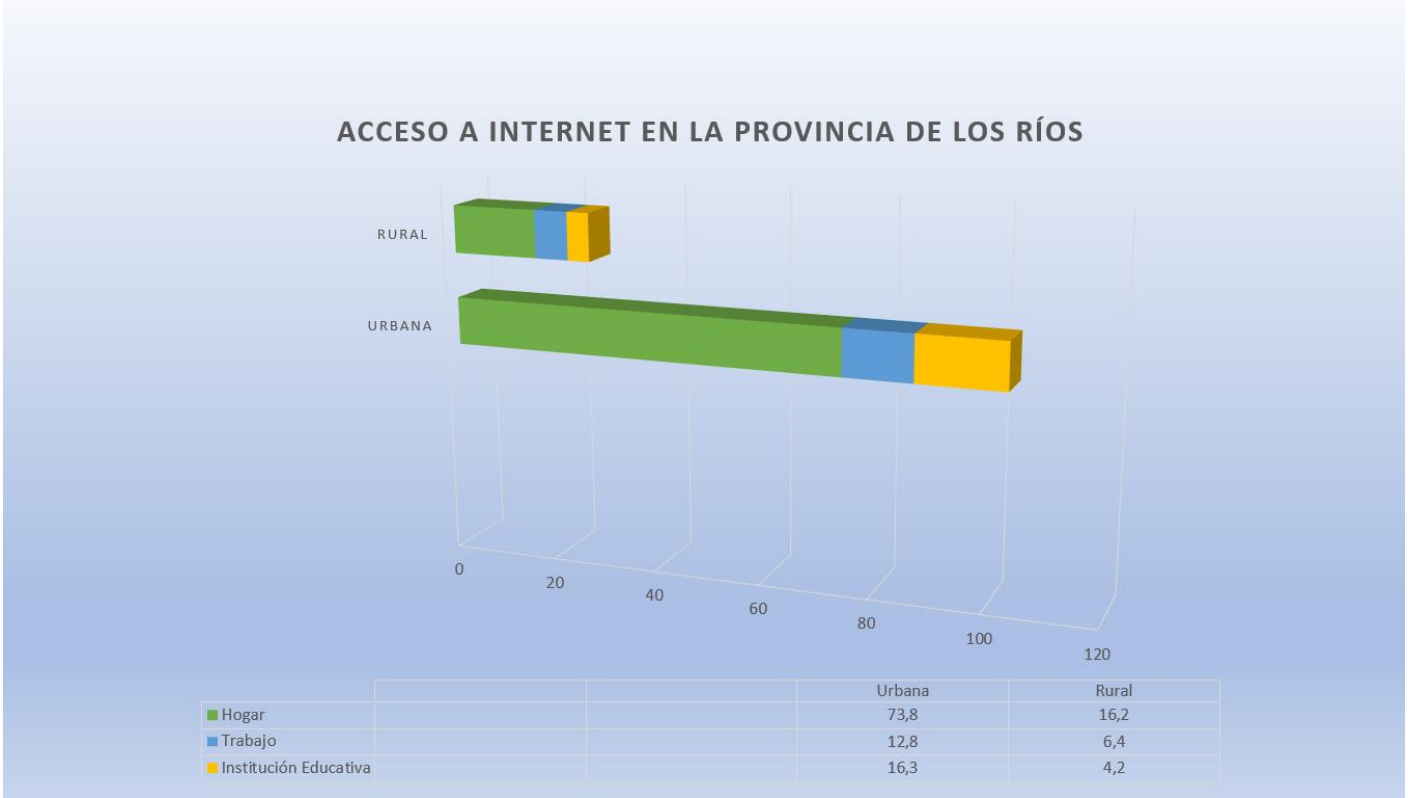
Este incidente de seguridad se considera uno de los mayores delitos cibernéticos en la historia de Ecuador y ha generado una gran preocupación en torno a la seguridad de los datos personales en el país. Las autoridades ecuatorianas han tomado medidas para investigar y castigar a los responsables de esta violación masiva de la privacidad, pero también se ha destacado la necesidad de mejorar la seguridad cibernética en el país y aumentar la conciencia pública sobre los riesgos asociados al uso de la tecnología. (Interior, 2020)

METODOLOGÍA

La investigación se realizó a través de los procesos cuantitativos (análisis de contenido), efectuando un estudio selectivo de información que revele el uso de la internet y las redes sociales en los ecuatorianos, también se generó un análisis de las diferentes redes sociales usadas en la provincia, dirigiéndose por las más usadas a la menos usadas, tanto como por la cantidad de usuarios y perfiles que estás redes sociales contienen. Categorizadas con una información selecta por medio de datos estadísticos y por medios de comunicación que cumplían con las características de esta investigación.

