



Universidad
Nacional
de Loja

Universidad Nacional de Loja

Facultad de la Educación, el Arte y la Comunicación

Carrera de Pedagogía de las ciencias experimentales Informática.

Diagnóstico de los riesgos del uso de internet de la guía del Ministerio de Educación del Ecuador para prevención de riesgos durante el uso de internet y dispositivos tecnológicos en el tercer año de bachillerato general unificado de la Unidad Educativa Fiscomisional La Inmaculada en el año lectivo 2022 – 2023.

Trabajo de Integración Curricular previo a la obtención del Título de Licenciado en Pedagogía de la Informática.

AUTOR:

Pablo Gabriel Vargas Barragán

DIRECTOR:

Lic. Gloria Cecibel Michay. Mg. Sc.

Loja – Ecuador

2024

Certificación

Loja, 06 de mayo de 2024

Lic. Gloria Cecibel Michay. Mg. Sc.

DIRECTORA DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICO:

Que he revisado y orientado el proceso de la elaboración del Trabajo de Integración Curricular denominado: **Diagnóstico de los riesgos del uso de internet de la guía del Ministerio de Educación del Ecuador para prevención de riesgos durante el uso de internet y dispositivos tecnológicos en el tercer año de bachillerato general unificado de la Unidad Educativa Fiscomisional La Inmaculada en el año lectivo 2022 – 2023.**, previo a la obtención del título de **Licenciado en Pedagogía de la Informática**, de autoría del estudiante **Pablo Gabriel Vargas Barragán**, con **cédula de identidad Nro. 1106081720**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.



Lic. Gloria Cecibel Michay. Mg. Sc.

DIRECTORA DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Autoría

Yo, **Pablo Gabriel Vargas Barragán**, declaro ser autor del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Integración Curricular en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma:



Cédula de Identidad: 1106081720

Fecha: 06 de mayo de 2024

Correo electrónico: pablo.g.vargas@unl.edu.ec

Teléfono: 0980522774

Carta de autorización por parte de la autora para la consulta de producción parcial o total y/o publicación electrónica de texto completo del Trabajo de Integración Curricular.

Yo, **Pablo Gabriel Vargas Barragán**, declaro ser autora del Trabajo de Integración Curricular denominado: **Diagnóstico de los riesgos del uso de internet de la guía del Ministerio de Educación del Ecuador para prevención de riesgos durante el uso de internet y dispositivos tecnológicos en el tercer año de bachillerato general unificado de la Unidad Educativa Fiscomisional La Inmaculada en el año lectivo 2022 – 2023.**, como requisito para optar el título de **Licenciado en Pedagogía de la Informática**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

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

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

Para constancia de esta autorización, suscribo, en la ciudad de Loja, a los seis días del mes de mayo del dos mil veinticuatro.

Firma:



Cédula de Identidad: 1106081720

Dirección: Av. Villonaco y Joaquín Gallegos Lara.

Correo electrónico: pablo.g.vargas@unl.edu.ec

Teléfono: 0980522774

DATOS COMPLEMENTARIOS:

Directora del Trabajo de Integración Curricular: Lic. Gloria Cecibel Michay. Mg. Sc.

Dedicatoria

Dedico la presente investigación a mi madre, fuente inagotable de amor y sabiduría, por ser mi guía en los momentos más difíciles y por animarme a nunca rendirme, su paciencia y aliento han sido fundamentales para alcanzar esta meta, y cada éxito que alcanzo es también suyo. A mi padre por enseñarme el valor del esfuerzo y la importancia del trabajo duro, sus consejos siempre han sido una luz que me ha iluminado el camino hacia mis metas. A mi querida familia, cada uno de ustedes ha contribuido de manera única en mi crecimiento personal y académico.

Pablo Gabriel Vargas Barragán.

Agradecimiento

Agradezco a todo el personal académico, directivo y administrativo de la Universidad Nacional de Loja, a todos quienes fueron mis docentes durante la carrera, en especial a la Ing. María de los Ángeles Coloma. Mg. Sc. y a mi estimada directora del trabajo de integración curricular Lic. Gloria Cecibel Michay. Mg. Sc. por sus invaluable contribuciones en mi trayectoria académica, cada una de ustedes ha dejado una huella indeleble en mi formación profesional.

A todos ellos gracias.

Pablo Gabriel Vargas Barragán.

Índice de contenidos

Portada	i
Certificación	ii
Autoría	iii
Carta de autorización	iv
Dedicatoria	v
Agradecimiento	vi
Índice de contenidos	vii
Índice de tablas:	viii
Índice de figuras:.....	ix
Índice de anexos:.....	x
1. Título	1
2. Resumen	2
Abstract	3
3. Introducción	4
4. Marco Teórico	5
4.1. Riesgos al usar internet.....	5
4.2. Herramienta para la prevención, identificación y conocimiento sobre los riesgos en el internet	15
5. Metodología	16
5.1. Área de estudio	16
6. Resultados	18
6.1. Resultados del objetivo 1.....	18
6.2. Resultados del objetivo 2.....	21
6.3. Resultados del objetivo 3.....	24
7. Discusión	51
8. Conclusiones	53
9. Recomendaciones	54
10. Bibliografía	55
11. Anexos	59

Índice de tablas:

Tabla 1. *Riesgos del uso de internet para jóvenes de bachillerato.*..... 19

Tabla 2. *Tabla de caracterización según la guía del ministerio de educación para prevención de riesgos durante el uso de internet y dispositivos tecnológicos.* 22

Tabla 3. *Rango de edades de los estudiantes.* 24

Índice de figuras:

Figura 1. <i>Ubicación de la Unidad Educativa Fiscomisional La Inmaculada.</i>	16
Figura 2. <i>Trata de personas.</i>	25
Figura 3. <i>Actividades de la trata de personas.</i>	26
Figura 4. <i>Flamming.</i>	27
Figura 5. <i>¿Reconoce usted las actividades del Flamming?</i>	28
Figura 6. <i>Grooming.</i>	29
Figura 7. <i>¿Reconoce cuando ocurre el Grooming?</i>	30
Figura 8. <i>Hacking.</i>	31
Figura 9. <i>¿Conoce usted sobre que trata el hacking?</i>	32
Figura 10. <i>Harassment.</i>	33
Figura 11. <i>¿Conoce usted sobre que trata el harassment?</i>	34
Figura 12. <i>Phishing.</i>	35
Figura 13. <i>¿Reconoce usted el Phishing?</i>	36
Figura 14. <i>Pornografía infantil.</i>	37
Figura 15. <i>¿Conoce usted que abarca la pornografía infantil?</i>	38
Figura 16. <i>Sexting.</i>	39
Figura 17. <i>¿Conoce usted sobre qué trata el Sexting?</i>	40
Figura 18. <i>Sextorsión.</i>	41
Figura 19. <i>Sextorsión.</i>	42
Figura 20. <i>Stalking.</i>	43
Figura 21. <i>¿La institución educativa ha proporcionado información acerca del Stalking?</i>	44
Figura 22. <i>Suplantación de identidad.</i>	45
Figura 23. <i>¿Conoce usted sobre qué trata la suplantación de identidad?</i>	46
Figura 24. <i>Delitos por medios digitales.</i>	47
Figura 25. <i>¿Conoce acerca de los delitos por medios digitales?</i>	48
Figura 26. <i>Lolicon/Shotacon.</i>	49
Figura 27. <i>¿Conoce acerca de que trata el Lolicon/Shotacon?</i>	50

Índice de anexos:

Anexo 1. *Solicitud a la Autoridad de la Institución Educativa.* 59

Anexo 2. *Validación del Instrumento.* 60

Anexo 3. *Instrumento.* 64

Anexo 4. *Certificación de traducción del resumen.* 72

1. Título

Diagnóstico de los riesgos del uso de internet de la guía del Ministerio de Educación del Ecuador para prevención de riesgos durante el uso de internet y dispositivos tecnológicos en el tercer año de bachillerato general unificado de la Unidad Educativa Fiscomisional La Inmaculada en el año lectivo 2022 – 2023.

2. Resumen

La presente investigación busca diagnosticar los riesgos del uso de internet de la guía del Ministerio de Educación del Ecuador para la prevención de riesgos durante el uso de internet y dispositivos tecnológicos en el tercer año de bachillerato general unificado de la Unidad Educativa Fiscomisional La Inmaculada en el año lectivo 2022 – 2023, para lo cual se elaboró y adaptó un cuestionario estructurado Ad hoc a partir de la guía para la prevención de riesgos durante el uso de internet y dispositivos tecnológicos del Ministerio de Educación de Ecuador (2020), distribuido por dimensiones, aplicado de forma presencial, mediante la técnica encuesta, cuyo medidor corresponde a la escala de frecuencia de Likert y preguntas dicotómicas de Si y No, los resultados arrojaron que la institución educativa ha brindado información de manera ocasional sobre: la trata de personas, grooming, pornografía infantil, sexting, stalking, suplantación de identidad y delitos por medios digitales, mientras que del flamming, hacking, harassment, phishing, sextorsión y lolicon/shotacon nunca han sido tratados. La metodología se realizó aplicando el método deductivo con un enfoque cuantitativo y un diseño de investigación de carácter exploratorio descriptivo, acorde al artículo 216 del Reglamento de Régimen Académico de la Universidad Nacional de Loja.

Palabras clave: *Riesgos en internet, Guía del ministerio de educación del Ecuador.*

Abstract

The present research seeks to diagnose the risks of internet use of the Ministry of Education of Ecuador guide for the prevention of risks during the use of internet and technological devices in the third year of unified general high school of the Fiscomisional Educational Unit La Inmaculada in the school year 2022 - 2023, for which an Ad hoc structured questionnaire was developed and adapted as of the guide for the prevention of risks during the use of internet and technological devices of the Ministry of Education of Ecuador (2020), distributed by dimensions, applied in person, through the survey technique, whose meter corresponds to the Likert frequency scale and dichotomous questions of Yes and No, the results showed that the educational institution has occasionally provided information on: human trafficking, grooming, child pornography, sexting, stalking, impersonation and digital media crimes, while flaming, hacking, harassment, phishing, sextortion and lolicon/shotacon have never been addressed. The methodology was carried out by applying the deductive method with a quantitative approach and a descriptive exploratory research design, according to article 216 of the Academic Regulations of the Loja National University.

Keywords: *Internet risks, Ministry of Education guide in Ecuador.*

3. Introducción

El rápido avance de la tecnología y el desarrollo informático en Ecuador han revolucionado la manera en que las personas se relacionan, proporcionando una amplia gama de oportunidades para conocer y difundir diversos tipos de contenidos. Sin embargo, este progreso también conlleva desafíos, como menciona Buenaño (2021), si bien es cierto que las TIC han sido participes del desarrollo económico, social, educativo e industrial del mundo también acarrea problemas que son perjudiciales para quienes no tienen ética digital y buscan sacar provecho de quienes tienen menos conocimiento de la utilidad de la información suministrada por medio de las redes sociales y el internet de manera general. Siendo los usuarios más jóvenes particularmente vulnerables a enfrentar dificultades en línea debido a su falta de experiencia y conocimiento sobre los riesgos asociados con el internet, tal y como menciona Esteras (2020), las TIC no están exentas de riesgos para los usuarios, y especialmente para los menores de edad. En este sentido, el Ministerio de Educación del Ecuador ha implementado estrategias para fortalecer el desarrollo de competencias digitales y pone a disposición de la comunidad educativa el portal El Mundo Virtual de Eugenia, como una campaña que inició en 2020 y busca brindar herramientas para la prevención, identificación y conocimiento sobre los riesgos en la internet, generar espacios de reflexión en la comunidad educativa en la prevención del mal uso de las tecnologías digitales, los riesgos y peligros a los que se exponen los niños, las niñas y los adolescentes en la navegación de plataformas digitales y uso de redes sociales (El mundo virtual de Eugenia, 2021, Recursos Educativos).

4. Marco Teórico

4.1. Riesgos al usar internet

Los riesgos al usar internet se refieren a las posibles amenazas, peligros y vulnerabilidades a los que los usuarios pueden estar expuestos mientras utilizan las tecnologías de la información y la comunicación (TIC), estos riesgos son variados, pueden afectar a los usuarios de diferentes formas, desde la exposición a contenido inapropiado, acoso o robo de identidad, acorde con Esteras (2020), señala que las TIC no están exentas de riesgos para los usuarios, y especialmente para los menores de edad, que pueden estar expuestos debido a la naturaleza de internet, estos riesgos se pueden clasificar en pasivos y activos, siendo los pasivos aquellos a los que se ven sometidos los menores involuntariamente por el hecho de navegar sin supervisión adulta, mientras que los activos engloban a aquellos derivados de comportamientos voluntarios que pueden resultar nocivos para ellos o para otros.

Por otra parte, Buenaño (2021), mencionó que si bien es cierto que las TIC han sido participes del desarrollo económico, social, educativo e industrial del mundo también acarrea problemas que son perjudiciales para quienes no tienen ética digital y buscan sacar provecho de quienes tienen menos conocimiento de la utilidad de la información suministrada por medio de las redes sociales y el internet de manera general.

En este sentido, el Ministerio de Educación del Ecuador implementa estrategias para fortalecer el desarrollo de competencias digitales y pone a disposición de la comunidad educativa: docentes, estudiantes, autoridades, madres y padres de familia, el portal El Mundo Virtual de Eugenia, en donde se presentan los siguientes riesgos al usar internet que se detallan a continuación.

4.1.1. Trata de personas

La trata de personas es una realidad alarmante y perturbadora, el Ministerio de Educación del Ecuador (2020), la define como la explotación violenta de seres humanos para el beneficio o lucro propio o de un tercero, mediante la manipulación, coerción y limitación de la libertad individual (p,13). Otras investigaciones realizadas por Dammert. et al., (2020), enfatizan que las situaciones de vulnerabilidad ocasionan que más personas sean involucradas en un proceso de explotación sea de tipo sexual, laboral o en forma de mendicidad, servidumbre, entre otras.

Siguiendo en la misma línea, el autor Meneses (2019), infiere que la trata de personas consiste en la captura, transporte, traslado, acogida o recepción de personas, recurriendo al uso de la fuerza u otras formas de coacción, rapto, fraude, engaño, abuso de poder o de una situación de vulnerabilidad, con el fin de realizarse recepciones de pagos y beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación, como la prostitución, servicios forzados, la esclavitud o la extracción de órganos.

El Ecuador como un Estado constitucional de derechos y justicia, establece esta práctica como un delito en su Código Orgánico Integral Penal (COIP) cuya última modificación fue en el año 2021, en donde el Artículo 91 manifiesta que: toda persona que capte, transporte, traslade, retenga o reciba personas; en el país, desde o hacia otros países con fines de explotación; para lo cual un tercero recurre a la amenaza, uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad, a la concesión o aceptación de pagos o beneficios, se constituye delito de trata de personas.

Por ende y como sanción a este delito según el Artículo 92 del COIP con pena privativa de libertad de trece a dieciséis años, con pena privativa de libertad de dieciséis a diecinueve años, si la infracción recae en personas de uno de los grupos de atención prioritaria o en situación de doble vulnerabilidad o si entre la víctima y el agresor ha existido relación afectiva, consensual de pareja, conyugal, convivencia, de familia o de dependencia económica o exista vínculo de autoridad civil, militar, educativa, religiosa o laboral, con pena privativa de libertad de diecinueve a veintidós años, si con ocasión de la trata de personas, la víctima ha sufrido enfermedades o daños psicológicos o físicos graves o de carácter irreversible, con pena privativa de libertad de veintidós a veintiséis años, si por motivo de la trata de personas se produce la muerte de la víctima.

Así también el artículo 174 del COIP estipula que la persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años.

4.1.2. Harassment

Harassment significa acoso en inglés, es un término utilizado para describir comportamientos no deseados, de acuerdo con lo que cita el Ministerio de educación del Ecuador

el harassment se entiende como la reproducción de amenazas, insultos, frases denigrantes y humillaciones mediante mensajes o llamadas, que incluye además la divulgación de fotos o rumores violentos en la red (p,14). Así mismo desde la posición de Neyra (2021), manifiesta que el harassment trata sobre ejercer hostigamiento por medio de las tecnologías de la información y la comunicación, principalmente el internet siendo esta modalidad la manera más común y frecuente de acoso, es una forma de violencia escolar que se gesta en línea, en el cual uno o varios agresores de manera intencionada acosan constantemente a una víctima con ataques repetitivos y constantes durante un tiempo indeterminado, para lo cual utilizan los recursos digitales como el chat, mensajería, correo electrónico, las redes sociales.

La autora mencionada en el párrafo anterior también señala que el harassment surge como un fenómeno derivado de la sociedad de la información y las tecnologías al tener una prevalencia en uso, sobre todo en los adolescentes y los jóvenes, ya que su mundo son las redes sociales y el ciberespacio, pero algunos aprovechan estos medios para incitar a la violencia y agresión o hacer uso de ella, por considerarse omnipotentes por el anonimato que le permite estas herramientas o aparatos electrónicos. De igual manera otros autores plantean el harassment como un conjunto de comportamientos constantes, reiterados y deliberados, que se realizan con el objetivo de agredir a iguales o coetáneos y que se llevan a cabo a través de medios electrónicos de comunicación como son las redes sociales o aplicaciones de mensajería instantánea que tienen la particularidad de la inmediatez y la amplia difusión (Munguía, et al. 2022).

Por su parte Recalde (2021), declara que el harassment es una manera de ciberacoso ya que consiste en el abuso e intimidación por medio de la tecnología como mensajes o publicaciones, no es una amenaza física, esto desemboca en efectos negativos a nivel psicológico para las víctimas; normalmente el harassment se da en menores de edad por su ingenuidad; este acoso puede llevar al suicidio a la persona; aunque esto afecte también a los que están la mayor parte del tiempo en redes sociales nadie está exento del harassment, algunas características son que: se genera en cualquier momento, es difícil de evadir, fácil de divulgar y los representantes son anónimos.