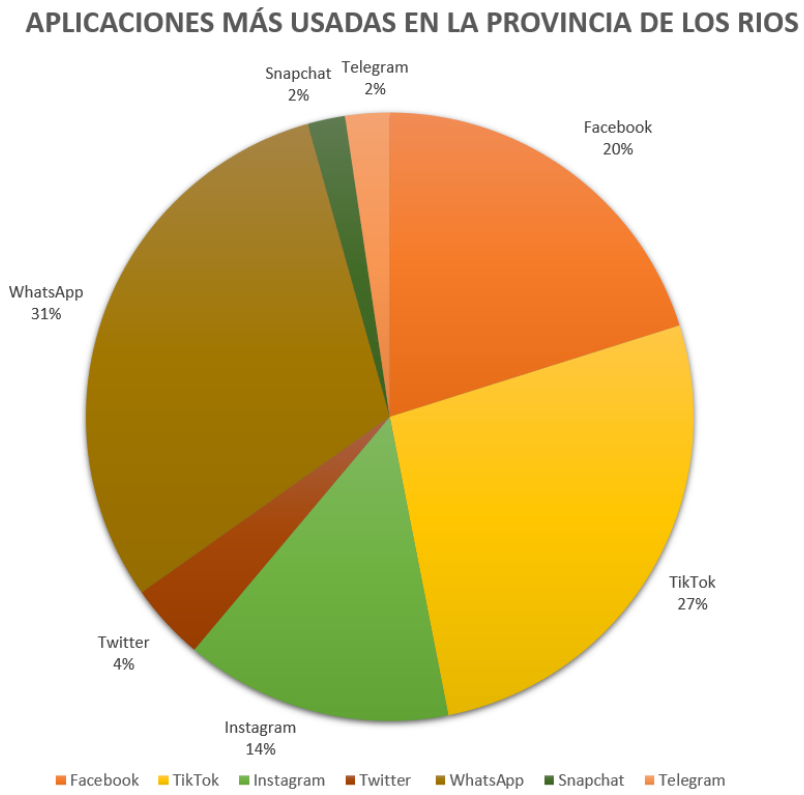
Esta técnica se basa en la recolección de datos numéricos, que se analizan utilizando herramientas estadísticas para identificar patrones y relaciones entre las variables. En este tipo de estudio, se utilizan cuestionarios estandarizados para recopilar información sobre el uso de internet y redes sociales, así como sobre los comportamientos y actitudes de los jóvenes y niños hacia los riesgos en línea. Los datos recopilados se analizan para determinar la prevalencia de diferentes tipos de riesgos, así como para identificar los factores que pueden estar asociados con un mayor riesgo de exposición. La metodología cuantitativa es una herramienta útil para entender mejor los riesgos en línea y desarrollar estrategias efectivas para prevenirlos. En cuanto a la información obtenida se inclinó al uso de las redes sociales en la población ecuatoriana y algunos datos estadísticos referente al uso de la tecnología y del uso de la Internet.

RESULTADOS

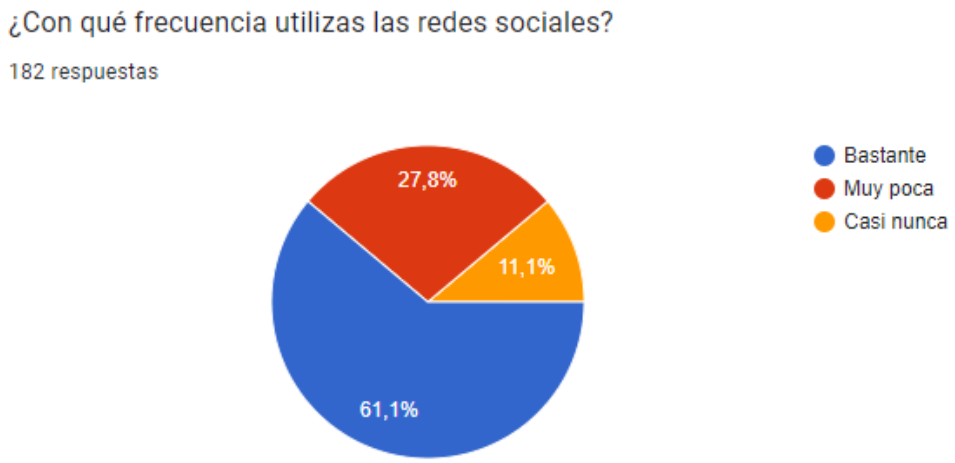


			Urbana	Rural
Hogar			73,8	16,2
Trabajo			12,8	6,4
Institución Educativa			16,3	4,2

Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]



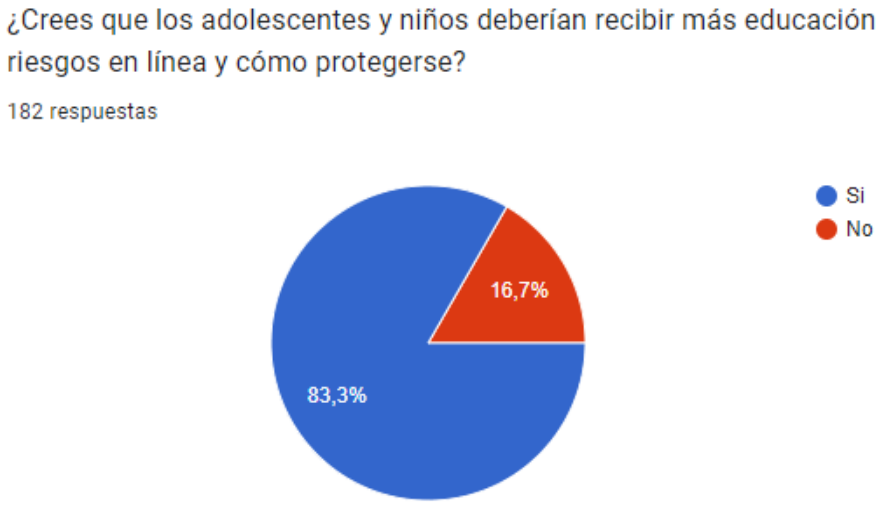
Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]



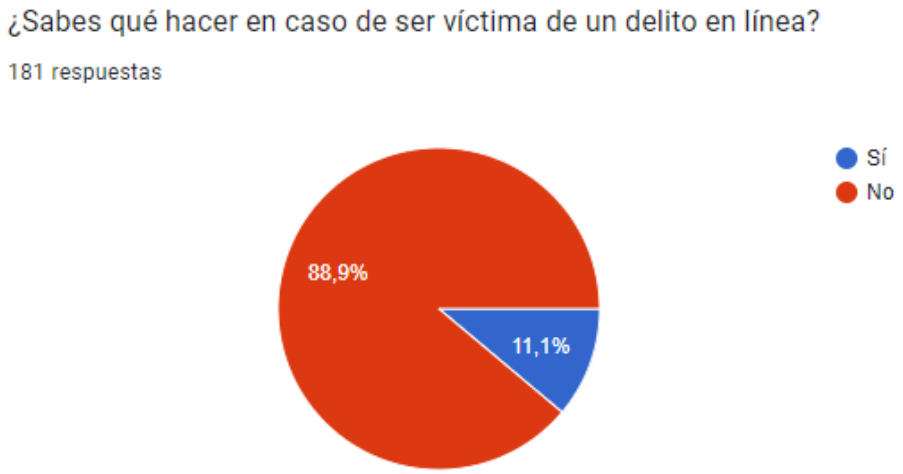
Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]

Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]

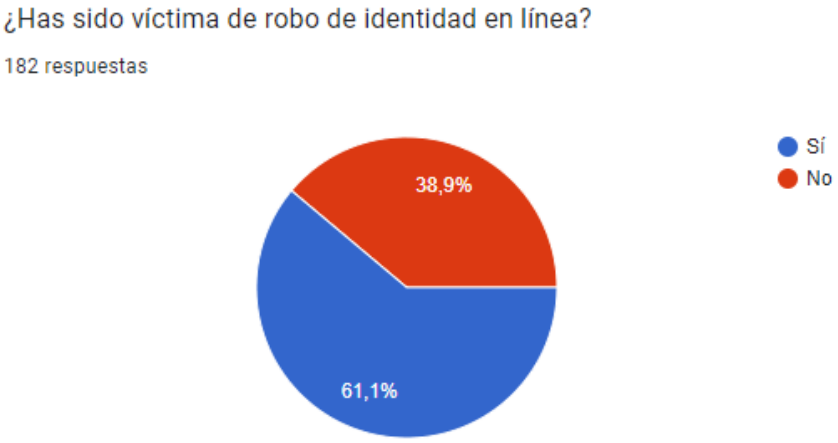
Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]



Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]



Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]



Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]

DISCUSIÓN DE RESULTADOS

Los resultados indican que el consumo internet y redes sociales a aumentado significativamente, esta tendencia se ha acelerado con la creciente accesibilidad de dispositivos móviles y la disponibilidad de internet en la mayoría de los hogares.

Los adolescentes y los niños usan las redes sociales para conectarse con amigos y familiares, compartir intereses y expresarse creativamente, como podemos notar en la gráfica de las aplicaciones que tienen más uso en la provincia de Los Ríos tenemos un gran abarcamiento en su mayoría por la aplicación de mensajería instantánea WhatsApp 31%, TikTok 27%, Facebook 20%, Instagram 14%, Twitter 4%, Snapchat 2%, Telegram 2% de usuarios.

De acuerdo con las estadísticas, la mayoría de los usuarios de redes sociales las utilizan con bastante frecuencia, representando el 61,1%. Mientras que un porcentaje significativamente menor, el 27,8%, las utiliza muy poco y solo un pequeño grupo, el 11,1%, rara vez las utiliza. En resumen, la mayoría de los usuarios son activos en las redes sociales, mientras que una minoría prefiere utilizarlas con moderación o casi nunca.

Los datos muestran que el ciberacoso es un problema común y extendido, con el 66,7% de los encuestados informando que han sido víctimas de este delito en línea. Es preocupante que un 33,3% de los encuestados aún no hayan experimentado el ciberacoso, ya que esto indica que el problema sigue siendo prevalente y que se deben tomar medidas para prevenirlo y proteger a los jóvenes en línea.