Para sancionar este tipo de acoso la Asamblea Nacional del Ecuador emitió en 2021 la Ley Orgánica Reformativa del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos, esta ley reforma el articulado del Código Penal a fin de tipificar delitos de violencia sexual cometidos a través de medios

digitales, donde agrega al Artículo 154 el COIP que expresa lo siguiente: La persona natural o jurídica que, por si misma o por tercero o a través de cualquier medio tecnológico o digital, moleste, perturbe o angustie de forma insistente o reiterada a otra, será sancionada con una pena privativa de libertad de seis meses a un año, siempre que el sujeto activo de la infracción busque cercanía con la víctima para poder causarle daño a su integridad física o sexual. Cuando la víctima sea menor de dieciocho años, o persona con discapacidad o cuando la persona no pueda comprender el significado del hecho o por cualquier causa no pueda resistirlo, será sancionado con pena privativa de libertad de uno a tres años.

4.1.3. Flamming

El flamming se refiere a un comportamiento agresivo en línea, de acuerdo con el Ministerio de Educación del Ecuador se lo define como una forma de ciberacoso a través de la utilización de un lenguaje intimidatorio, violento, vulgar o soez (p.14). En relación con lo mismo Lozada et al., (2016) como se citó en Orozco (2020), lo establece como la provocación mediante un mensaje enviado a foros o listas de correos, cuyo objetivo es generar reacciones llenas de furia por parte de los participantes, suele contener insultos u ofensas y puede estar dirigido a todos en general, a un grupo de usuarios o a alguien en particular.

Por otra parte, Fernández (2021), expresa que el flamming consiste en iniciar y alimentar discusiones y peleas en espacios virtuales donde confluyen varias personas, con el propósito de que tengan un impacto real en las relaciones físicas de los involucrados: una vez que se haya logrado el propósito, se retira del conflicto, permitiendo que otros sean vistos como los participantes principales. Este tipo de violencia está incluido en el Ecuador como un tipo de acoso que se sanciona igual que el harassment.

4.1.4. Grooming

Para el Ministerio de Educación del Ecuador (2020), el grooming ocurre cuando una persona adulta manipula a menores de edad con el fin de ganar su confianza y obtener videos o fotos de carácter sexual (p.14). Como lo hace notar Rosero (2022), el Grooming como ciberacoso sexual siempre lo perpetra un adulto contra un menor de edad, donde el acosador, utiliza las redes sociales para contactar y relacionarse con menores de edad, asumiendo una supuesta identidad de otro niño o adolescente, con propósitos sexuales que habitualmente se basan en pretender imágenes

o vídeos de la víctima. Indica que estas imágenes a veces son usadas por las redes de pornografía infantil, que pretenden envolver al menor en actividades sexuales reales.

Para Clajer (2019) citado por Rosero (2022), el Grooming es la conducta premeditada de un adulto, hombre o mujer, de acosar sexualmente a una niña, niño o adolescente utilizando medios virtuales que faciliten la interacción entre el acosador y el niño o adolescente, como por ejemplo las diferentes redes sociales, correo electrónico, mensajería de texto, sitios de juegos online o chats. Los adultos que practican el Grooming generalmente generan uno o diferentes perfiles falsos, haciéndose pasar por otro niño, o adolescente, persiguiendo la creación de una relación amistosa y de confianza con la víctima. Por su lado Fernández (2021), manifiesta que el grooming referencia a una situación de acoso hacia un menor, ejercida por una persona adulta, con fines sexuales.

Este delito se sanciona según el artículo 173 del COIP que indica que la persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que la propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años. La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.

4.1.5. Sexting

El Sexting según el Ministerio de Educación del Ecuador (2020), se da cuando una persona se toma fotos o se graba en videos, de índole sexual, y las comparte a través de teléfonos inteligentes, correos electrónicos, entre otros (p.14). Para Ressett (2019), el sexting es la creación e intercambio de mensajes de texto, videos, imágenes o fotos con contenido sexual personal usando las nuevas tecnologías de la información. Así mismo Orozco (2020), indica que la palabra sexting es un acrónimo en inglés formado por `sex´ (sexo) y `texting´ (escribir mensajes) también se le conoce como Sexteo, es un término que implica la recepción o transmisión de imágenes o videos que conllevan un contenido sexual a través de las redes sociales, ya sea con o sin autorización de quien los coloca en el medio.

Para Fernández (2021), consiste en la publicación o envío, a través de las TIC de contenido de carácter sexual de otra persona sin su consentimiento que, como consecuencia, produce una serie de peligros para la víctima tales como chantajes, amenazas a su privacidad y/o riesgos psicológicos, la autora también señala que se trata del envío de fotografías o videos de tipo sexual, producidos por el propio remitente, a segundas personas por medio de dispositivos móviles. Cuando un adulto realiza sexting con menores de edad se considerará como corrupción de niñas, niños y adolescentes y se sancionará según el Artículo 168 del COIP que expresa que la persona que permita el acceso o exposición de niñas, niños o adolescentes de forma intencionada a contenido nocivo sexualizado, violento o que llame a cometer actos de odio será sancionada con una pena privativa de uno a tres años.

4.1.6. Hacking

El Hacking según el Ministerio de Educación del Ecuador (2020), se trata de una intervención o alteración de sistemas informáticos, realizada con el objetivo de robar datos personales y/o financieros (p.14). Así mismo Sánchez (2019), manifiesta que consiste en acceder desde algún lugar del ciberespacio a un ordenador privado valiéndose de deficiencias en los sistemas de seguridad, aprovechando su vulnerabilidad u obteniendo contraseñas de acceso haciéndose pasar por usuarios legítimos.

Esta actividad es sancionada según el Artículo 232, que manifiesta que la persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseados, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de TIC, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionado con una pena privativa de libertad de tres a cinco años.

4.1.7. Phishing

El phishing es definido por el Ministerio de Educación del Ecuador (2020), como la difusión de mensajes falsos en internet, diseñados para usurpar o robar datos de cualquier tipo (p.15). Es una modalidad de estafa informática cuyo objeto principal es obtener del usuario, entre otros, datos, claves o números de cuentas bancarias con la finalidad de obtener un beneficio

económico ilícito utilizando para ello de forma fraudulenta y mediante engaño datos personales del usuario (García, 2018). Así también Herrera (2016), expresa que el phishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta. El objetivo del delito informático de Phishing es utilizar la clave de correo personal, referencia o cuenta de usuario y contraseña para realizar transferencias bancarias, retiros de efectivo, o compras por internet a nombre de la víctima.

El literal segundo del Artículo 230 del COIP sanciona esta actividad con pena privativa de libertad de tres a cinco años a la persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombre de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder.

4.1.8. Pornografía infantil

La pornografía infantil es definida por el Ministerio de Educación del Ecuador (2020), como cualquier representación o imagen de una niña o niño involucrados en actividades o situaciones de carácter sexual, reales o simuladas (p.15). Por pornografía infantil, Alarcón (2015), manifiesta que es toda representación visual de índole sexual, de menores de edad, con la finalidad de producirla, ofertarla, difundirla, adquirirla o poseerla por cualquier medio, la obtención de pornografía infantil a través del servicio web constituye un paso relativamente sencillo, en tanto basta únicamente localizar la ubicación en el ciberespacio de la página en cuestión, algo bastante simple ya que, si se desconoce, podría acudirse a cualquier buscador e introducir palabras clave relacionadas con la naturaleza del material, obteniendo de manera rápida la dirección necesaria para visualizar el contenido.

Este tipo de contenido es sancionado por la ley del Ecuador según el artículo 103 del COIP que indica que la persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños

o adolescentes en actitud sexual; será sancionado con pena privativa de libertad de trece a dieciséis años.

Asimismo, el artículo 104 del COIP manifiesta que la persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionado con pena privativa de libertad de diez a trece años.

4.1.9. Sextorsión

El Ministerio de Educación del Ecuador (2020), define a la sextorsión como una extorsión bajo la amenaza de publicar fotografías o videos sexuales de la víctima (p.15). Igualmente, los autores Cuentas y Echeverria (2022), expresan que se refiere al uso de las tecnologías digitales para chantajear a una víctima, generalmente amenazando con publicar imágenes íntimas de la víctima con el fin de obtener más fotos explícitas, videos, u obtener sexo de la víctima.

Por su parte Orosco y Pomasunco (2020), manifiestan que para que este tipo de ciberacoso pueda darse, es necesario la existencia de cierto tipo de material, bien sea imágenes o videos, de una persona determinada (la víctima) en actos o poses sexuales, bien sea desnuda(o) o semidesnuda(o), es una modalidad de ciberacoso en la que el acosador extorsiona a la víctima para conseguir algo a cambio de esta basado en el ultimátum de publicar imágenes íntimas comprometedoras que logró obtener bien por hackeo de las cuentas de redes sociales de la persona chantajeadada o porque la misma en una determinada oportunidad se las envió.

Según Rosero (2020), la sextorsión es conocida como chantaje online, es un tipo de extorsión en la cual se amenaza con publicar fotos o vídeos con contenido sexual si no se da cumplimiento a los requerimientos del ciberacosador. Esta forma de ciberacoso es sancionada con la ley según el Artículo 172.1 del COIP que expresa que la persona que, mediante el uso de violencia, amenazas o chantaje induzca, incite u obligue a otra a exhibir su cuerpo desnudo, semidesnudo, o en actitudes sexuales, con el propósito de obtener provecho personal o para un tercero, ya sea de carácter sexual o de cualquier otro tipo, será sancionado con pena privativa de libertad de tres a cinco años.

4.1.10. Stalking

El Ministerio de Educación del Ecuador (2020), manifiesta que el stalking implica un acoso reiterado y agresivo, ejercido con la finalidad de amedrentar, intimidar y atemorizar a la víctima (p.16). El autor Orozco (2020), expresa que supone una intromisión indeseada, obsesiva y persistente de una persona en la vida de otra, la víctima o target, que rechaza la relación con el sujeto que lleva a cabo los contactos, el acosador o stalker, a través de todo tipo de medios: llamadas telefónicas, mensajes de texto, e-mails o cartas; también intenta comunicarse con la víctima mediante el envío de regalos u otros materiales que pueden parecer amenazantes o causar miedo, o intentan acercarse a la víctima merodeando cerca de su casa, lugar de trabajo o frecuentando lugares a los que ésta acude en su tiempo libre, espiándolas.

A su vez Guzmán (2016), expresa que el stalking es el término usado para referirse a la perturbación que tiene una persona que lo lleva a espiar a su víctima, principalmente se da en redes sociales como Facebook, Instagram o Twitter, donde la mayoría de personas dejan su información disponible para cualquier persona, por medio del correo electrónico o por servicios de mensajería instantánea como WhatsApp, este delito se puede prevenir al saber hacer uso de las herramientas TIC ya que cada una de ellas permite realizar su perfil como público o privado.

Igualmente Rosero (2022), argumenta que la palabra stalking, es un término anglosajón, cuyo origen viene del verbo stalk que cuenta con un significado desde dos perspectivas: por una parte, caminar con furia, ira, de un modo amenazador por determinado lugar, por otra parte, se usa en la cacería para designar a la persona que se moviliza lo más cerca posible del animal, ocultándose para definitivamente atraparlo, desde este enfoque, se concibe al stalking como aquella conducta caracterizada por seguir deliberadamente y observar ilegalmente a una determinada persona por un determinado espacio de tiempo.

Esta forma de acosos es sancionada por el Artículo 178 del COIP donde dicta que la persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

4.1.11. Suplantación de identidad

Por suplantación de identidad El Ministerio de Educación del Ecuador (2020), la define como la apropiación y suplantación de la identidad de una persona por parte de otra, con el fin de acceder a recursos y beneficios económicos, jurídicos, entre otros (p.16). Por su parte el autor Vera (2019), indica que es aquella acción por la que una persona se hace pasar por otra en internet para llevar a cabo actividades de carácter ilegal, como pueden ser pedir un crédito o préstamo hipotecario, contratar nuevas líneas telefónicas o realizar ataques contra terceras personas. Este delito es sancionado según el Artículo 212 del COIP que indica que la persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para si o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años.

4.1.12. Delitos por medios digitales

Por delitos por medios digitales el Ministerio de Educación del Ecuador (2020), expresa que son las diferentes formas de apropiación y utilización de la imagen de una persona sin su consentimiento (p.16). Por su parte los autores Acosta et al., (2020), indica que son actos ilícitos cometidos mediante el uso inadecuado de la tecnología, atentando contra la privacidad de la información de terceras personas, dañando o extrayendo cualquier tipo de datos que se encuentren almacenados en servidores o gadgets.

La autora Paguay (2020), comenta que, en el caso de Ecuador, en los últimos años, estos delitos por medios digitales no eran muy comunes, pero con el aumento del acceso al internet de las personas, estos se iban incrementando. En la actualidad, es muy común hablar de delitos informáticos, por cuanto son miles las personas que han sido víctimas de estas infracciones, de manera especial cuando se efectúan compras de bienes y servicios a través del internet. Para la sancionar y tipificar este tipo de delitos cometidos a través de medios digitales, la asamblea del Ecuador en el año 2021, aprobó la Ley Orgánica Reformatoria del Código Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la lucha contra los Delitos Informáticos.

4.1.13. Lolicon/Shotacon

El Ministerio de Educación del Ecuador (2020), define al Lolicon/Shotacon como un tipo de producción ilustrada/animada en formato manga o anime en la que los niños son representados

en relaciones implícita o explícitamente sexuales con adultos (p.16). La autora Aguilera (2019,) manifiesta que el término “Lolicon” hace referencia a niñas menores de 12 años, excesivamente lindas e inocentes que tanto estéticamente como de personalidad suelen ser niñas débiles y adorables.

Este tipo de contenido, aunque ilustrado cae en la categoría de pornografía infantil siendo sancionado por la ley en el artículo 103 del COIP que expresa que la persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionado con pena privativa de libertad de trece a dieciséis años.

Al igual que el artículo 104 del COIP que manifiesta que la persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionado con pena privativa de libertad de diez a trece años.

4.2. Herramienta para la prevención, identificación y conocimiento sobre los riesgos en el internet

4.2.1. El mundo virtual de Eugeni

El mundo virtual de Eugenia es una campaña por parte del Ministerio de Educación que inició en 2020 y busca brindar herramientas para la prevención, identificación y conocimiento sobre los riesgos en la internet, generar espacios de reflexión en la comunidad educativa en la prevención del mal uso de las tecnologías digitales, los riesgos y peligros a los que se exponen los niños, las niñas y los adolescentes en la navegación de plataformas digitales y uso de redes sociales; así como desarrollo competencias digitales en miembros de la comunidad educativa, trabajando con recomendaciones y estrategias para el conocimiento, la identificación y el cuidado de la integridad de los más pequeños. (El mundo virtual de Eugenia, 2021, Recursos Educativos).

5. Metodología

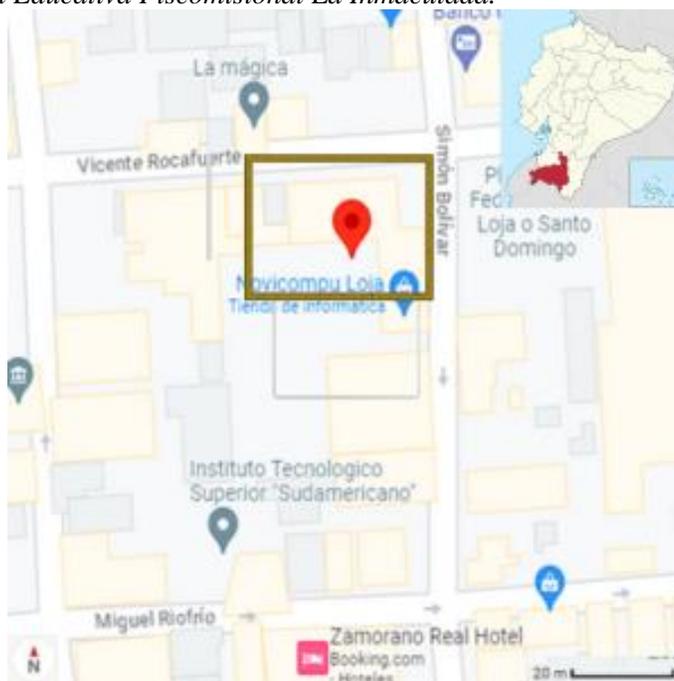
Según el Artículo 216 del reglamento de régimen académico de la Universidad Nacional de Loja manifiesta que el trabajo de integración curricular, es un tipo de investigación exploratorio, descriptivo, con la finalidad de validar los conocimientos y capacidades del perfil de egreso de la carrera, aportará la definición, explicación y resolución de los problemas prioritarios para el desarrollo social, científico y tecnológico, e incorporará a su futuro ejercicio profesional los aportes científicos, tecnológicos y saberes ancestrales. Para el desarrollo del presente proyecto de investigación se utilizó el método deductivo, con un enfoque cuantitativo de alcance exploratorio descriptivo, con un estudio transversal.

5.1. Área de estudio

El proyecto de investigación se realizó en la Unidad Educativa Fiscomisional La Inmaculada, que se encuentra ubicada en las calles Bolívar y Vicente Rocafuerte, de la parroquia el Sagrario del cantón Loja, provincia de Loja, de la zona Urbana, código AMIE 11H00011.

Figura 1.

Ubicación de la Unidad Educativa Fiscomisional La Inmaculada.



Nota. La figura muestra el área de estudio. Fuente Google (s.f.).

La población del estudio fueron todas las estudiantes de la Unidad Educativa La Inmaculada, donde se tomó como muestra los cuatro paralelos de tercer año de bachillerato general unificado de la Unidad Educativa Fiscomisional La Inmaculada, sumando un total de 112 estudiantes de género femenino. Para recabar la información se utilizó la técnica de la encuesta, con un instrumento del tipo cuestionario.

Para poder dar cumplimiento con los objetivos planteados por el proyecto de investigación se han desarrollado las siguientes actividades de acuerdo a los objetivos específicos: Definir los riesgos del uso de internet para los jóvenes del tercer año general unificado, se realizó búsquedas bibliográficas en los diferentes repositorios digitales de universidades, base de datos indexadas, Scopus, entre otros, que se plasmó en una figura donde se definen en los resultados.

Para el segundo objetivo específico que trato sobre *Identificar los riesgos del uso del internet para los jóvenes del tercer año del bachillerato general unificado de la guía del Ministerio de Educación del Ecuador, para prevención de riesgos durante el uso de internet y dispositivos tecnológicos*, se hizo una descripción de los riesgos del uso del internet para los jóvenes del tercer año del bachillerato general unificado a partir de la guía del Ministerio de Educación del Ecuador, para prevención de riesgos durante el uso de internet y dispositivos tecnológicos, que se la encuentra como la Tabla 1 en los resultados.

Para el tercer objetivo específico que va sobre *Diagnosticar los riesgos del uso de internet en el tercer año de bachillerato general unificado en la Unidad Educativa Fiscomisional La Inmaculada en el año lectivo 2022 – 2023*, se elaboró y adapto un cuestionario Ad hoc a partir de la Guía para Prevención de Riesgos durante el uso de internet y dispositivos tecnológicos del Ministerio de Educación del Ecuador, para la validación de este instrumento se realizó una prueba piloto, a dos expertos del tema. Una vez aprobado, se procedió aplicar el instrumento de forma presencial a las estudiantes del tercer año de bachillerato general unificado en la Unidad Educativa Fiscomisional La Inmaculada de forma presencial.

Una vez recopilada toda la información se tabuló los datos utilizando las hojas de cálculo del programa Excel y se analizó la información haciendo uso de la estadística descriptiva.

6. Resultados

Los Resultados de los tres objetivos planteados en esta investigación se dan a conocer a continuación:

6.1. Resultados del objetivo 1

De acuerdo al objetivo número 1, denominado: *Definir los riesgos del uso de internet para los jóvenes del tercer año de bachillerato general unificado*, para dar cumplimiento a la siguiente investigación de acuerdo al objetivo 1 se hicieron búsquedas en repositorios digitales para indagar los riesgos de internet que se representaron en una tabla de caracterización la cual permitió ordenar ideas y conceptos sobre los riesgos al usar el internet, lo que se detalla en la tabla 1.

Tabla 1.*Riesgos del uso de internet para jóvenes de bachillerato.*

Riesgos del uso de internet	Definición
Trata de personas.	Captura de personas recurriendo al uso de la fuerza u otras formas de coacción con fines de explotación, como la prostitución, la esclavitud o la extracción de órganos, (Meneses 2019).
Harassment.	Hostigamiento por medio de las TIC, principalmente internet, (Neyra 2021).
Grooming.	Es un tipo de chantaje online en el cual se amenaza con publicar fotos o vídeos con contenido sexual si no se da cumplimiento a los requerimientos del ciberacosador, (Rosero 2020).
Sextorsión.	Se refiere al uso de las tecnologías digitales para chantajear a una víctima, generalmente amenazando con publicar imágenes íntimas de la víctima con el fin de obtener más fotos explícitas, videos, u obtener sexo de la víctima (Cuentas y Echeverria, 2022).
Suplantación de identidad.	Aquella acción por la que una persona se hace pasar por otra en internet para llevar a cabo actividades de carácter ilegal, como un crédito o préstamo hipotecario, contratar nuevas líneas telefónicas o realizar ataques contra terceras personas, (Vera, 2019).
Doxing.	Publicación de información privada de la víctima; es una violación de la privacidad de la persona, (Cuentas y Echeverria, 2022).
Ciberadicción.	Patrón de comportamiento que se caracteriza por la pérdida de control sobre el uso de Internet, la cual puede conducir al aislamiento y al descuido de las relaciones sociales, las actividades académicas y recreativas, la salud y la higiene personal entre otros (Tsitsika, et al., 2012, citado por Esteras, 2020).

(Continúa)

(Continuación)

Stalking.	Cuando un acosador espía a su víctima, principalmente en redes sociales como Facebook, Instagram o Twitter, donde la mayoría de personas dejan su información disponible para cualquiera, (Guzmán, 2016).
Ciberacoso inmobiliario.	Comportamiento reiterado para obstaculizar el derecho al disfrute de la vivienda al propietario de la misma o en su defecto el inquilino, se realiza a través de internet, (Rosero, 2022).
Ciberacoso de género.	Conocido como ciberviolencia de género, caracterizándose por maltrato psicológico a través de las redes sociales u otro entorno virtual de comunicación sobre una determinada persona basado en su orientación sexual, (Rosero, 2022).
Cybermobbing.	Modalidad de acoso laboral a través de medios virtuales, como las redes sociales o por los chats institucionales, ejercido habitualmente entre compañeros de trabajo, personal supervisor hacia subordinados o igualmente personal subordinado a sus supervisores, su fin es que la víctima renuncie a su cargo, (Rosero, 2022).
Fraping.	Ciberacoso en el que el acosador logra o bien hackear las cuentas de la víctima para controlar sus redes sociales y asumir su identidad publicando contenido personal, con la finalidad de obtener algo a cambio de devolver el control de las redes (Rosero, 2022).
Porno venganza.	Surge cuando se difunde de forma pública información íntima con materiales determinados y sin consentimiento. (Cuentas y Echeverría, 2022).
Acceso a contenidos inadecuados.	El uso de internet pone a menores de edad en contacto de forma potencial con contenidos de todo tipo: chats, aplicaciones, videos, información, que no son siempre adecuados para su edad y desarrollo psicosocial y afectivo-emocional (Esteras, 2020).

Nota. Datos obtenidos de búsquedas bibliográficas en los diferentes repositorios digitales de universidades, base de datos indexadas, Scopus, entre otros.

Como se pudo evidenciar dentro de la tabla 1 se plasman catorce riesgos del uso de internet que pueden sufrir los estudiantes de tercer año del Bachillerato General Unificado, los mismos que se adaptaron de la guía del ministerio y de varios autores recopilados de la revisión bibliográfica.

6.2. Resultados del objetivo 2

En relación al objetivo número 2 de la investigación denominado: *Identificar los riesgos del uso del internet para los jóvenes del tercer año del bachillerato general unificado de la guía del Ministerio de Educación del Ecuador, para prevención de riesgos durante el uso de internet y dispositivos tecnológicos*, para dar cumplimiento al objetivo antes mencionado se hizo una tabla de caracterización basado en la guía emitida por el Ministerio de Educación del Ecuador (2020), denominada Guía para Prevención de Riesgos durante el uso de internet y dispositivos tecnológicos. En donde se han podido recopilar los siguientes riesgos de internet que se muestran en la tabla 2.

Tabla 2.

Tabla de caracterización según la guía del ministerio de educación para prevención de riesgos durante el uso de internet y dispositivos tecnológicos.

Riesgos de internet	Descripción	Sanciones
Trata de personas.	Explotación violenta de seres humanos, mediante la manipulación, coerción y limitación de la libertad individual. (Ministerio de Educación del Ecuador, 2020, p,13).	Artículo 92 del COIP: Pena privativa de libertad de trece a dieciséis años.
Harassment.	Reproducción de amenazas, insultos y humillaciones además de la divulgación de fotos o rumores violentos en la red. (Ministerio de Educación del Ecuador, 2020, p,14).	Artículo 154 el COIP: Pena privativa de libertad cuando la víctima sea menor de dieciocho años de uno a tres años.
Flamming.	Forma de ciberacoso a través de la utilización de un lenguaje intimidatorio, violento, vulgar o soez, (Ministerio de Educación del Ecuador, 2020, p,14).	Artículo 154 el COIP: Pena privativa de libertad cuando la víctima sea menor de dieciocho años será sancionado con pena privativa de libertad de uno a tres años.
Grooming.	Ocurre cuando una persona adulta manipula a menores de edad con el fin de ganar su confianza y obtener videos o fotos de carácter sexual. (Ministerio de Educación del Ecuador, 2020, p,14).	Artículo 173 del COIP: Pena privativa de libertad de tres a cinco años.
Sexting.	Cuando una persona se toma fotos o se graba en videos, de índole sexual, y las comparte a través de teléfonos inteligentes, correos electrónicos, entre otros, (Ministerio de Educación del Ecuador, 2020, p,14).	Artículo 168 del COIP: Pena privativa de uno a tres años.
Hacking.	Se trata de una intervención o alteración de sistemas informáticos, realizada con el objetivo de robar datos personales y/o financieros, (Ministerio de Educación del Ecuador, 2020, p,14).	Artículo 232 del COIP: pena privativa de libertad de tres a cinco años.
Phishing.	Difusión de mensajes falsos en internet, diseñados para usurpar o robar datos de cualquier tipo, (Ministerio de Educación del Ecuador, 2020, p,15).	Artículo 230 del COIP: pena privativa de libertad de tres a cinco años.

(Continúa)

(Continuación)

Riesgos de internet	Descripción	Sanciones
Pornografía infantil.	Cualquier representación o imagen de una niña o niño involucrados en actividades o situaciones de carácter sexual, reales o simuladas, (Ministerio de Educación del Ecuador, 2020, p,15).	Artículo 103 del COIP: Pena privativa de libertad de trece a dieciséis años a la persona que produzca este contenido. Artículo 104 del COIP: Pena privativa de libertad de diez a trece años a la persona que almacene este contenido.
Sextorsión.	Una extorsión bajo la amenaza de publicar fotografías o videos sexuales de la víctima, (Ministerio de Educación del Ecuador, 2020, p,15).	Artículo 172.1 del COIP: Pena privativa de libertad de tres a cinco años.
Stalking.	Acoso reiterado y agresivo, ejercido con la finalidad de amedrentar, intimidar y atemorizar a la víctima, (Ministerio de Educación del Ecuador, 2020, p,16).	Artículo 178 del COIP: Pena privativa de libertad de uno a tres años.
Suplantación de identidad.	Apropiación y suplantación de la identidad de una persona por parte de otra, con el fin de acceder a recursos y beneficios económicos, jurídicos, entre otros, (Ministerio de Educación del Ecuador, 2020, p,16).	Artículo 212 del COIP: Pena privativa de libertad de uno a tres años.
Delitos por medios digitales.	Las diferentes formas de apropiación y utilización de la imagen de una persona sin su consentimiento, (Ministerio de Educación del Ecuador, 2020, p,16).	Los delitos cometidos a través de medios digitales, se sancionan según su tipo a través de la LOEI en su reforma para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la lucha contra los Delitos Informáticos.
Lolicon/Shotacon.	Producción ilustrada/animada en formato manga o anime en la que los niños son representados en relaciones implícita o explícitamente sexuales con adultos, (Ministerio de Educación del Ecuador, 2020, p,16).	Artículo 104 del COIP: Pena privativa de libertad de diez a trece años. (aquí puede existir un vacío legal al ser contenido ilustrado, investigar mejor.)

Nota. Datos obtenidos de acuerdo a la investigación bibliográfica que se realizó a partir de la guía del Ministerio de Educación del Ecuador, y el COIP.

Como se pudo evidenciar dentro de la tabla de caracterización 2, se plasman trece riesgos del uso de internet que pueden sufrir los estudiantes de tercer año del Bachillerato General Unificado, los mismos que se adaptaron de la guía del Ministerio de Educación del Ecuador.

6.3. Resultados del objetivo 3

Para dar cumplimiento al objetivo específico 3: *Diagnosticar los riesgos del uso de internet en el tercer año de bachillerato general unificado en la Unidad Educativa Fiscomisional La Inmaculada en el año lectivo 2022 – 2023*; se elaboró y adaptó un cuestionario estructurado Ad hoc en dos secciones a partir de la Guía del Ministerio de Educación del Ecuador, para la Prevención de riesgos durante el Uso de Internet y Dispositivos Tecnológicos, mismo que fue aplicado de forma presencial a los estudiantes de tercer año de bachillerato general unificado en la Unidad Educativa Fiscomisional La Inmaculada, una vez recolectada la información se procedió a tabular y analizar la misma, haciendo uso de la estadística descriptiva.

En la primera sección del instrumento se recolectó datos informativos de los estudiantes de tercer año de Bachillerato General Unificado de la Unidad Educativa Fiscomisional La Inmaculada, en relación a los años que tienen los estudiantes divididos en dos rangos como se muestra en la tabla 2.

Tabla 3.

Rango de edades de los estudiantes.

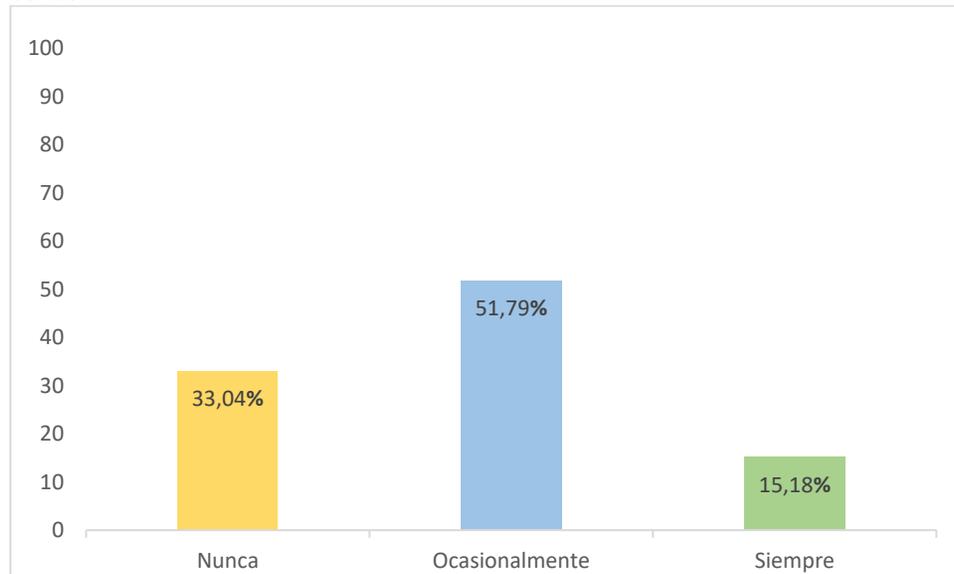
Edad	F	%
16 – 18	112	100
20 o mas	0	0
Total:	112	100

Nota. Datos obtenidos a partir de la encuesta aplicada a los estudiantes de Tercer año de Bachillerato General Unificado.

Como se puede evidenciar en la tabla 2 en relación al rango de edades que poseen las estudiantes que se han considerado para la investigación el 100% se encuentra en el rango de edades de 16 a 18 años. En la segunda sección del instrumento aplicado se evidenciaron 13 dimensiones de acuerdo a los riesgos por el uso del internet de acuerdo a la Guía del Ministerio de Educación del Ecuador (2020), en donde los resultados son los siguientes.

Para la dimensión 1 denominada Trata de personas se ha ubicado dos tipos de preguntas, la primera mediante la escala de Likert, así como también preguntas dicotómicas, como se muestra en la figura 2.

Figura 2.
Trata de personas.



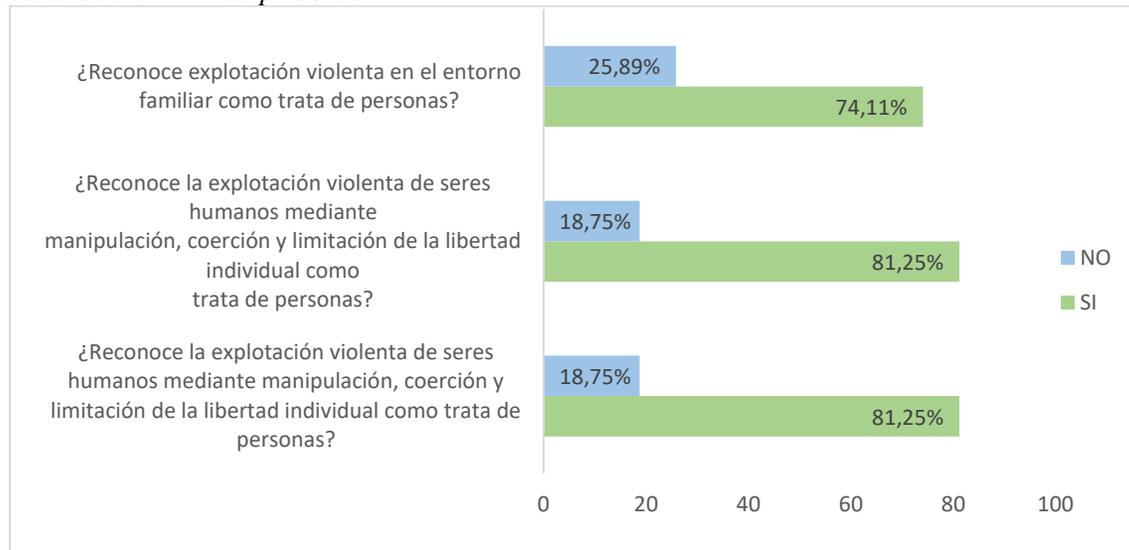
Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 2, correspondiente a la pregunta: *¿La institución educativa le ha brindado información acerca de la trata de personas?*, las respuestas indica que en el rango de Ocasionalmente tiene un porcentaje del 51.79%, así mismo en el rango de Nunca con un valor de 33.04% y finalmente en el rango de Siempre con un valor del 15.18%.

Así mismo se indican los resultados de las preguntas dicotómicas en relación con la dimensión 1 de las actividades de la trata de personas las cuales se grafican en la figura 3.

Figura 3.