Los resultados de una encuesta reciente indican que un gran porcentaje de usuarios de redes sociales, el 72,2%, no saben cómo proteger su privacidad en línea. Es importante que los usuarios entiendan cómo las redes sociales recopilan y utilizan su información personal, y cómo pueden controlar quién puede acceder a ella. Los usuarios pueden proteger su privacidad ajustando su configuración de privacidad en sus cuentas de redes sociales, limitando la información personal que comparten y evitando publicar

información sensible. Por otro lado, el 27,8% de los usuarios encuestados que conocen cómo proteger su privacidad pueden servir como modelos a seguir para otros usuarios de redes sociales.

Los datos muestran que la educación sobre los riesgos en línea y cómo protegerse es ampliamente valorada, con el 83,3% de los encuestados indicando que sería beneficioso recibir más educación sobre este tema. Es importante que se brinden oportunidades para la educación en línea y se concientice sobre los riesgos y precauciones que se deben tomar para evitar el acoso, la exposición a contenidos inapropiados y la vulnerabilidad a los delitos en línea. Aunque el 16,7% de los encuestados no creen que sería beneficioso recibir educación adicional, es importante continuar fomentando la importancia de la educación sobre seguridad en línea para garantizar un entorno en línea seguro y protegido para todos los usuarios.

Los datos indican que la mayoría de los usuarios, el 88,9%, no sabe qué hacer en caso de ser víctimas de un delito en línea. Es importante que se brinden recursos y orientación para ayudar a los usuarios a tomar medidas enérgicas y reportar cualquier actividad delictiva en línea a las autoridades adecuadas. El 11,1% de los usuarios encuestados que saben qué hacer en caso de ser víctimas de delitos en línea pueden servir como modelos a seguir y ayudar a difundir información sobre los recursos disponibles y los pasos que se deben tomar en caso de ser víctima de un delito en línea.

Según la información recopilada, el robo de identidad en línea es un problema común, ya que el 61,1% de los usuarios encuestados han sido víctimas de este delito en línea. El robo de identidad puede tener graves consecuencias financieras y personales para las víctimas, y puede ser difícil de resolver una vez que ha ocurrido. Es alentador ver que el 38,9% de los usuarios encuestados aún no han sido víctimas de robo de identidad en línea, pero es importante seguir fomentando la educación sobre la protección de la identidad en línea y la seguridad cibernética en general. Es importante que se brinden

herramientas y recursos para ayudar a los usuarios a proteger su información personal y financiera en línea, y que se tomen medidas para prevenir el robo de identidad y proteger a los usuarios en línea.

CONCLUSIONES

En conclusión, el estudio de caso sobre los riesgos del internet y redes sociales en los adolescentes y niños realizado en la provincia de Los Ríos evidencia la importancia de educar y concienciar a los jóvenes sobre los peligros asociados con el uso irresponsable de estas herramientas digitales.

La seguridad en línea es un tema crítico debido a los numerosos riesgos a los que los usuarios están expuestos. Estos riesgos incluyen, entre otros, el malware, el phishing, la ingeniería social, el ransomware, la suplantación de identidad, el robo de información personal, el acoso en línea, el sexting, el grooming y la exposición a contenidos inapropiados. Además, el aumento de los dispositivos conectados a Internet, como los dispositivos IoT, también ha dado lugar a nuevas vulnerabilidades de seguridad. Por lo tanto, es importante que los usuarios estén al tanto de los peligros en la internet y así puedan tener en cuenta medidas para resguardar su información personal en línea.

La falta de educación digital temprana podría tener consecuencias negativas a largo plazo para los niños y jóvenes. Sin una comprensión adecuada de los riesgos y beneficios de la tecnología, los niños podrían estar expuestos a riesgos en línea, como la exposición a contenido inapropiado o peligroso, el acoso en línea, el grooming y el sexting. Además, la falta de educación digital podría llevar a un uso excesivo y poco saludable de la tecnología, lo que podría afectar negativamente la salud mental y física de los niños.

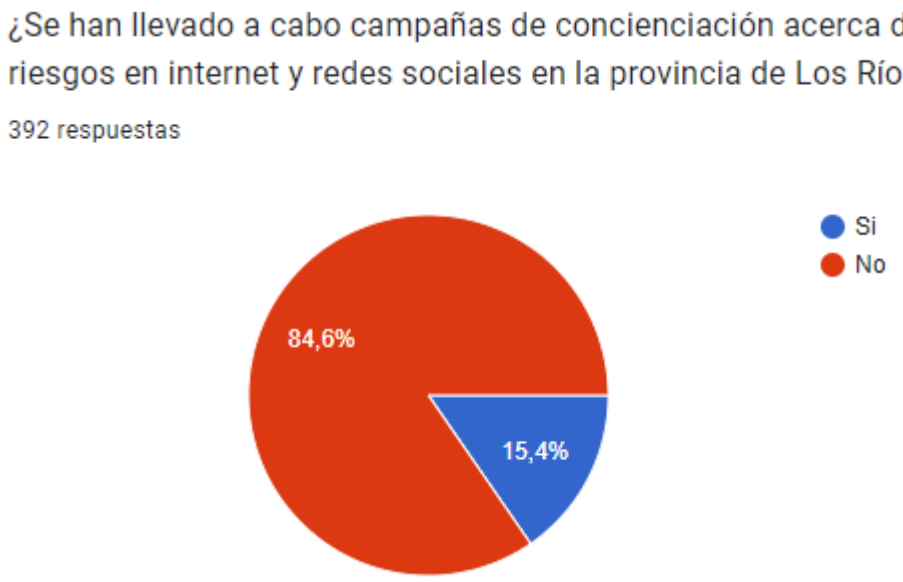
La falta de supervisión y comunicación abierta sobre temas de riesgos en internet y redes sociales puede ser perjudicial para los niños y adolescentes. Si los padres y tutores no supervisan el uso de internet y las redes sociales, los niños y adolescentes pueden estar en riesgo de exponer su información personal en línea, ser víctimas de acoso en línea o ser expuestos a contenidos inapropiados