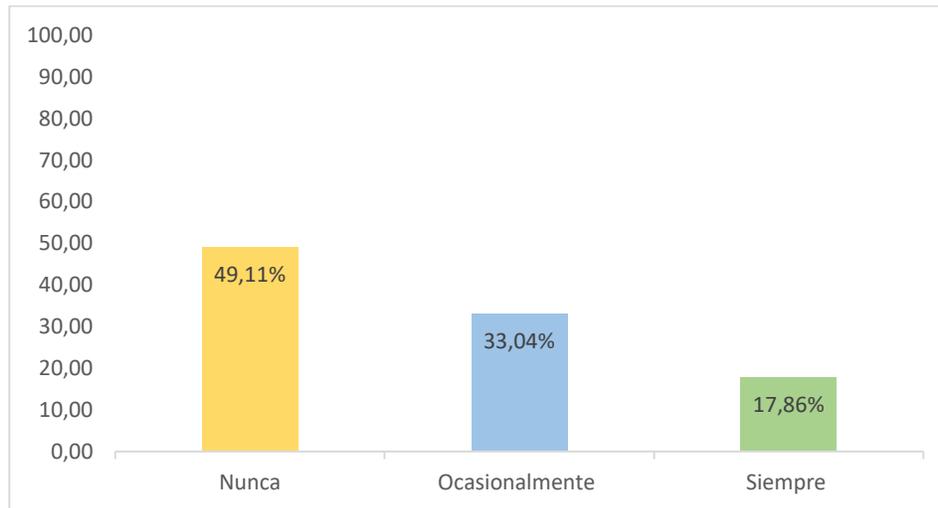
Actividades de la trata de personas.



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo a los resultados que se evidencian en la figura 3, se puede describir respecto a si *¿Reconoce la explotación violenta de seres humanos con fines de lucro, ya sea para beneficio propio o de terceros, como un caso de trata de personas?*, la respuesta Si, tiene un valor del 74, 11%, y la opción No representa el 25,89%: así mismo para las siguientes interrogantes denominadas: *¿Reconoce la explotación violenta de seres humanos mediante manipulación, coerción y limitación de la libertad individual como trata de personas?* Y *¿Reconoce explotación violenta en el entorno familiar como trata de personas?*, los resultados muestran de manera igualitaria un 81,25% a la opción Si y el No con el 18, 75%.

Figura 4.
Flamming.



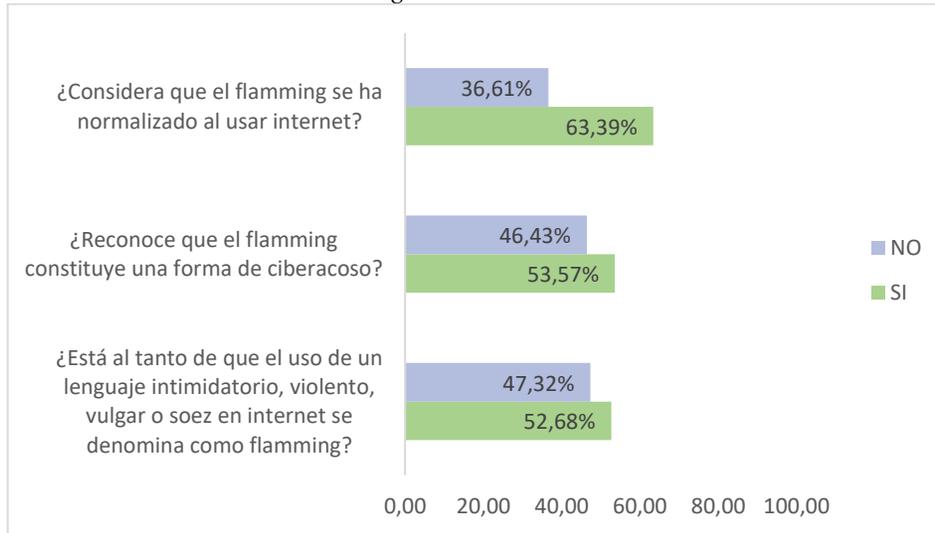
Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 4, correspondiente a la pregunta: *¿La institución educativa ha brindado información acerca del fenómeno flaming?*, las respuestas indica que en el rango de Nunca tiene un porcentaje del 49.11%, así mismo en el rango de Ocasionalmente con un valor de 33.04% y finalmente en el rango de Siempre con un valor del 17.86%.

Así mismo se indican los resultados de las preguntas dicotómicas en relación con la dimensión 2 de las actividades del flaming las cuales se grafican en la figura 5.

Figura 5.

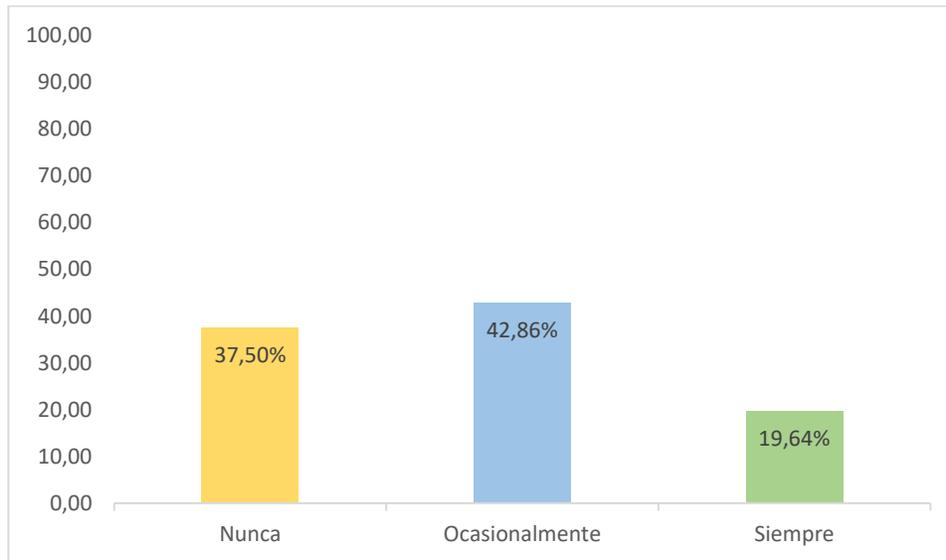
¿Reconoce usted las actividades del Flaming?



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo a los resultados que se evidencian en la figura 5, se puede reseñar respecto a si *¿Considera que el flaming se ha normalizado al usar internet?* Respondieron Si el 63.39% y No el 36.61%, así también para la pregunta *¿Reconoce que el flaming constituye una forma de ciberacoso?* Respondieron Si el 53.57% y No el 46.43% restante y para la pregunta *¿Está al tanto de que el uso de un lenguaje intimidatorio, violento, vulgar o soez en internet se denomina como flaming?* La respuesta Si cuenta con un 52.68% y el No el 47.32% restante.

Figura 6.
Grooming.



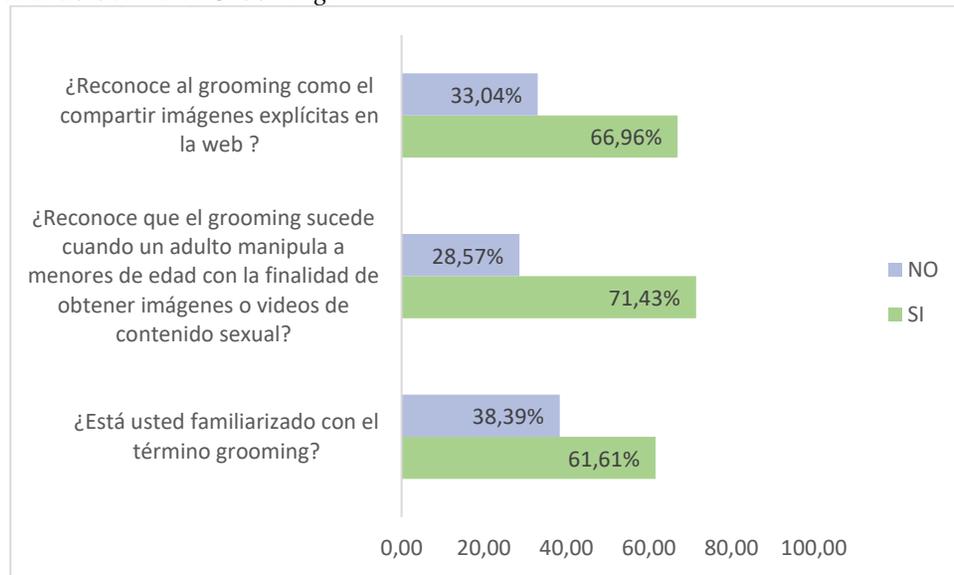
Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 6, correspondiente a la pregunta: *¿La institución educativa ha proporcionado información sobre el grooming?*, las respuestas indica que en el rango de Ocasionalmente tiene un porcentaje del 42.86%, así mismo en el rango de Nunca con un valor de 37.50% y finalmente en el rango de Siempre con un valor del 19.64%.

Así mismo se indican los resultados de las preguntas dicotómicas en relación con la dimensión 3 de las actividades del grooming las cuales se grafican en la figura 7.

Figura 7.

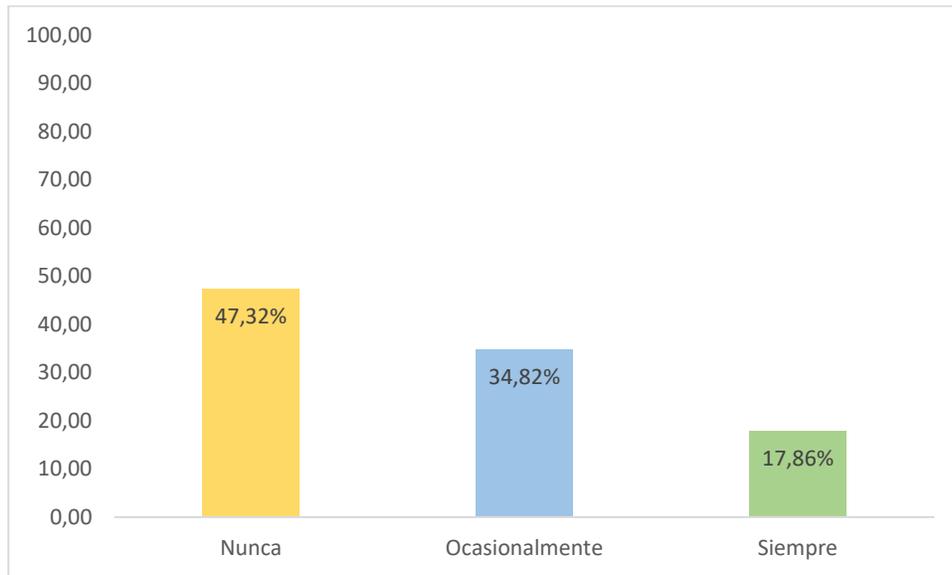
¿Reconoce cuando ocurre el Grooming?



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo a los resultados que se evidencian en la figura 7, se puede describir respecto a si *¿Reconoce al grooming como el compartir imágenes explícitas en la web?* El 33.04% respondió que No, mientras que el 66.96% contestó que Si, por su parte para la pregunta: *¿Reconoce que el grooming sucede cuando un adulto manipula a menores de edad con la finalidad de obtener imágenes o videos de contenido sexual?* El porcentaje de personas que respondieron No es del 28.57% y del Si 71.43%, y por último la pregunta: *¿Está usted familiarizado con el término grooming?* El 38.39% de los encuestados contestaron que No, mientras que el porcentaje de quienes contestaron Si fue del 61.61%.

Figura 8.
Hacking.



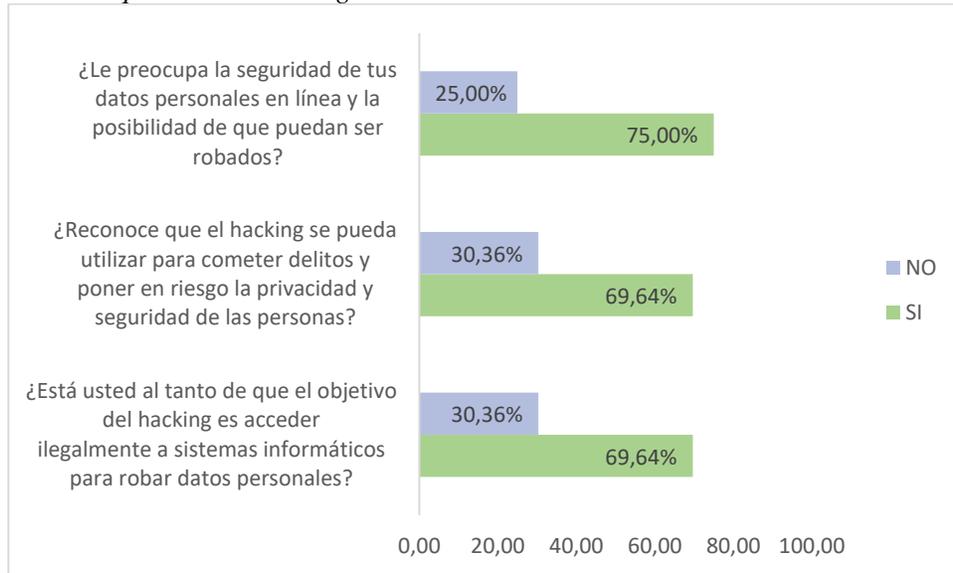
Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 8, correspondiente a la pregunta: *¿La institución educativa ha brindado información acerca del hacking?*, las respuestas indica que en la escala de Nunca tiene un porcentaje del 47.32%, así mismo en el rango de Ocasionalmente cuenta con un valor de 34.82% y finalmente en el rango de Siempre con un valor del 17.86%.

Así mismo se indican los resultados de las preguntas dicotómicas en relación con la dimensión 4 de las actividades del hacking las cuales se grafican en la figura 9.

Figura 9.

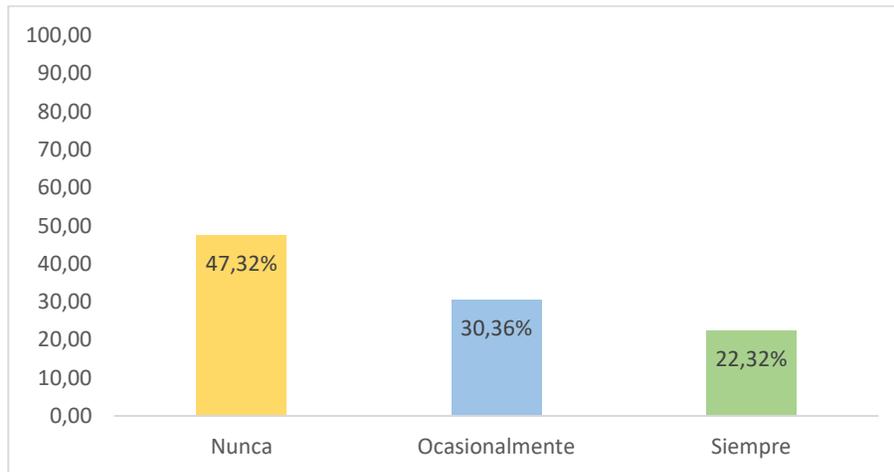
¿Conoce usted sobre que trata el hacking?



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo a los resultados que se evidencian en la figura 9, se puede describir respecto a si *¿Le preocupa la seguridad de tus datos personales en línea y la posibilidad de que puedan ser robados?*, la respuesta No fue marcada por el 75.00% y el Si cuenta con el 25.00% restante, para las preguntas *¿Reconoce que el hacking se pueda utilizar para cometer delitos y poner en riesgo la privacidad y seguridad de las personas?* Y *¿Está usted al tanto de que el objetivo del hacking es acceder ilegalmente a sistemas informáticos para robar datos personales?* El 69.64% de los encuestados respondieron que Si y el 30.36% restante No en ambas preguntas.

Figura 10.
Harassment.



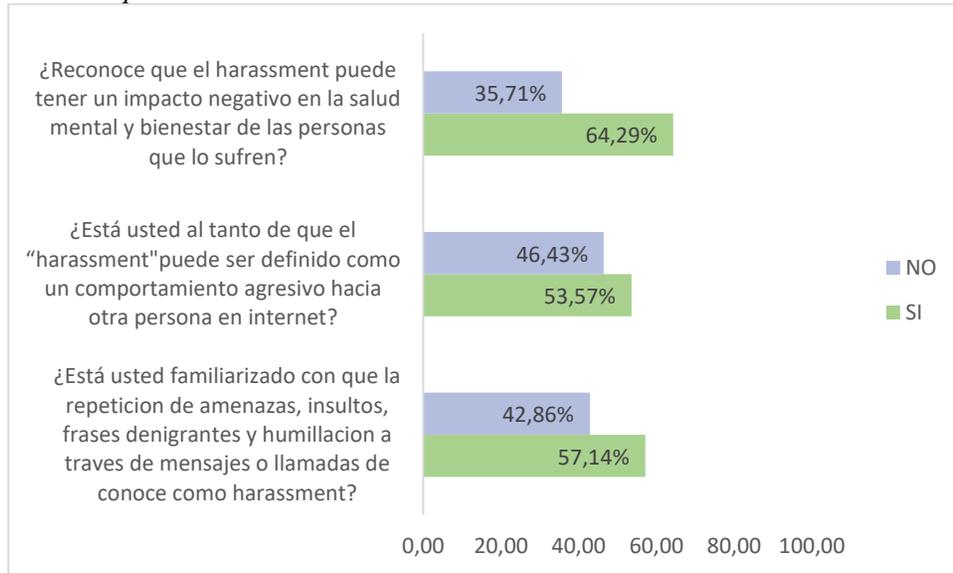
Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 10, correspondiente a la pregunta: ¿La institución educativa ha brindado información acerca del Harassment?, las respuestas indican que en la escala de Nunca tiene un porcentaje de 47.32%, Ocasionalmente 30.36% y finalmente Siempre el 22.32% restante.

Así mismo se indican los resultados de las preguntas dicotómicas en relación a la dimensión 6: ¿Conoce usted sobre que trata el harassment? Las cuales se grafican en la figura 11.

Figura 11.

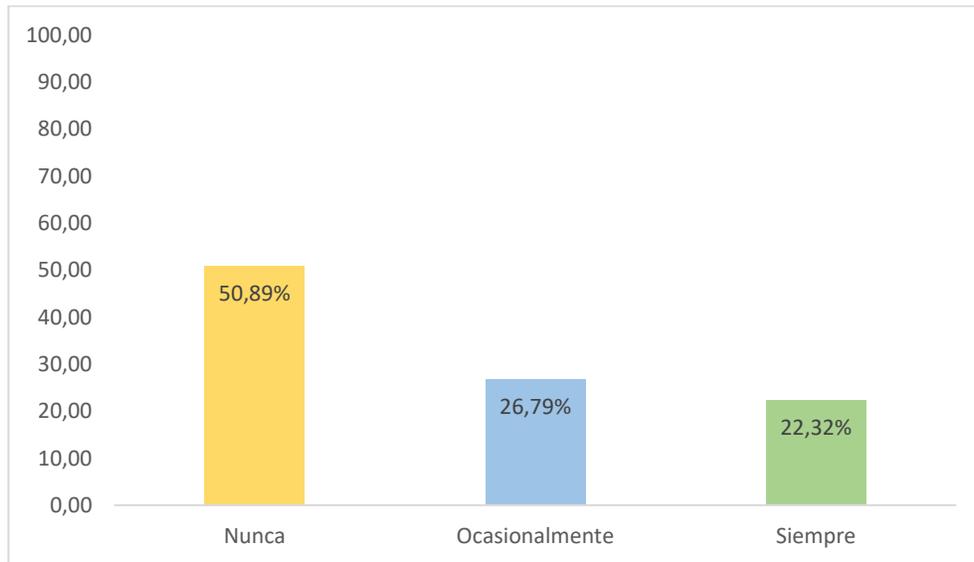
¿Conoce usted sobre que trata el harassment?



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Conforme a los resultados que se evidencian en la figura 11, se puede comentar respecto a la pregunta: *¿Reconoce que el harassment puede tener un impacto negativo en la salud mental y bienestar de las personas que lo sufren?* Que el 64.29% respondió que Si mientras que el 35.71% respondió No, así mismo para la pregunta *¿Está usted al tanto de que el "harassment "puede ser definido como un comportamiento agresivo hacia otra persona en internet?* El 53.57% de los encuestados respondió Si y el 46.43% restante respondió no, por último, para la pregunta: *¿Está usted familiarizado con que la repetición de amenazas, insultos, frases denigrantes y humillación a través de mensajes o llamadas se conoce cómo harassment?* Encontramos que el 42.86% respondieron que No y el 57.14% respondió Si.

Figura 12.
Phishing.

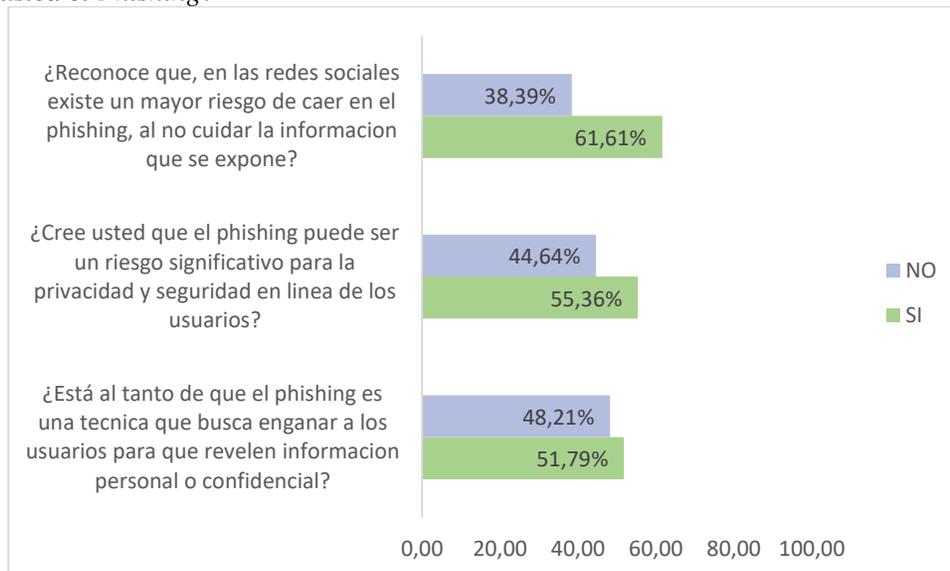


Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 12, corresponden a la pregunta: ¿La institución educativa ha brindado información acerca del phishing?, las respuestas indican que en el rango de Nunca hay un porcentaje de 50.89%, el rango Ocasionalmente tiene un porcentaje de 26.79% y por último el rango de Siempre cuenta con el porcentaje de 22.32%.

Así mismo se indican los resultados de las preguntas dicotómicas en relación a la dimensión 6 de ¿Reconoce usted el Phishing? Los cuales se representan en la figura 13.

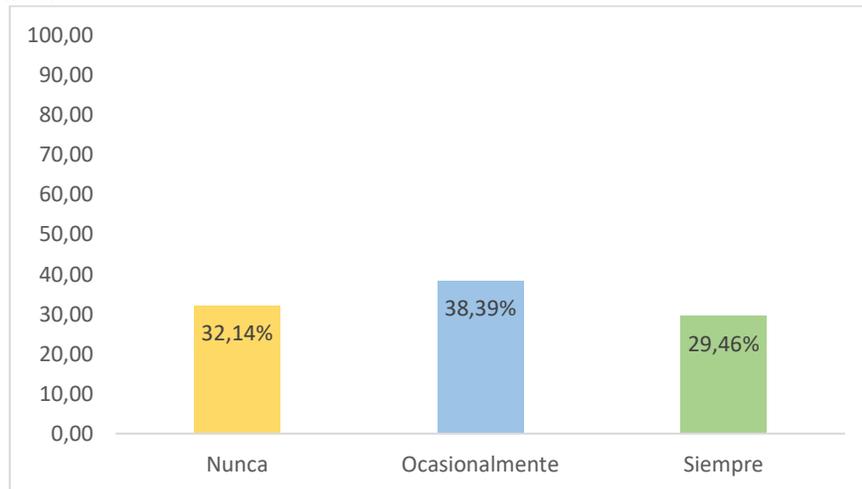
Figura 13.
¿Reconoce usted el Phishing?



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo a los resultados que se evidencian en la figura 13, se puede evidenciar respecto si ¿Reconoce que, en las redes sociales existe un mayor riesgo de caer en el phishing, al no cuidar la información que se expone?, las respuesta Si tiene un 61.61% mientras que el No contempla un 38.39%, mientras que la pregunta ¿Cree usted que el phishing puede ser un riesgo significativo para la privacidad y seguridad en línea de los usuarios? Las personas que respondieron Si corresponden al 55.36% y el No tiene un 44.64%, por último, la pregunta sobre si ¿Está al tanto de que el phishing es una técnica que busca engañar a los usuarios para que revelen información personal o confidencial? El Si tiene un 51.79% y el No con 48.21%.

Figura 14.
Pornografía infantil.



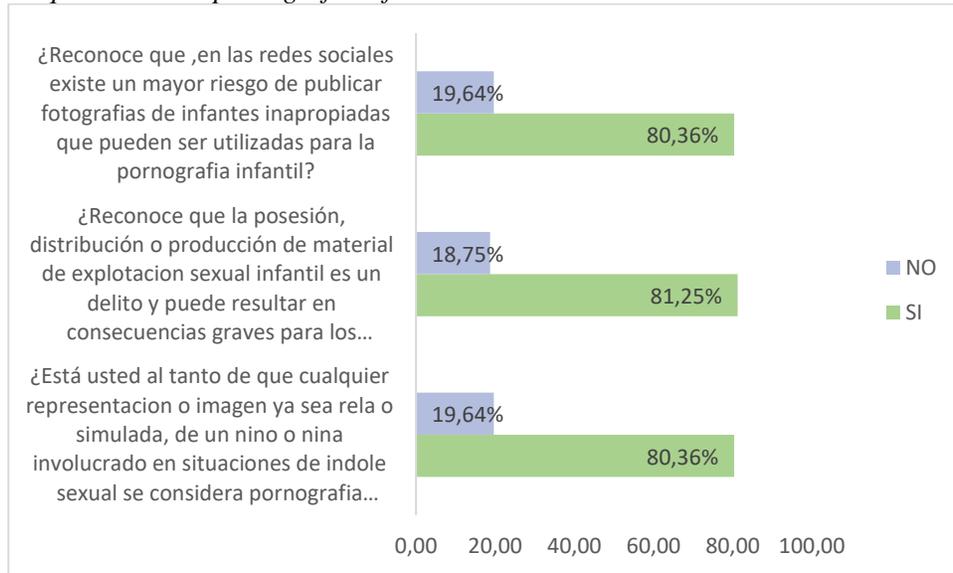
Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 14, corresponden a la pregunta: ¿La institución educativa ha brindado información acerca de la pornografía infantil?, las respuestas indican que en el rango de Ocasionalmente hay un porcentaje de 38.39%, el rango Nunca tiene un porcentaje de 32.14% y por último el rango de Siempre cuenta con el porcentaje de 29.46%.

Así mismo se indican los resultados de las preguntas dicotómicas en relación a la dimensión 7 de ¿Conoce usted que abarca la pornografía infantil? Los cuales se representan en la figura 15.

Figura 15.

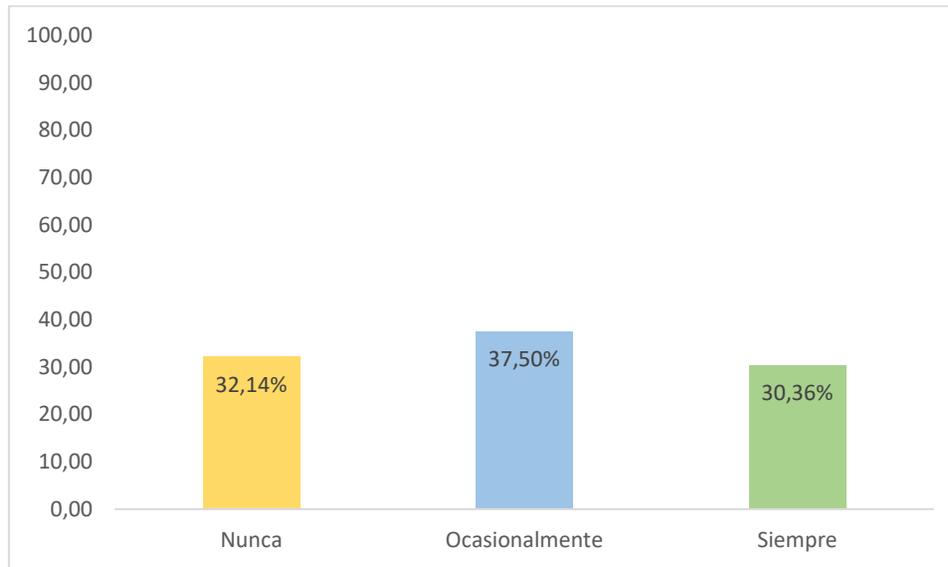
¿Conoce usted que abarca la pornografía infantil?



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo a los resultados que se evidencian en la figura 15, se puede determinar que respecto a la pregunta de si ¿Reconoce que, en las redes sociales existe un mayor riesgo de publicar fotografías de infantes inapropiadas que pueden ser utilizadas para la pornografía infantil? El Si corresponde al 80.36% y el No al 19.64%, para la siguiente pregunta sobre si ¿Reconoce que la posesión, distribución o producción de material de explotación sexual infantil es un delito y puede resultar en consecuencias graves para los infractores? El 81.25% contestó que Si, mientras que el 18.75% respondió que No, para la última pregunta que dice ¿Está usted al tanto de que cualquier representación o imagen ya sea real o simulada, de un niño o niña involucrado en situaciones de índole sexual se considera pornografía infantil? El 80.36% de los encuestados respondieron Si, mientras que el 19.64% restante respondió que No.

Figura 16.
Sexting.



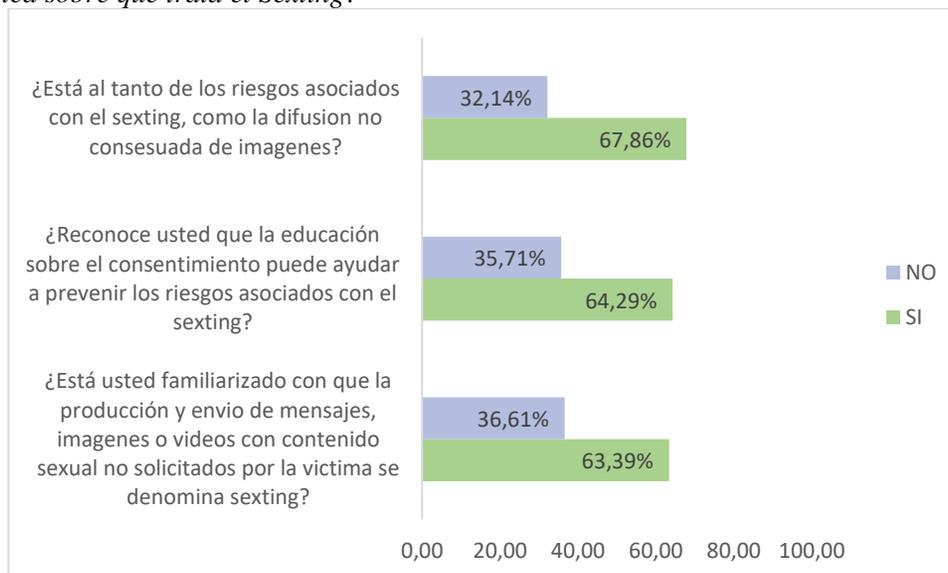
Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 16, corresponden a la pregunta: ¿Conoce usted sobre qué trata el Sexting?, las respuestas indican que en el rango de Ocasionalmente hay un porcentaje de 37.50%, el rango Nunca tiene un porcentaje de 32.14% y por último el rango de Siempre cuenta con el porcentaje de 30.36%.

Así mismo se indican los resultados de las preguntas dicotómicas en relación a la dimensión 7 de ¿Conoce usted sobre qué trata el Sexting? Los cuales se representan en la figura 17.

Figura 17.

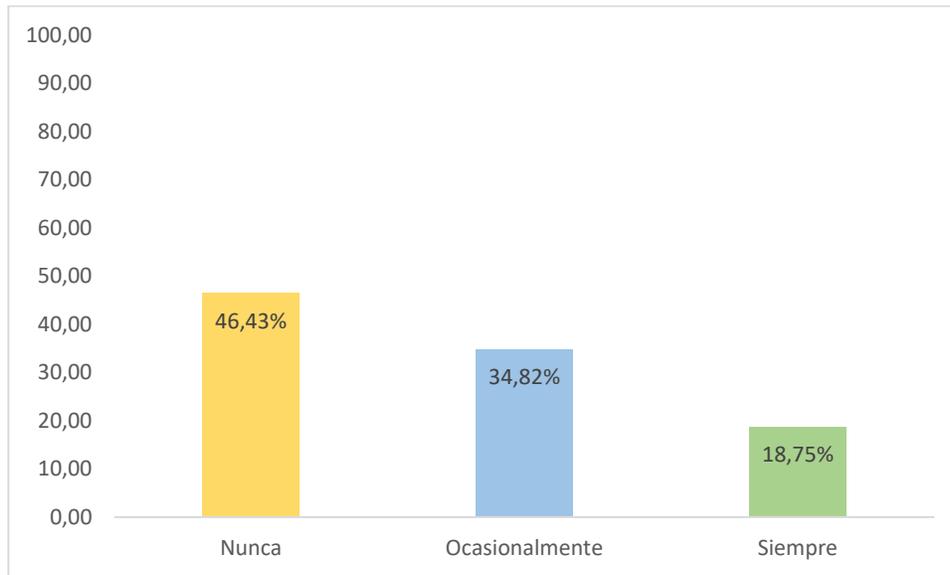
¿Conoce usted sobre qué trata el Sexting?



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo a los resultados que se evidencian en la figura 17, se puede determinar para la pregunta *¿Está al tanto de los riesgos asociados con el sexting, como la difusión no consensuada de imágenes?* El 67.86% corresponde al sí y el 32.14% al no, así también para la pregunta *¿Reconoce usted que la educación sobre el consentimiento puede ayudar a prevenir los riesgos asociados con el sexting?* El 64.29% respondió Si mientras que el 35.71% respondió No y para la última pregunta *¿Está usted familiarizado con que la producción y envío de mensajes, imágenes o videos con contenido sexual no solicitados por la víctima se denomina sexting?* El 63.39% respondió Si y el 35.61% No.

Figura 18.
Sextorsión.

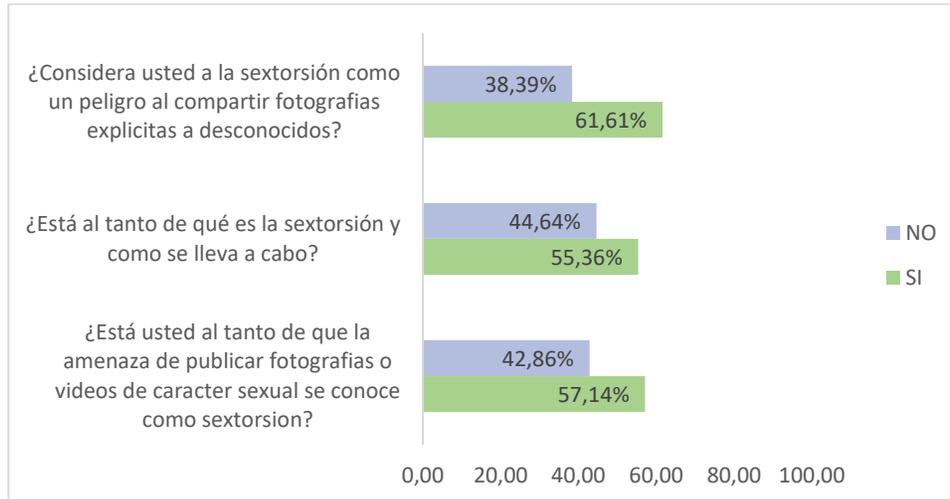


Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 18, corresponden a la pregunta: ¿La institución educativa ha proporcionado información acerca de la sextorsión?, las respuestas indican que en el rango de Nunca hay un porcentaje de 46.43%, el rango Ocasionalmente tiene un porcentaje de 34.82% y por último el rango de Siempre cuenta con el porcentaje de 18.75%.