RECOMENDACIONES

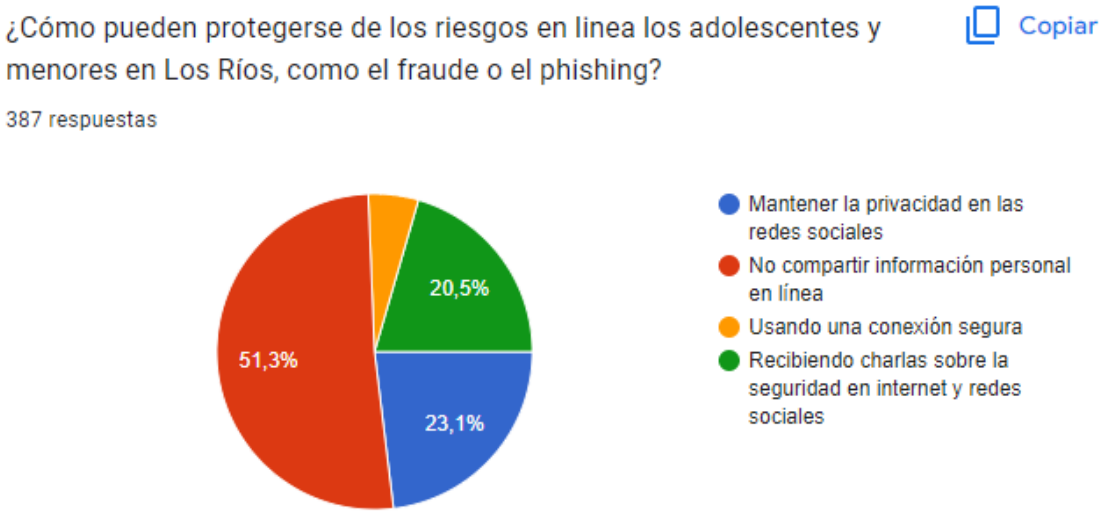
Basándonos en los hallazgos encontrados en el estudio de riesgos de seguridad en internet y redes sociales en adolescentes y niños en la provincia de Los Ríos, podemos aplicar algunas recomendaciones acerca sobre los riesgos en la red.

- **Promover una educación digital temprana:** Es importante que los padres, tutores y educadores enseñen a los niños y adolescentes a usar internet de forma responsable y segura desde una edad temprana. Esto puede incluir la enseñanza de cómo proteger su información personal en línea, cómo identificar el acoso en línea y cómo evitar sitios web inapropiados.
- **Supervisión y comunicación abierta:** Es fundamental que los padres, tutores y educadores mantengan una comunicación abierta y honesta con los niños y adolescentes sobre su actividad en línea. También es importante que se involucren en supervisar las actividades de los menores en línea para asegurarse de que estén seguros y no estén expuestos a ningún riesgo.
- **La educación sobre la seguridad en línea:** Puede enseñar a las personas cómo proteger su información personal, identificar correos electrónicos fraudulentos, evitar estafas en línea y proteger su privacidad. Además, la educación sobre la seguridad en línea también puede ayudar a las personas a reconocer y enfrentar el ciberacoso, el acoso en línea y otros tipos de comportamientos inapropiados en línea. Al tener una educación sólida sobre la seguridad en línea, las personas pueden navegar de manera más segura y confiada en el mundo digital.