Así mismo se indican los resultados de las preguntas dicotómicas en relación a la dimensión 8 de ¿La institución educativa ha proporcionado información acerca de la Sextorsión? Los cuales se representan en la figura 19.

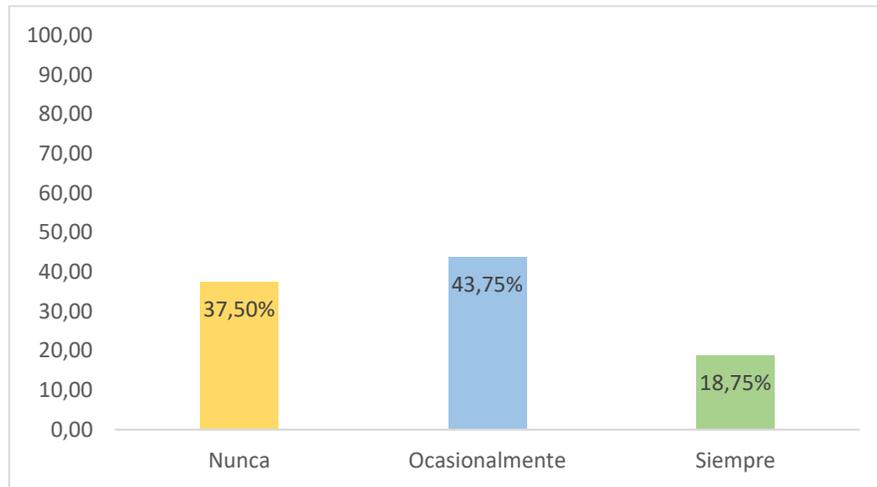
Figura 19.
Sextorsión.



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo con los datos que se evidencian en la figura 19, se han recopilado los datos de las siguientes preguntas, para *¿Considera usted a la sextorsión como un peligro al compartir fotografías explícitas a desconocidos?* El 61.61% respondieron Si y el 38.39% No, para la siguiente pregunta *¿Está al tanto de qué es la sextorsión y como se lleva a cabo?* El 55.36% respondió que Si y el 44.64% No, y para la última pregunta *¿Está usted al tanto de que la amenaza de publicar fotografías o videos de carácter sexual se conoce como sextorsión?* El 57,14% respondió que Si y el 42.86% No.

Figura 20.
Stalking.



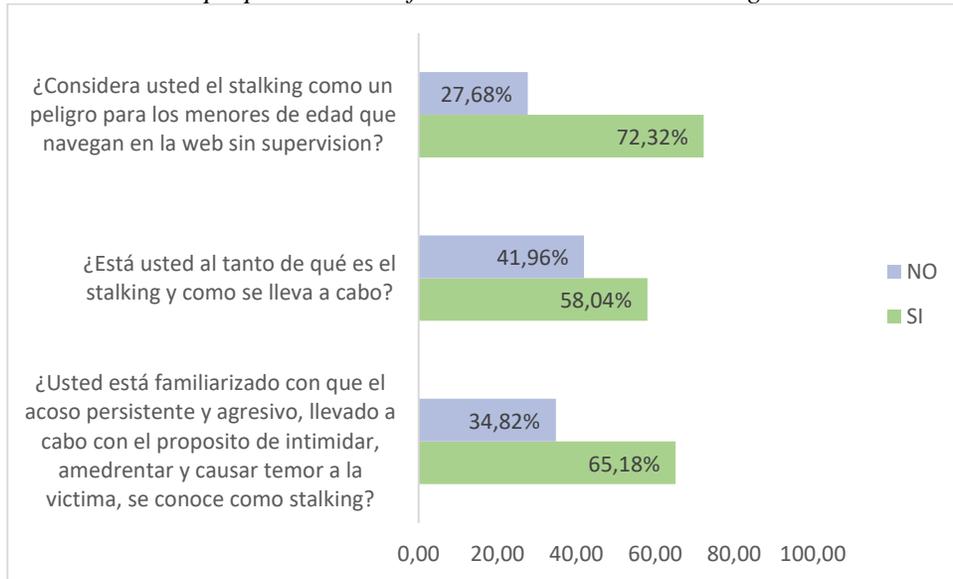
Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 20, corresponden a la pregunta: ¿La institución educativa ha proporcionado información acerca del stalking?, las respuestas indican que en el rango de Ocasionalmente hay un porcentaje de 43.75%, el rango Nunca tiene un porcentaje de 37.50% y por último el rango de Siempre cuenta con el porcentaje de 18.75%.

Así mismo se indican los resultados de las preguntas dicotómicas en relación a la dimensión 9 de ¿La institución educativa ha proporcionado información acerca de la Sextorsión? Los cuales se representan en la figura 21.

Figura 21.

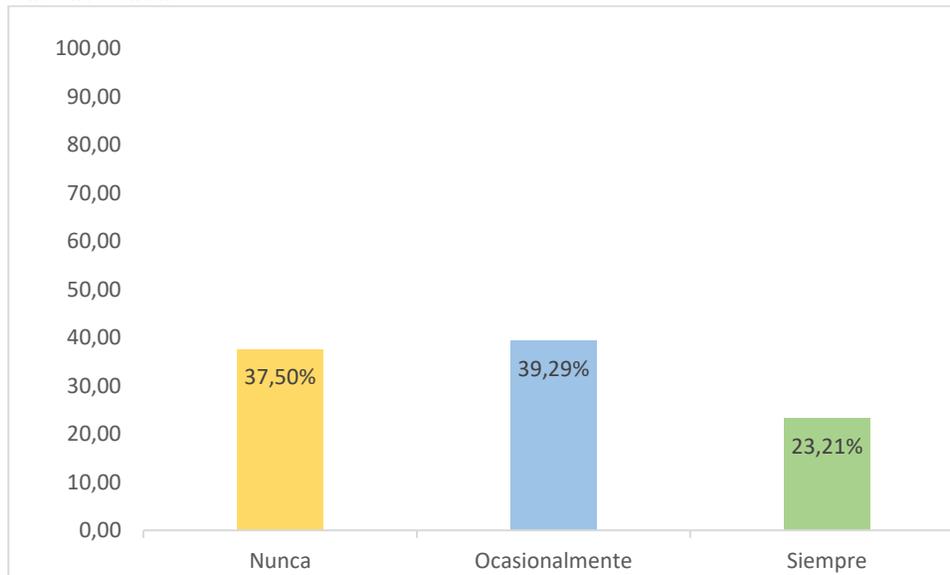
¿La institución educativa ha proporcionado información acerca del Stalking?



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo a los resultados de la figura 23, se puede describir respecto a si ¿Considera usted el stalking como un peligro para los menores de edad que navegan en la web sin supervisión? La respuesta Si tiene un 72.32% mientras que el 27.68% respondió No, para la pregunta ¿Está usted al tanto de qué es el stalking y como se lleva a cabo? El porcentaje de personas que respondieron Si es del 58.04% y No el 41.96%, para la última pregunta ¿Usted está familiarizado con que el acoso persistente y agresivo, llevado a cabo con el propósito de intimidar, amedrentar y causar temor a la víctima, se conoce como stalking? El 65.18% respondió Si, mientras que 34.82% restante respondió No.

Figura 22.
Suplantación de identidad.



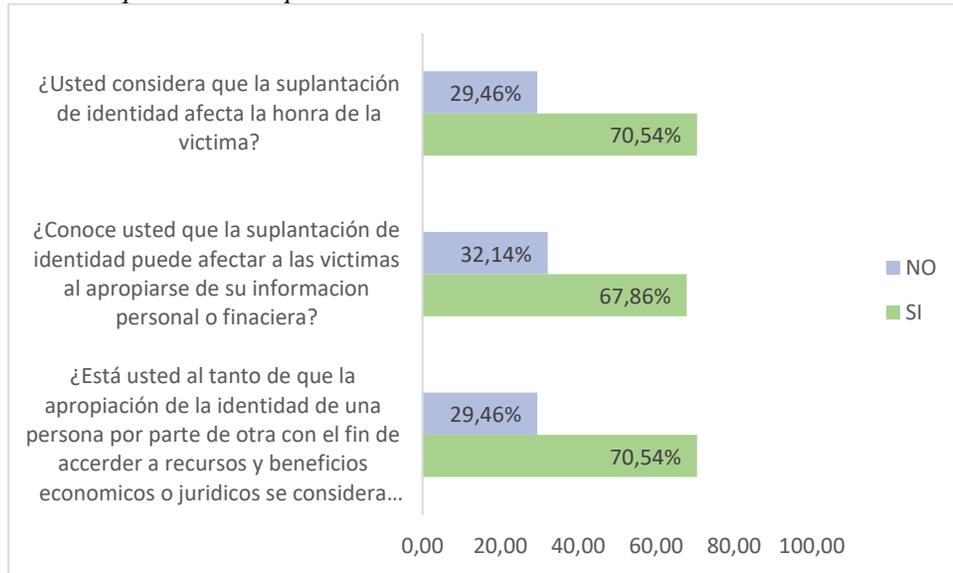
Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 22, corresponden a la pregunta: ¿La institución educativa ha proporcionado información acerca de la suplantación de identidad?, las respuestas indican que en el rango de Ocasionalmente hay un porcentaje de 39.29%, el rango Nunca tiene un porcentaje de 37.50% y por último el rango de Siempre cuenta con el porcentaje de 23.21%.

Así mismo se indican los resultados de las preguntas dicotómicas en relación a la dimensión 10 de ¿La institución educativa ha proporcionado información acerca de la Suplantación de identidad? Los cuales se representan en la figura 23.

Figura 23.

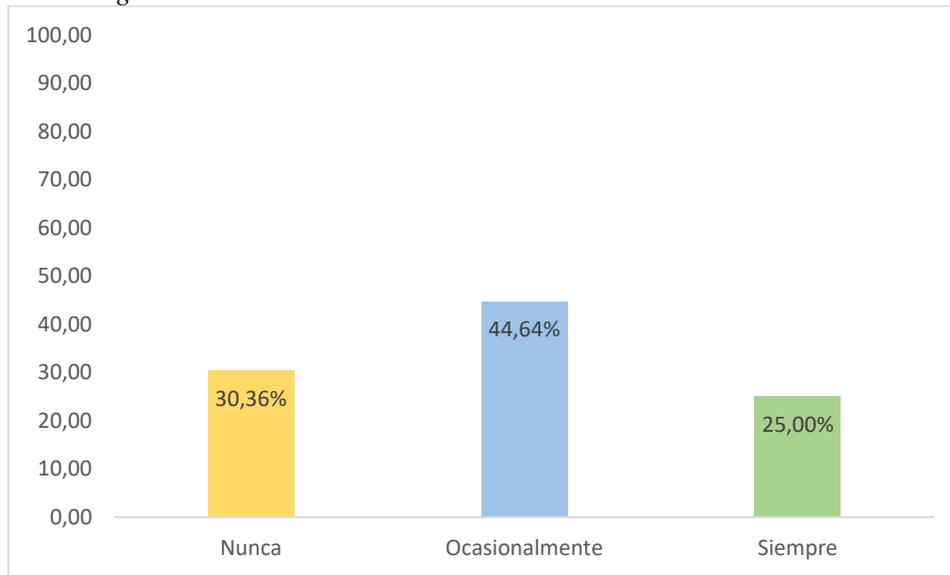
¿Conoce usted sobre qué trata la suplantación de identidad?



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo a los resultados que se evidencian en la figura 23, se puede describir respecto a la pregunta *¿Usted considera que la suplantación de identidad afecta la honra de la víctima?* El 70.54% respondió Si y No el 29.46%, para la pregunta *¿Conoce usted que la suplantación de identidad puede afectar a las víctimas al apropiarse de su información personal o financiera?* El 67.86% respondió que Si y el 32.14% No, y por último para la pregunta *¿Está usted al tanto de que la apropiación de la identidad de una persona por parte de otra con el fin de acceder a recursos o beneficios económicos o jurídicos se considera suplantación de identidad?* El 70.54% de los encuestados respondió que Si y el 29.46% restante No.

Figura 24.
Delitos por medios digitales.



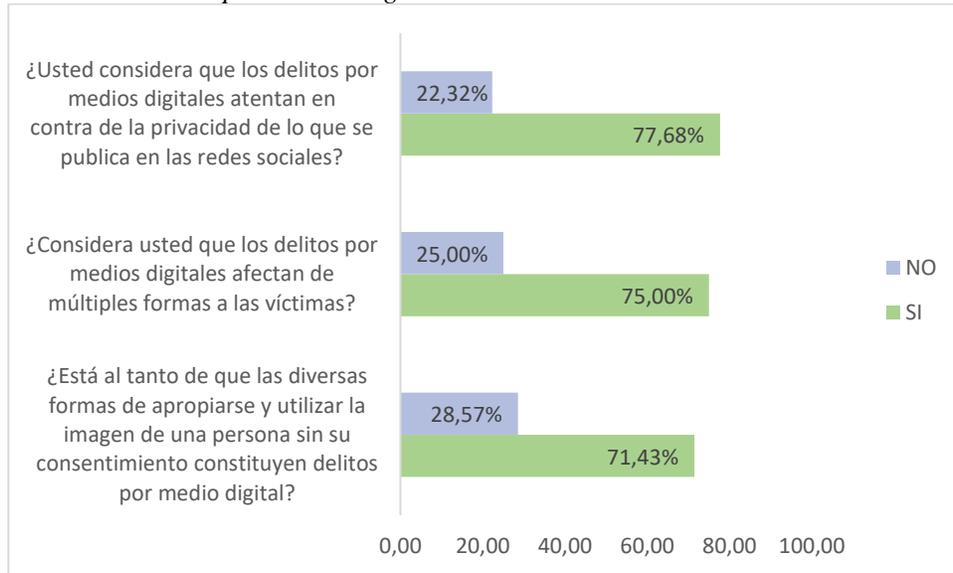
Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 24, corresponden a la pregunta: ¿La institución educativa ha proporcionado información acerca de los delitos por medios digitales?, las respuestas indican que en el rango de Ocasionalmente hay un porcentaje de 44.64%, el rango Nunca tiene un porcentaje de 30.36% y por último el rango de Siempre cuenta con el porcentaje de 25.00%.

Así mismo se indican los resultados de las preguntas dicotómicas en relación a la dimensión 11 de ¿La institución educativa ha proporcionado información acerca de los delitos por medios digitales? Los cuales se representan en la figura 25.

Figura 25.

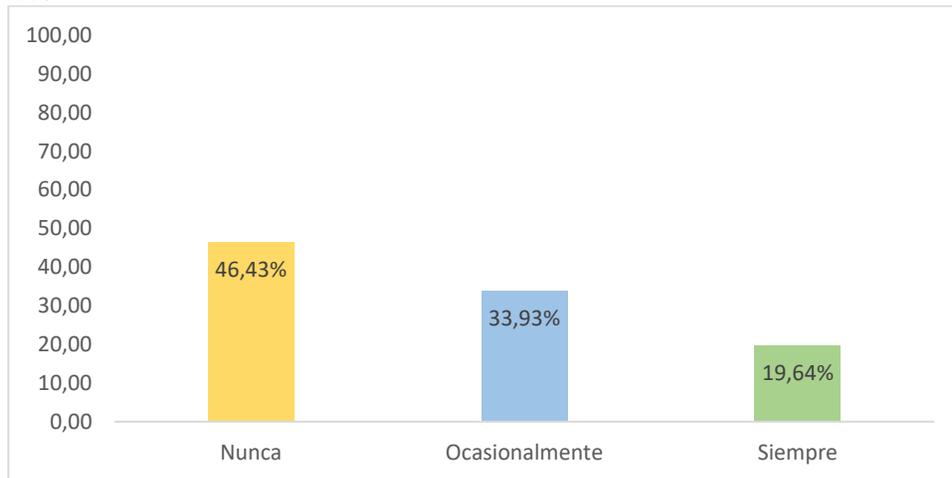
¿Conoce acerca de los delitos por medios digitales?



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo a los resultados que se evidencian en la figura 25, respecto a si ¿Usted considera que los delitos por medios digitales atentan en contra de la privacidad de lo que se publica en las redes sociales? El 77.68% de los encuestados respondieron Si, mientras que el 22.32% No, para la pregunta ¿Considera usted que los delitos por medios digitales afectan de múltiples formas a las víctimas? El 75.00% respondió Si y No el 25.00% restante y para la última pregunta ¿Está al tanto de que las diversas formas de apropiarse y utilizar la imagen de una persona sin su consentimiento constituyen delitos por medio digital? El 71.43% respondió Si y el 28.57% No.

Figura 26.
Lolicon/Shotacon.