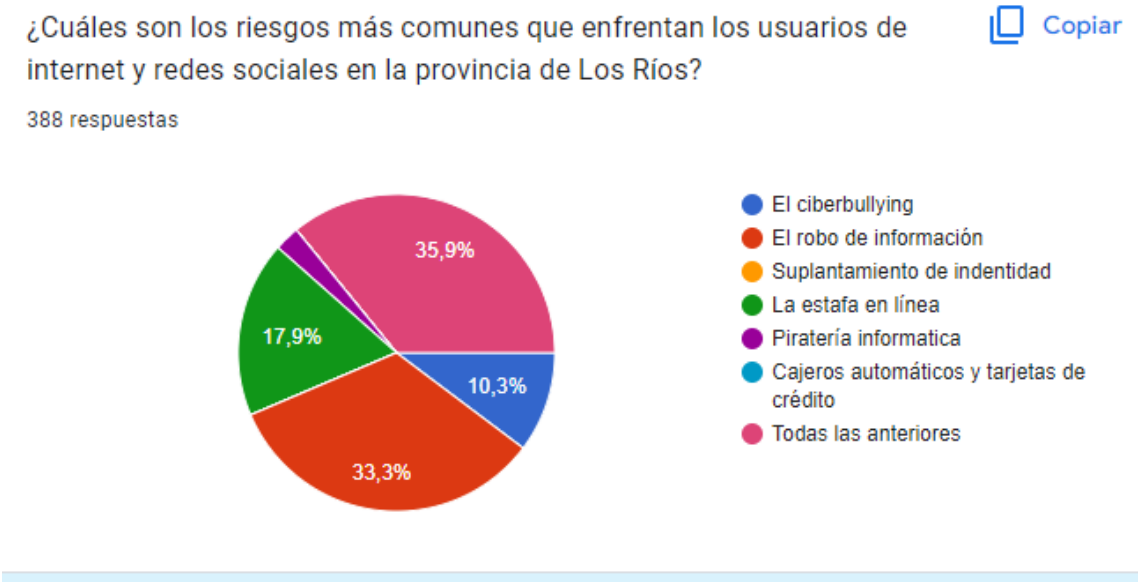
ANEXOS



Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]

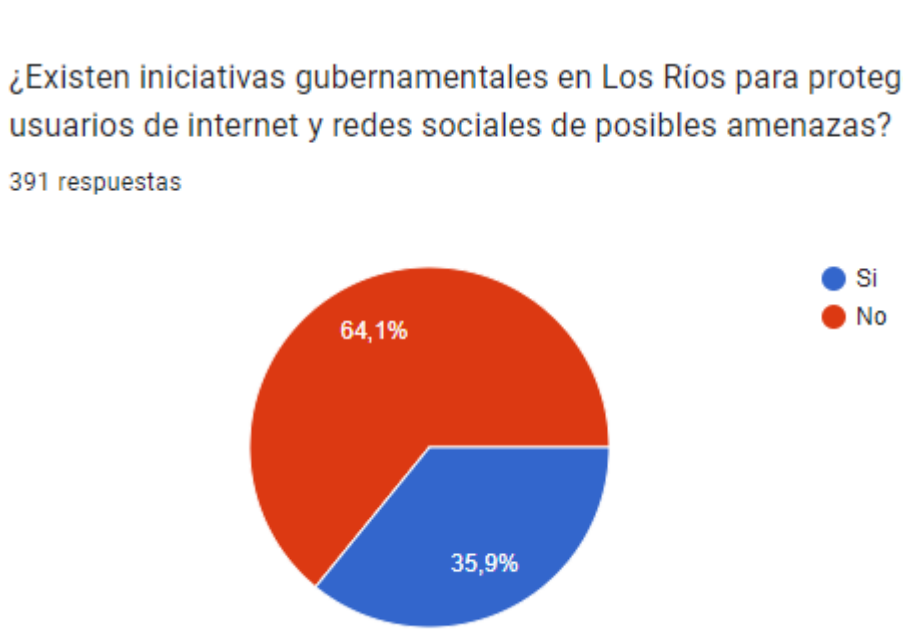


Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]

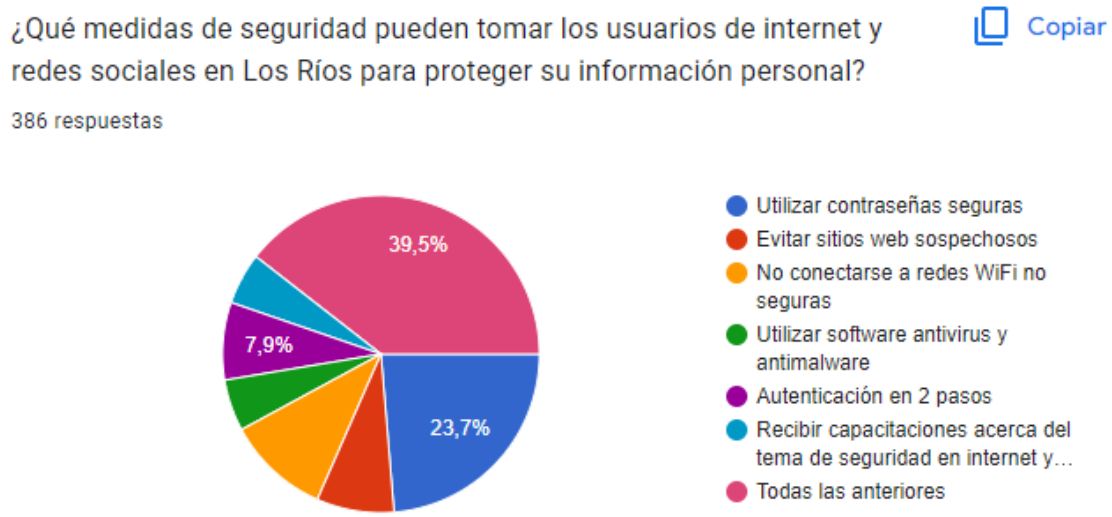


Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]