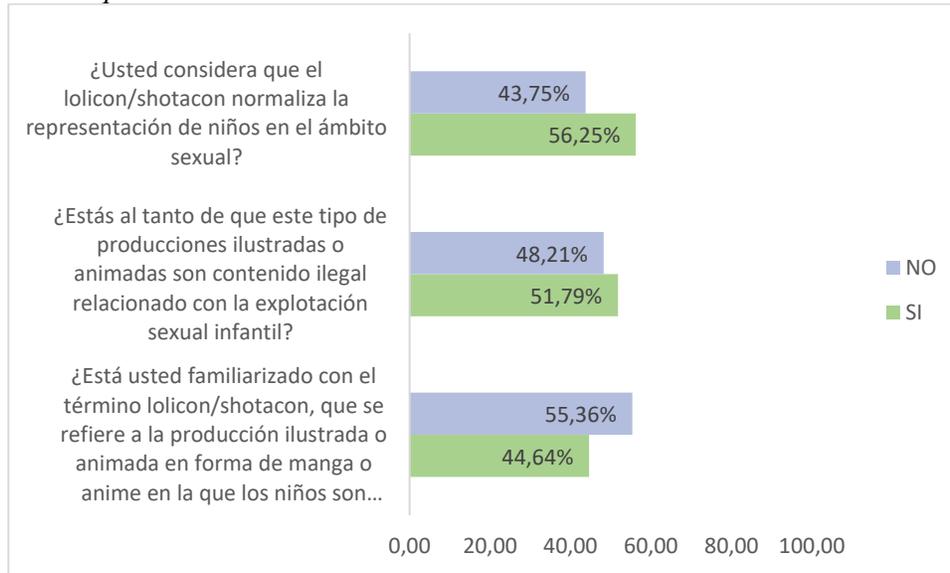
Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

Los resultados que se muestran en la figura 26, corresponden a la pregunta: ¿La institución educativa ha proporcionado información acerca del Lolicon/Shotacon?, las respuestas indican que en el rango de Nunca hay un porcentaje de 46.43%, el rango Ocasionalmente tiene un porcentaje de 33.93% y por último el rango de Siempre cuenta con el porcentaje de 19.64%

Así mismo se indican los resultados de las preguntas dicotómicas en relación a la dimensión 12 de ¿Conoce acerca de que trata el Lolicon/Shotacon? Los cuales se representan en la figura 27.

Figura 27.

¿Conoce acerca de que trata el Lolicon/Shotacon?



Nota. Resultados obtenidos de la encuesta aplicada a los estudiantes del tercer año de BGU, adaptado de la guía del Ministerio de Educación del Ecuador (2020).

De acuerdo a los resultados que se evidencian en la figura 27, se puede describir respecto a si *¿Usted considera que el Lolicon/Shotacon normaliza la representación de niños en el ámbito sexual?*, la respuesta Si tiene 56.25% y No un 43.75%, para la pregunta *¿Está al tanto de que este tipo de producciones ilustradas o animadas son contenido ilegal relacionado con la explotación sexual infantil?*, el 51,79% de la población encuestado respondió Si mientras que el 48.21% respondió No, y por ultimo para la pregunta *¿Está usted familiarizado con el termino Lolicon/Shotacon, que se refiere a la producción ilustrada o animada en forma de manga o anime en la que los niños son representados en relaciones sexuales implícitas o explícitas con adultos?* El 44,64% respondió Si y el 55.36% No.

La mayoría de las estudiantes conocen los riesgos asociados al uso de internet a partir de la guía del Ministerio de Educación y pueden identificar las diversas actividades que las constituyen. Sin embargo, existen áreas donde su conocimiento es limitado, especialmente en cuanto a riesgos como el lolicon y la suplantación de identidad.

7. Discusión

En el Ecuador al igual que en el resto del mundo, muchos niños y adolescentes transitan momentos embarazosos en su vida por ser víctimas de la violencia física o psicológica proveniente de personas de su entorno cercano o social que influyen desfavorablemente en su vida, el acoso puede consistir en un ataque directo por parte de una persona o un grupo de estas que pretende perturbar la integridad de un niño o adolescente; a veces aprovechándose de medios tecnológicos para perpetrar y extender sus conductas generando un gran daño (Rosero 2022).

Con lo mencionado anteriormente es preciso dar respuesta a la investigación planteada en el presente trabajo de integración curricular, en donde la metodología utilizada fue idónea y adecuada lo cuál se pudo dar contestación a cada una de las interrogantes planteadas entre ellas la general reza: ¿Cuál es el diagnóstico de los riesgos del uso de internet en los estudiantes de tercer año de bachillerato general unificado de la Unidad Educativa Fiscomisional La Inmaculada?

Siendo así, la investigación estuvo conformada por preguntas de investigación, en donde la primera menciona: ¿Qué riesgos existen al usar internet para los jóvenes?, para lo cual se hizo búsquedas en repositorios digitales para indagar los riesgos de internet que se representaron en una tabla de caracterización la cual permitió ordenar ideas y conceptos sobre los riesgos al usar el internet, que como menciona el autor Esteras (2020), se refieren a las posibles amenazas, peligros y vulnerabilidades a los que los usuarios pueden estar expuestos mientras utilizan las TIC, estos riesgos son variados, pueden afectar a los usuarios de diferentes formas, desde la exposición a contenido inapropiado, acoso o robo de identidad.

Así mismo con relación a la segunda pregunta ¿Cómo identificar los riesgos del uso de internet para los jóvenes a partir de la Guía del Ministerio de Educación del Ecuador, para prevención de riesgos durante el uso de internet y dispositivos tecnológicos? Se hizo una tabla de caracterización sobre los riesgos en el uso de internet identificados en la guía del Ministerio de Educación, que son: trata de personas, harassment, flamming, grooming, sexting, hacking, phishing, pornografía infantil, sextorsión, stalking, suplantación de identidad, delitos por medios digitales, lolicon/shotacon.

En relación con lo anterior el Ministerio de Educación (2020), manifiesta que es importante que las y los estudiantes mantengan una actitud crítica ante lo que encuentran y lo que publican en

Internet, al no poder evitar que otras personas sean agresoras o busquen hacer daño, su seguridad depende en gran medida de la información que posean, de su actitud responsable y de su atención para identificar malas prácticas (p.13).

Considerándose así, que las faltas de políticas de educación, prevención y uso adecuado del internet, hacen que el acceso a la red se convierta en un problema para los jóvenes que están expuestos a diferentes problemáticas que en muchas ocasiones no son detectados, ignorados o naturalizados por la sociedad, (Buenaño, 2021).

Consecuentemente el presente trabajo de integración consta de una tercera pregunta denominada ¿Cuál es el diagnóstico de los riesgos del uso de internet en los estudiantes de tercer año de bachillerato general unificado de la Unidad Educativa Fiscomisional La Inmaculada?, en donde los resultados arrojados en relación a si la institución educativa ha proporcionado información de manera ocasional sobre los riesgos como la trata de personas, grooming, pornografía infantil, sexting, stalking, suplantación de identidad y delitos por medios digitales. Mientras que los riesgos: flammig, hacking, harassment, phishing, sextorsión y Lolicon/Shotacon nunca han sido tratados.

De acuerdo a los resultados anteriormente mencionados, es preciso que por parte de la institución promover el buen uso del internet, tal como lo menciona Buenaño (2021), es necesario aplicar campañas para desarrollar una estrategia que busque la creación de la conciencia y uso legal de la red de internet, ya que muchas veces las víctimas muerden en anzuelo por desconocimiento de prácticas ilícitas que buscan sacar provechos de las desventajas de la falta de habilidades tecnológicas en la población.

Se pretende que con el trabajo de integración curricular formulado se pueda generar nuevas investigaciones en este campo a fin de poder prevenir los diferentes riesgos que existen en el internet al momento de su uso, es importante destacar que una de las limitaciones fue la poca información sobre estudios que hablen de los riesgos al usar internet y dispositivos tecnológicos en la ciudad de Loja.

8. Conclusiones

Se pudo definir los riesgos del uso de internet para jóvenes de bachillerato general unificado en una tabla de caracterización, los cuales son: trata de personas, (Meneses, 2019), harassment, (Neyra, 2021), grooming, ciberacoso inmobiliario, ciberacoso de género, cybermobbing, fraping, (Rosero, 2020), sextorsión, doxing, porno venganza (Cuentas y Echeverria, 2022), suplantación de identidad, (Vera, 2019), ciberadicción, (Tsitsika, et al., 2012, citado por Esteras, 2020), stalking, (Guzmán, 2016), acceso a contenido inadecuado, (Esteras, 2020).

Se logró identificar trece riesgos del uso del internet que establece la guía del Ministerio de Educación del Ecuador (2020), cuales son: trata de personas, harassment, flammimg, grooming, sexting, hacking, phishing, pornografía infantil, sextorsión, stalking, suplantación de identidad, delitos por medios digitales, lolicon/shotacon, para organizar esta información, se creó una tabla de caracterización, donde cada riesgo identificado en la guía se relacionó con el COIP del Ecuador. Esta relación permitió resaltar la importancia de comprender las implicaciones legales asociadas con ciertas acciones en línea.

Se diagnosticó que los riesgos, se desprende que en la Unidad Educativa Fiscomisional La Inmaculada, la atención hacia la prevención de riesgos durante el uso de internet y dispositivos tecnológicos no se trata siempre. Sin embargo, es evidente que la mayoría de las estudiantes de esta institución, de acuerdo a sus respuestas, demuestran habilidad para identificar dichos riesgos, lo que sugiere que han adquirido conocimientos a través de la iniciativa propia o la influencia de familias responsables en el uso de internet y dispositivos tecnológicos.

9. Recomendaciones

Basados en los resultados de esta investigación, se recomienda a las autoridades de la institución educativa fortalecer el enfoque hacia la prevención de riesgos del uso de internet y dispositivos tecnológicos, con el fin de formar ciudadanos preparados para el mundo digital, que generen un entorno seguro, dándole un uso adecuado, responsable, ético y respetuoso.

10. Bibliografía

- Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista venezolana de gerencia*, 89(89), 351–368. <https://doi.org/10.37960/revista.v25i89.31534>
- Aguilera, S., & Estefania, A. (2019). Baby Otako: Hipersexualización e infantilización de la mujer en la animación japonesa. Universidad de La Laguna. <https://riull.ull.es/xmlui/handle/915/17094>
- Alarcón Bowen, José Luis. El tratamiento del delito de pornografía infantil en la legislación ecuatoriana. Quito, 2015, 108 p. Tesis (Maestría en Derecho Penal). Universidad Andina Simón Bolívar, Sede Ecuador. Área de Derecho. <https://repositorio.uasb.edu.ec/handle/10644/4500>
- Alonso, N. (2020). ¿Qué es el flaming en Internet? <https://protecciondatos-lopd.com/empresas/flaming/>
- Alonso, N. (2020, octubre 5). ¿Qué es el flaming en Internet? Grupo Atico34; Ático34 Protección de datos para empresas y autónomos. <https://protecciondatos-lopd.com/empresas/flaming/>
- Avila, S., & Angel, M. (2019). Hacking ético: impacto en la sociedad. <http://repository.unipiloto.edu.co/handle/20.500.12277/4919>
- Bermeo, R., & Isaac, P. (2022). *El Hostigamiento (Stalking) Como Delito En La Legislación Ecuatoriana*. Universidad Internacional SEK. <https://repositorio.uisek.edu.ec/handle/123456789/4893>
- Buenaño Mora, M. F. (2021). Estudio sobre el uso de Internet y riesgos asociados en jóvenes universitarios de 18 a 30 años.
- Calderón, H., & Ángel, E. (2016). El Phishing como Delito Informático y su Falta de Tipificación en el Código Orgánico Integral Penal. Quito: UCE. <http://www.dspace.uce.edu.ec/handle/25000/8132>
- Cuentas Gómez, M. J., & Echeverria Amaris, C. A. (2022). Sexting, sextorsión, doxing y porno venganza como manifestación de violencia contra la mujer en el municipio de Sabanalarga

- Atlántico 2021-2022. Corporación universidad de la Costa.
<https://repositorio.cuc.edu.co/handle/11323/9816>
- Cuentas, M., y Echeverria, C., (2022). Sexting, sextorsión, doxing y porno venganza como manifestación de violencia contra la mujer en el municipio de Sabanalarga Atlántico 2021-2022.
- Dammert Guardia, M., Dammert, L., & Sarmiento, K. (2020). La trata de personas en los Andes: dinámicas socio-espaciales en las fronteras de Perú. *Íconos - Revista De Ciencias Sociales*, (68), 117–134. <https://doi.org/10.17141/iconos.68.2020.4043>
- El mundo virtual de Eugenia – Recursos Educativos. (2021). Gob.ec.
<https://recursos2.educacion.gob.ec/euinicio/>
- Esteras, P. (2020). Prevención de riesgos en Internet y redes sociales en Secundaria, desde la tríada alumnos, padres y profesores.
<https://repositorio.ucam.edu/bitstream/handle/10952/4425/Esteras%20Saz%2C%20Pablo.pdf?sequence=1&isAllowed=y>
- Fernández Reigosa, P. (2021). Propuesta de prevención, detección e intervención en ciberbullying en el ámbito educativo. Universidad de Oviedo. <http://hdl.handle.net/10651/60562>
- Gamito, R. Pilar, A. Olasolo, T. Vizcarra, T. (2017). La necesidad de trabajar los riesgos de internet en el Aula.
- García, G., y Eloy, D. (2018). El Phishing como delito de estafa informática.
http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572018000100025
- Herrera, A., García, J., & Tapia, G. (2015). La percepción del hostigamiento y acoso sexual en mujeres estudiantes en dos instituciones de educación superior. *Revista de la educación superior*, 44(176), 63–82. <https://doi.org/10.1016/j.resu.2015.12.004>
- Liliana, V., & Calderón, P. (2021). Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través de internet. Universidad Nacional de Chimborazo.
<http://dspace.unach.edu.ec/handle/51000/7607>

- Mandato, P., & Nacional, L. A. (n.d.). CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP. Gob.Ec. Retrieved June 6, 2023, from https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf
- Meneses Falcón, C. (2019). ¿Por qué se identifican tan pocas víctimas de trata de seres humanos?. Revista De La Facultad De Derecho, (107). <https://doi.org/10.14422/icade.i107.y2019.001>
- Ministerio de Educación del Ecuador (2018). Guía para Prevención de Riesgos durante el uso de internet y dispositivos tecnológicos.
- Ministerio de Educación del Ecuador (2021). Promoción de derechos en el uso seguro de Internet, desde las familias.
- Morán, M. (2015). Educación. Desarrollo Sostenible. <https://www.un.org/sustainabledevelopment/es/education/>
- Neyra, O., (2021). Cyberbullying: El acoso escolar en el ciberespacio e implicancias psicológicas. Hamut'ay, 8 (1), <http://dx.doi.org/10.21503/hamu.v8i1.2238>
- Orosco, J. R. y Pomasunco, R. (2020). Adolescentes frente a los riesgos en el uso de las TIC. Revista Electrónica de Investigación Educativa, 22, e17, 1-13. <https://redie.uabc.mx/redie/article/view/2298>
- Orosco, J., y Pomasunco, R. (2020). Adolescentes frente a los riesgos en el uso de las TIC. Revista Electrónica de Investigación Educativa, 22, e17, 1-13. <https://doi.org/10.24320/redie.2020.22.e17.2298>.
- Orozco Báez, M. (2020). Influencia de los hogares disfuncionales en el ciberacoso. Propuesta pedagógica dirigida a acudientes. Universidad Pedagógica y Tecnológica de Colombia. <https://repositorio.uptc.edu.co/handle/001/3207>
- Pardillo, Z., & Elisabeth, N. (2015). El stalking como nueva forma de acoso: las limitaciones de la regulación y la intervención actuales. <https://ddd.uab.cat/record/133348>
- Pérez, P. (2018). Online Grooming: Características y Factores de Riesgo del Abuso Sexual de Menores a través de Internet.
- Recalde, J. (2021). El ciberacoso por redes sociales en el Ecuador.

Resolución del Consejo de Educación Superior. (2017). Reglamento de régimen Académico Consejo de Educación Superior.

Ressett, S. (2019). Sexting en adolescentes: su predicción a partir de los problemas emocionales y la personalidad oscura. *Escritos de psicología*, 12(2), 93–102.
<https://doi.org/10.24310/espsiescpsi.v12i2.10060>

Sánchez, L., García, A., y Álvarez, F., (2022.). Transformación Digital de las Instituciones Educativas. <http://www.aniei.org.mx/Archivos/Libros/Libro2022.pdf#page=36>

Save the Children (2019). Grooming, qué es, cómo detectarlo y prevenirlo.
<https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo>

Vera, H., & Antonio, D. (2019). La suplantación de identidad cibernética en el Ecuador.
<https://bdigital.uexternado.edu.co/entities/publication/e4c9884a-ad38-4350-a324-fc732276eb93/full>

11. Anexos

Anexo 1.

Solicitud a la Autoridad de la Institución Educativa.



Of. No. UNL-FEAC-CPCEI-2023-057-OF

Loja, 13 de marzo de 2023

PARA: Hna.
**RECTORA DE LA UNIDAD EDUCATIVA FISCOMISIONAL
"LA INMACULADA"**

ASUNTO: Autorización para elaborar Proyecto de Investigación

De mi consideración:

Por medio de la presente me dirijo a Usted para expresarle un cordial saludo y a la vez exponerle y solicitarle lo siguiente:

Uno de los objetivos de la Carrera de Pedagogía de las Ciencias Experimentales Informática señalados en su Plan de Estudios es: Vincular al Estudiante con los futuros escenarios de desempeño laboral en el medio educativo, así como promover y potenciar la integración de recursos digitales en una red de contextos de aula o a lo interno de las instituciones educativas.

Por ello, cumpíeme solicitarle, comedidamente, se sirva autorizar al señor **Pablo Gabriel Vargas Barragán**, estudiante del séptimo ciclo de la carrera pueda obtener en la Institución de su acertada dirección la información necesaria para elaborar el Proyecto de Investigación: **Diagnóstico de los riesgos del uso de internet de la guía del Ministerio de Educación del Ecuador para prevención de riesgos durante el uso de internet y dispositivos tecnológicos en el tercer año de bachillerato general unificado de la Unidad Educativa Fiscomisional La Inmaculada en el año lectivo 2022 - 2023.**

Le agradezco de antemano su favorable atención a la presente y hago propicia la ocasión para reiterarle los sentimientos de consideración distinguidos.

Atentamente,

Milton Leonardo Labanda Jarapillo, Ms.