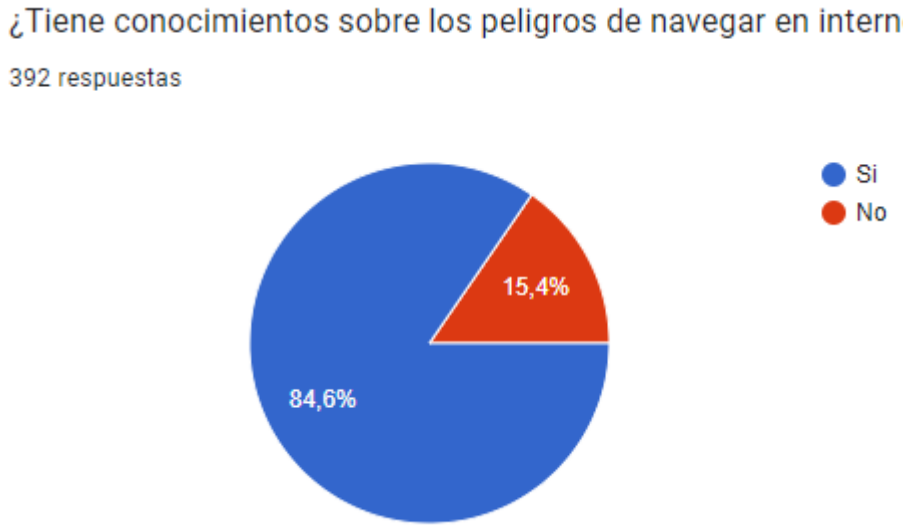
Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]



Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]



Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]



Beltrán, S. (2023) Encuesta realizada a ciudadanos de la provincia de Los Ríos. [Figura]

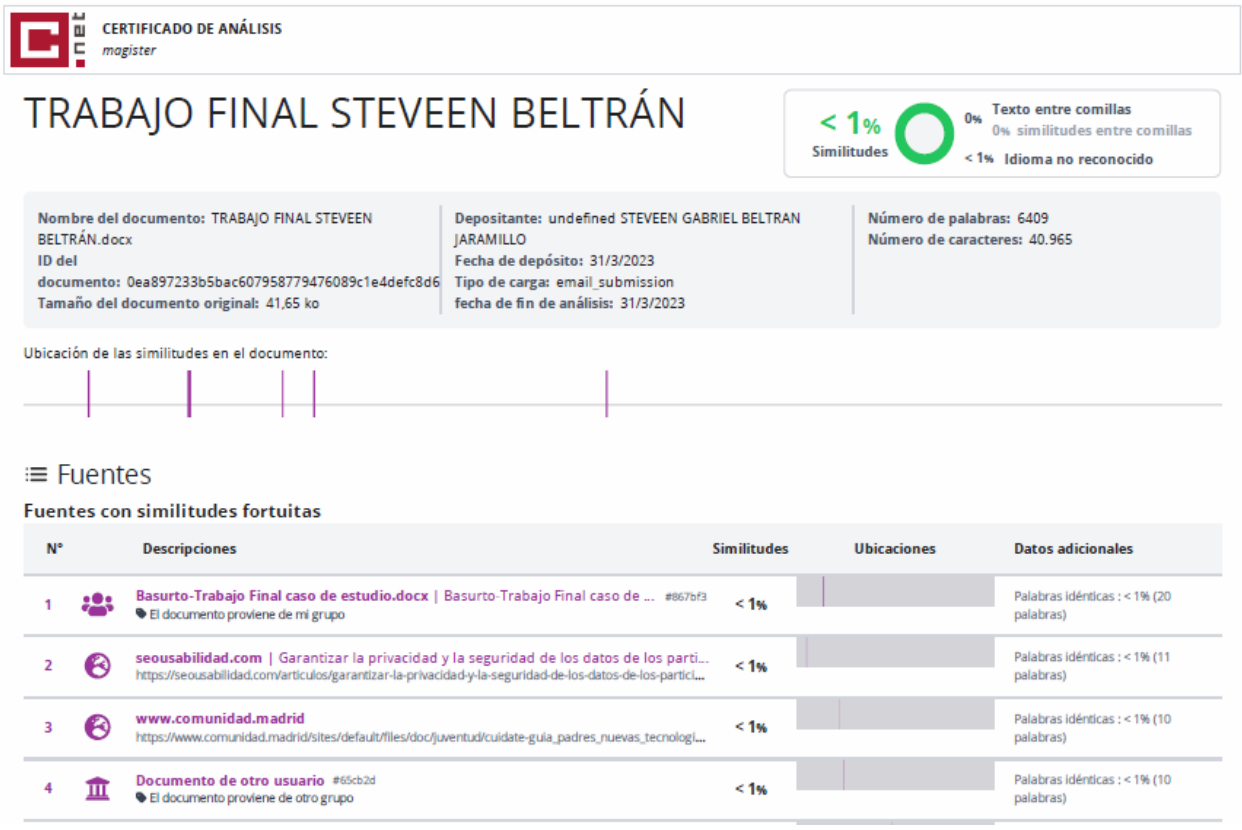
UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE SISTEMAS DE INFORMACIÒN

Babahoyo, 03 de Abril del 2023

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Estudio de Caso del estudiante: Beltrán Jaramillo Steveen Gabriel, cuyo tema es: **Análisis sobre los riesgos de seguridad informática en el internet y aplicaciones de redes sociales en adolescentes y menores de edad en la provincia de Los Ríos**, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio, obteniendo como porcentaje de similitud de **[1%]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.