**DIRECTOR DE LAS CARRERAS INFORMÁTICA EDUCATIVA Y
PEDAGOGÍA DE LAS CIENCIAS EXPERIMENTALES INFORMÁTICA**

C c Archivo
M.L.J./mamut



Ciudad Universitaria "Guillermo Falconi Espinosa" Casilla letra "S"
Teléfono: 2547 - 252 Ext. 101-2547-200
direccion.cle@unl.edu.ec / secretaria.cle@unl.edu.ec 2545640

Anexo 2.
Validación del Instrumento.



UNL

Universidad Nacional de Loja

Carrera de Pedagogía de las Ciencias Experimentales Informática

Validación del Instrumento

Nombre: *Harbe Halcabado Jimenez*

1. Presentación

(Marque con una X su valoración)

	Excelente	Buena	Regular	Malo
Claridad del planteamiento	<input checked="" type="checkbox"/>			
Adecuación a los destinatarios	<input checked="" type="checkbox"/>			
Longitud del texto	<input checked="" type="checkbox"/>			
Calidad de contenido (redacción)	<input checked="" type="checkbox"/>			
Modificaciones que haría a la presentación <i>Organizar la información para que este claro sobre un tema en una hoja, y no se corte la información. Numerar el contenido (letra).</i>				

2. Instrucciones para el proceso de respuesta

(Marque con una X su valoración)

	Excelente	Buena	Regular	Malo
Claridad	<input checked="" type="checkbox"/>			
Adecuación	<input checked="" type="checkbox"/>			
Cantidad	<input checked="" type="checkbox"/>			
Calidad	<input checked="" type="checkbox"/>			
Modificaciones que haría a las instrucciones <i>Principio</i>				

3. Preguntas del cuestionario

(Marque con una X su valoración)

	Excelente	Buena	Regular	Malo
Orden lógico de presentación	<input checked="" type="checkbox"/>			
Claridad en la redacción	<input checked="" type="checkbox"/>			
Adecuación de las opciones de respuesta	<input checked="" type="checkbox"/>			
Cantidad de preguntas	<input checked="" type="checkbox"/>			
Adecuación de los destinatarios	<input checked="" type="checkbox"/>			
Eficacia para proporcionar los datos requeridos	<input checked="" type="checkbox"/>			
Modificaciones que haría a las preguntas <i>Ninguna</i>				



UNL

Universidad Nacional de Loja

Carrera de Pedagogía de las Ciencias Experimentales Informática

Validación del Instrumento

Nombre: *Rolando Galindo Sandoval*

1. Presentación

(Marque con una X su valoración)

	Excelente	Buena	Regular	Malo
Claridad del planteamiento	<input checked="" type="checkbox"/>			
Adecuación a los destinatarios	<input checked="" type="checkbox"/>			
Longitud del texto	<input checked="" type="checkbox"/>			
Calidad de contenido (redacción)	<input checked="" type="checkbox"/>			
Modificaciones que haría a la presentación <i>Organizar la información para que quede claro sobre una hoja en una página, no se corte la información. Presentación del instrumento (hoja)</i>				

2. Instrucciones para el proceso de respuesta

(Marque con una X su valoración)

	Excelente	Buena	Regular	Malo
Claridad	<input checked="" type="checkbox"/>			
Adecuación	<input checked="" type="checkbox"/>			
Cantidad	<input checked="" type="checkbox"/>			
Calidad	<input checked="" type="checkbox"/>			
Modificaciones que haría a las instrucciones <i>Preguntas</i>				

3. Preguntas del cuestionario

(Marque con una X su valoración)

	Excelente	Buena	Regular	Malo
Orden lógico de presentación	<input checked="" type="checkbox"/>			
Claridad en la redacción	<input checked="" type="checkbox"/>			
Adecuación de las opciones de respuesta	<input checked="" type="checkbox"/>			
Cantidad de preguntas	<input checked="" type="checkbox"/>			
Adecuación de los destinatarios	<input checked="" type="checkbox"/>			
Eficacia para proporcionar los datos requeridos	<input checked="" type="checkbox"/>			
Modificaciones que haría a las preguntas <i>Preguntas</i>				



UNL

Universidad Nacional de Loja

Carrera de Pedagogía de las Ciencias Experimentales Informática

Validación del instrumento

Nombre: Milton Fabauda J.

1. Presentación

(Marque con una X su valoración)

	Excelente	Buena	Regular	Malo
Claridad del planteamiento	X			
Adecuación a los destinatarios	X			
Longitud del texto	X			
Calidad de contenido (redacción)	X			
Modificaciones que haría a la presentación				
NINGUNA				

2. Instrucciones para el proceso de respuesta

(Marque con una X su valoración)

	Excelente	Buena	Regular	Malo
Claridad	X			
Adecuación	X			
Cantidad	X			
Calidad	X			
Modificaciones que haría a las instrucciones				
NINGUNA				

3. Preguntas del cuestionario

(Marque con una X su valoración)

	Excelente	Buena	Regular	Malo
Orden lógico de presentación	X			
Claridad en la redacción	X			
Adecuación de las opciones de respuesta	X			
Cantidad de preguntas	X			
Adecuación de los destinatarios	X			
Eficacia para proporcionar los datos requeridos	X			
Modificaciones que haría a las preguntas				
NINGUNA				



unl

Universidad Nacional de Loja

Carrera de Pedagogía de las Ciencias Experimentales Informática

4. Valoración general del cuestionario

(Marque con una X su valoración)

	Excelente	Buena	Regular	Malo
Validez de contenido del cuestionario	X			
Percepción general sobre el cuestionario				
ES UN INSTRUMENTO VÁLIDO Y ADECUADO PARA LA INVESTIGACIÓN				

Observaciones y recomendaciones

NINGUNA

Gracias por su valioso aporte a esta investigación

Anexo 3.
Instrumento.



UNL

Universidad Nacional
de Loja

Facultad
de la Educación,
el Arte y la
Comunicación

Carrera de
Pedagogía de las Ciencias
Experimentales Informática

Diagnóstico de los riesgos del uso de internet de la guía del Ministerio de Educación del Ecuador para estudiantes de BGU

¡Estimada estudiante!

Reciba un cordial saludo a nombre de la carrera de Pedagogía de las Ciencias Experimentales Informática de la Universidad Nacional de Loja, como estudiante de la misma tengo el grato honor de dirigirme a usted para solicitar su valiosa colaboración en el desarrollo de la presente encuesta cuyo como objetivo es diagnosticar los riesgos del uso de internet a partir de la guía del Ministerio de Educación del Ecuador (2018), para prevención de riesgos durante el uso de internet y dispositivos tecnológicos en el tercer año de bachillerato general unificado de la Unidad Educativa Fiscomisional La Inmaculada en el año lectivo 2022 – 2023. De antemano agradezco su gentil ayuda. Cabe mencionar que la información recolectada es confidencial y para fines académicos.

Marque con una X según corresponda:

1. Información general

1.1 Edad (años)	16-18	20 o más
	<input type="checkbox"/>	<input type="checkbox"/>

2. Diagnóstico de los riesgos del uso de internet de la guía del Ministerio de Educación del Ecuador.

Marque con una X en el casillero del número que mejor refleje su opinión considerando la frecuencia de Likert del 1 al 3, siendo el número 1 "Nunca" y el número 3 "Siempre", basado y adaptado de la Guía del Ministerio de Educación (2018).

NUNCA	OCASIONALMENTE	SIEMPRE
1	2	3

Las preguntas también requerirán una respuesta de sí o no, por lo que marque con X en la opción que mejor refleje su situación.

2.1 Dimensión I. Trata de personas

Marque con una (X) según corresponda.

Dimensión I. Trata de personas. Consiste en la explotación violenta de seres humanos para el beneficio/ lucro propio o de un tercero, mediante manipulación, coerción y limitación de la libertad individual.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa le ha brindado información acerca de la trata de personas?			
Actividades de la trata de personas		SI	NO
¿Reconoce la explotación violenta de seres humanos con fines de lucro, ya sea para beneficio propio o de terceros, como un caso de trata de personas?			
¿Reconoce la explotación violenta de seres humanos mediante manipulación, restricción y limitación de la libertad individual como trata de personas?			
¿Reconoce la explotación violenta en el entorno familiar como trata de personas?			

2.2 Dimensión II. Flamming.

Marque con una (X) según corresponda.

Dimensión II. Flamming. Es una forma de ciberacoso a través de la utilización de un lenguaje intimidatorio, violento, vulgar o soez.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha brindado información acerca del fenómeno flaming?			
Actividades del flaming		SI	NO
¿Está al tanto de que el uso de un lenguaje intimidatorio, violento, vulgar o soez en internet se denomina como flaming?			
¿Reconoce que el flaming constituye una forma de ciberacoso?			
¿Considera que el flaming se ha normalizado al usar internet?			

2.3 Dimensión III. Grooming.

Marque con una (X) según corresponda.

Dimensión III. Grooming. Ocurre cuando una persona adulta manipula a menores de edad con el fin de ganar su confianza y obtener videos o fotos de carácter sexual.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha proporcionado información sobre el grooming?			
Reconocimiento del grooming		SI	NO
¿Está usted familiarizado con el término grooming?			
¿Reconoce que el grooming sucede cuando un adulto manipula a menores de edad con la finalidad de obtener imágenes o videos de contenido sexual?			
¿Reconoce al grooming como el compartir imágenes explícitas en la web ?			

2.4 Dimensión IV. Hacking.

Marque con una (X) según corresponda.

Dimensión IV. Hacking. Se trata de una intervención o alteración de sistemas informáticos, realizada con el objetivo de robar datos personales y/o financieros.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha brindado información acerca del "hacking"?			
Hacking		SI	NO
¿Está usted al tanto de que el objetivo del hacking es acceder ilegalmente a sistemas informáticos para robar datos personales?			
¿Reconoce que el hacking se pueda utilizar para cometer delitos y poner en riesgo la privacidad y seguridad de las personas?			
¿Le preocupa la seguridad de tus datos personales en línea y la posibilidad de que puedan ser robados?			

2.5 Dimensión V. Harassment.

Marque con una (X) según corresponda.

Dimensión V. Harassment. Se define como la reiteración de amenazas, insultos, frases denigrantes y humillaciones mediante mensajes o llamadas. Incluye además la divulgación de fotos o rumores violentos en la red. También se conoce como ciberacoso o cyberbulling.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha brindado información acerca del "harassment"?			
Harassment		SI	NO
¿Está usted familiarizado con que la repetición de amenazas, insultos, frases denigrantes y humillación a través de mensajes o llamadas se conoce como harassment?			
¿Está usted al tanto de que el "harassment" puede ser definido como un comportamiento agresivo hacia otra persona en internet?			
¿Reconoce que el harassment puede tener un impacto negativo en la salud mental y el bienestar de las personas que lo sufren?			

2.6 Dimensión VI. Phishing.

Marque con una (X) según corresponda.

Dimensión VI. Phishing. Se define como la difusión de mensajes falsos en Internet, diseñados para usurpar o robar datos de cualquier tipo.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha brindado información acerca del phishing?			
Phishing		SI	NO
¿Está al tanto de que el phishing es una técnica que busca engañar a los usuarios para que revelen información personal o confidencial?			

¿Cree usted que el phishing puede ser un riesgo significativo para la privacidad y seguridad en línea de los usuarios?		
¿Reconoce que, en las redes sociales existe un mayor riesgo de caer en el phishing, al no cuidar la información que se expone?		

2.7 Dimensión VII. Pornografía infantil.

Marque con una (X) según corresponda.

Dimensión VII. Pornografía infantil. Abarca cualquier representación o imagen de una niña o un niño involucrados en actividades o situaciones de carácter sexual, reales o simuladas.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha brindado información acerca de la pornografía infantil?			
Pornografía infantil		SI	NO
¿Está usted al tanto de que cualquier representación o imagen, ya sea real o simulada, de un niño o niña involucrado en situaciones de índole sexual se considera pornografía infantil?			
¿Reconoce que la posesión, distribución o producción de material de explotación sexual infantil es un delito y puede resultar en consecuencias graves para los infractores?			
¿Reconoce que, en las redes sociales existe un mayor riesgo de publicar fotografías de infantes inapropiadas que pueden ser utilizadas para la pornografía infantil?			

2.8 Dimensión VIII. Sexting.

Marque con una (X) según corresponda.

Dimensión VIII. Sexting. Supone una forma de violencia en la que un remitente produce y envía mensajes, imágenes o videos con contenidos sexuales no deseados a la víctima.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha proporcionado información acerca del sexting?			
Sexting		SI	NO

¿Está usted familiarizado con que la producción y envío de mensajes, imágenes o videos con contenido sexual no solicitados por la víctima se denomina sexting?		
¿Reconoce usted que la educación sobre el consentimiento puede ayudar a prevenir los riesgos asociados con el sexting?		
¿Está al tanto de los riesgos asociados con el sexting, como la difusión no consentuada de imágenes?		

2.9 Dimensión IX. Sextorsion.

Marque con una (X) según corresponda

Dimensión IX. Sextorsion. Se define como una extorsión bajo la amenaza de publicar fotografías o videos sexuales de la víctima.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha proporcionado información acerca de la Sextorsion?			
Sextorsion		SI	NO
¿Está usted al tanto de que la amenaza de publicar fotografías o videos de carácter sexual se conoce como "sextorsión"?			
¿Está al tanto de qué es la sextorsión y cómo se lleva a cabo?			
¿Considera usted a la sextorsión como un peligro al compartir fotografías explícitas a desconocidos?			

2.10 Dimensión X. Stalking.

Marque con una (X) según corresponda.

Dimensión X. Stalking. Implica un acoso reiterado y agresivo, ejercido con la finalidad de amedrentar, intimidar y atemorizar a la víctima.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha proporcionado información acerca del stalking?			
Stalking		SI	NO
¿Usted está familiarizado con que el acoso persistente y agresivo, llevado a cabo con el propósito de intimidar, amedrentar y causar			

temor a la víctima, se conoce como stalking?		
¿Está usted al tanto de qué es el stalking y cómo se lleva a cabo?		
¿Considera usted el stalking como un peligro para los menores de edad que navegan en la web sin supervisión?		

2.11 Dimensión XI. Suplantación de identidad.

Marque con una (X) según corresponda.

Dimensión XI. Suplantación de identidad. Supone la apropiación y suplantación de la identidad de una persona por parte de otra, con el fin de acceder a recursos y beneficios económicos, jurídicos, etc.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha proporcionado información acerca de la suplantación de identidad?			
Suplantación de identidad		SI	NO
¿Está usted al tanto de que la apropiación de la identidad de una persona por parte de otra con el fin de acceder a recursos y beneficios económicos o jurídicos se considera suplantación de identidad?			
¿Conoce usted que la suplantación de identidad puede afectar a las víctimas al apropiarse de su información personal o financiera?			
¿Usted considera que la suplantación de identidad afecta la honra de la víctima?			

2.12 Dimensión XII. Delitos por medio digitales.

Marque con una (X) según corresponda.

Dimensión XII. Delitos por medios digitales. Resume las diferentes formas de apropiación y utilización de la imagen de una persona sin su consentimiento.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha proporcionado información acerca de los delitos por medios digitales?			
Delitos por medios digitales		SI	NO
¿Está al tanto de que las diversas formas de apropiarse y utilizar la			

imagen de una persona sin su consentimiento constituyen delitos por medio digital?		
¿Considera usted que los delitos por medios digitales afectan de múltiples formas a las víctimas?		
¿Usted considera que los delitos por medios digitales atentan en contra de la privacidad de lo que se publica en las redes sociales?		

2.13 Dimensión XIII. Lolicon/shotacon.

Marque con una (X) según corresponda.

Dimensión XIII. Lolicon/shotacon. Es un tipo de producción ilustrada/animada en formato manga o anime en la que niños (Shotacon) o niñas (Lolicon) son representados en relaciones implícita o explícitamente sexuales con adultos.	ALTERNATIVAS DE RESPUESTA		
	1	2	3
¿La institución educativa ha proporcionado información acerca del lolicon/shotacon?			
Lolicon/shotacon		SI	NO
¿Está usted familiarizado con el término lolicon/shotacon, que se refiere a la producción ilustrada o animada en forma de manga o anime en la que los niños son representados en relaciones sexuales implícitas o explícitas con adultos?			
¿Estás al tanto de que este tipo de producciones ilustradas o animadas son contenido ilegal relacionado con la explotación sexual infantil?			
¿Usted considera que el lolicon/shotacon normaliza la representación de niños en el ámbito sexual?			

MUCHAS GRACIAS

Referencia:

Ministerio de Educación del Ecuador (2018). Guía para Prevención de Riesgos durante el uso de internet y dispositivos tecnológicos. https://recursos.educacion.gob.ec/wp-content/uploads/Eugenia/Guias/GUIA_BACHILLERATO.pdf

Anexo 4.

Certificación de traducción del resumen.



Loja, 07 de mayo de 2024

Lic. Karina Yajaira Martínez Luzuriaga

LICENCIADA EN CIENCIAS DE LA EDUCACIÓN MENCIÓN INGLÉS

CERTIFICO:

Yo, Karina Yajaira Martínez Luzuriaga con cédula de identidad Nro. 1104902679, Licenciada en Ciencias de la Educación Mención Inglés por la Universidad Técnica Particular de Loja, con número de registro 1031-2022-2574017 en la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación, señalo que el presente documento es fiel traducción del idioma español al idioma inglés del resumen del Trabajo de Integración Curricular denominado "Diagnóstico de los riesgos del uso de internet de la guía del Ministerio de Educación del Ecuador para prevención de riesgos durante el uso de internet y dispositivos tecnológicos en el tercer año de bachillerato general unificado de la Unidad Educativa Fiscomisional La Inmaculada en el año lectivo 2022 - 2023." elaborado por el Sr. Pablo Gabriel Vargas Barragán, con cédula de identidad Nro. 1106081720, estudiante egresado de la carrera de Pedagogía de las Ciencias Experimentales Informática de la Universidad Nacional de Loja.



Lic. Karina Yajaira Martínez Luzuriaga

C.I. 1104902679

REGISTRO SENESCYT N°: 1031-2022-2574017