CERTIFICADO DE ANÁLISIS
magister

TRABAJO FINAL STEVEEN BELTRÁN

< 1% Similitudes
0% Texto entre comillas
0% similitudes entre comillas
< 1% Idioma no reconocido

Nombre del documento: TRABAJO FINAL STEVEEN BELTRÁN.docx
ID del documento: 0ea897233b5bac607958779476089c1e4defc8d6
Tamaño del documento original: 41,65 ko

Depositante: undefined STEVEEN GABRIEL BELTRAN JARAMILLO
Fecha de depósito: 31/3/2023
Tipo de carga: email_submission
fecha de fin de análisis: 31/3/2023

Número de palabras: 6409
Número de caracteres: 40.965

Ubicación de las similitudes en el documento:

Fuentes

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Basurto-Trabajo Final caso de estudio.docx | Basurto-Trabajo Final caso de ... #867bf3 El documento proviene de mi grupo	< 1%		Palabras idénticas : < 1% (20 palabras)
2	seousabilidad.com | Garantizar la privacidad y la seguridad de los datos de los parti... https://seousabilidad.com/articulos/garantizar-la-privacidad-y-la-seguridad-de-los-datos-de-los-partici...	< 1%		Palabras idénticas : < 1% (11 palabras)
3	www.comunidad.madrid https://www.comunidad.madrid/sites/default/files/doc/juventud/cuidate-guia_padres_nuevas_tecnologi...	< 1%		Palabras idénticas : < 1% (10 palabras)
4	Documento de otro usuario #65cb2d El documento proviene de otro grupo	< 1%		Palabras idénticas : < 1% (10 palabras)

Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

_____
Ing. Wellington Isaac Maliza Cruz, Ph.D.
DOCENTE TUTOR

REFERENCIAS

Confianza, G. (01 de 05 de 2020). Obtenido de https://www.internetsociety.org/es/news/comunicados-de-prensa/2019/las-preocupaciones-sobre-la-privacidad-y-la-seguridad-contribuyen-a-que-los-consumidores-desconfien-de-los-productos-conectados/

Duggan. (20 de 08 de 2019). *Scielo*. Obtenido de https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1409-42582019000300339#:~:text=Entre%20los%20principales%20hallazgos%2C%20se,cibern%C3%A9tica%2C%20les%20hace%20m%C3%A1s%20vulnerables.

Et, K. (2019).

Etecé. (15 de 06 de 2021). Obtenido de https://concepto.de/riesgos-y-peligros-de-las-redes-sociales/

Etecé. (06 de 02 de 2023). Obtenido de https://concepto.de/riesgos-de-internet/

Evans, S. (17 de 09 de 2019). *ThinkBig*. Obtenido de https://blogthinkbig.com/como-protegerse-en-internet

Galán, C. (03 de 12 de 2021). *elcano*. Obtenido de https://www.realinstitutoelcano.org/analisis/las-campanas-de-desinformacion-y-la-responsabilidad-de-las-redes-y-plataformas-de-comunicacion-el-caso-de-telegram/

Interior, M. d. (14 de 09 de 2020). Obtenido de https://www.ministeriodelinterior.gob.ec/

Kaspersky. (10 de 02 de 2023). Obtenido de https://www.kaspersky.es/resource-center/preemptive-safety/protecting-wireless-networks

Kraus. (12 de 05 de 2019). *Scielo*. Obtenido de https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1409-42582019000300339#:~:text=Entre%20los%20principales%20hallazgos%2C%20se,cibern%C3%A9tica%2C%20les%20hace%20m%C3%A1s%20vulnerables.

Malckiff, J. (25 de 04 de 2021). Obtenido de https://www.is4k.es/necesitas-saber/privacidad

Moreno. (04 de 06 de 2021). *BBVA*. Obtenido de https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/riesgos-de-seguridad-y-privacidad-en-redes-sociales.html#:~:text=Algunos%20de%20los%20riesgos%20m%C3%A1s,con%20otros%20ni%C3%B1os%20o%20adolescentes).

NortonLife. (10 de 03 de 2021). Obtenido de https://blogs.funiber.org/tecnologias-informacion/2022/05/10/ciberdelito-que-es-y-como-se-previene

Paredes, R. (29 de 04 de 2021). Obtenido de https://www.rigobertoparedes.com/es/que-son-los-delitos-ciberneticos/

Rodriguez, R. (19 de 06 de 2021). *Psiquion*. Obtenido de https://www.psiquion.com/blog/adiccion-redes-sociales