PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE EDUCACIÓN

Percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana

Tesis para obtener el título profesional de Licenciado en Educación con especialidad en Educación Primaria que presenta:

Michael Santiago Bautista Altamirano

Asesora:
Roxana Vanessa Villa Longa

Lima, 2022

AGRADECIMIENTOS

Le agradezco en especial a Dios, quien me brindó las fortalezas para concluir con la elaboración de este trabajo investigativo, por cuidarme y guiarme a lo largo de mis estudios profesionales y brindarme una vida llena de experiencias de aprendizaje.

A todos mis familiares, amigos y docentes de la carrera de educación de la PUCP por el apoyo incondicional, por confiar en mis capacidades y por apoyarme en los momentos más difíciles.

Asimismo, quiero expresar mi agradecimiento a los estudiantes del 6to grado A del turno mañana, quienes participaron en este estudio, por su predisposición, apoyo y tiempo.

Finalmente, agradecer a mi asesora Roxana Villa Longa, quien me guió y orientó en todo este proceso de investigación, por su paciencia, actitud y confianza mostrada hacia mis habilidades.

RESUMEN

El presente trabajo de investigación se centra en las percepciones de los estudiantes de 6to grado sobre sus competencias en seguridad. En la actualidad, a causa del COVID-19 se observa una mayor demanda por utilizar las TIC, así como una mayor presencia en el mundo digital por parte de los alumnos, lo cual ha representado una mayor exposición y riesgo a que se vulnere su derecho a la protección de sus datos personales, privacidad y salud. En base a ello, el objetivo general del estudio es analizar las percepciones de los estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana, y como objetivos específicos se plantea los siguientes: (1) Describir las percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana y (2) describir el nivel de competencias digitales en seguridad. Para ello, se emplea el enfoque cualitativo de tipo descriptivo, pues nos permite describir de forma sistemática el nivel de percepción que poseen los estudiantes sobre sus competencias en seguridad del proyecto DIGCOMP. Una de las conclusiones que se ha llegado es que los estudiantes mencionados tienen un nivel de percepción intermedio sobre las competencias en torno a la protección de datos personales y salud. Por tanto, es importante seguir promoviendo la formación de estas competencias desde la educación básica regular, a fin de que todo niño navegue y utilice las TIC de forma responsable y segura.

Palabras clave: Seguridad, redes sociales, competencia digital, protección de datos personales y privacidad, protección de la salud y bienestar.

ABSTRACT

This research work focuses on the perceptions of 6th grade students about their safety skills. Currently, due to COVID-19, there is a greater demand for using ICT, as well as a greater presence in the digital world by students, which has represented greater exposure and risk of their rights being violated. to the protection of your personal data, privacy and health. Based on this, the general objective of the study is to analyze the perceptions of 6th grade students about their digital skills in security in a public educational institution in Metropolitan Lima, and the following are proposed as specific objectives: (1) Describe the perceptions of 6th grade students about their digital security skills in a public educational institution in Metropolitan Lima and (2) describe the level of digital security skills. For this, the descriptive qualitative approach is used, since it allows us to systematically describe the level of perception that students have about their DIGCOMP project security skills. One of the conclusions that has been reached is that the related users have an intermediate level of perception about the competences around the protection of personal data and health. Therefore, it is important to continue promoting the training of these skills from regular basic education, so that every child navigates and uses ICTs responsibly and safely.

Key words: Security, social networks, digital competence, personal data protection and privacy, health protection and well-being.

ÍNDICE

INTRODUCCIÓN

La presente investigación se ha denominado “Percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana”. El interés por investigar este tema surge debido que en la actualidad con el avance de las tecnologías de la información y de la comunicación, el aprendizaje, la comunicación y el entrenamiento se encuentran sujetos a nuevos paradigmas mediados por las TIC y el internet, por lo que existe una mayor presencia de los niños en el mundo digital. Esta situación se ha visibilizado con mayor significatividad durante el contexto de la pandemia del Covid19, pues durante el 2020, el 94,2% de niños entre 6 a 11 años han empleado las TIC como un medio para dar continuidad a su aprendizaje y otras actividades académicas (Instituto Nacional de Estadística e Informática [INE], 2020).

Todo ello pone en evidencia que los niños se encuentran inmersos a diario en el internet y, en muchos casos, sin el acompañamiento o monitoreo por parte de sus padres. La presencia de estos en el mundo digital si bien puede representar mayores oportunidades para su aprendizaje, sin embargo, según Gamito, Aristizabal y Olasolo (2017) también representa un desafío en la protección se su seguridad, ya que cuando los estudiantes se encuentran a diario en el internet están expuestos y vulnerables a una serie de riesgos cibernéticos que puede afectar su imagen, conducta, identidad digital y salud.

En el 2020, en América Latina y España, el 33% de estudiantes, niños y adolescentes han sido víctimas de ciberbullying durante la cuarentena (Cedillo, 2020). Al respecto, en el Perú, según el informe del Foro Económico Mundial y DQ Institute, ponen de manifiesto que 6 de cada 10 niños de 8 a 12 años están expuestos a algún riesgo en internet (Ministerio de Salud [MINSA], 2020). Frente a esa situación, García, Salvador, Casillas y Basilotta (2019) sostienen que esta problemática se debe a que los estudiantes no cuentan con competencias, conocimientos y habilidades vinculados con la seguridad para utilizar de forma segura y responsable las TIC, así como para hacer frente de forma eficaz a los diferentes peligros digitales que se encuentran.

Sobre la base del contexto descrito, se puede evidenciar la necesidad de que los alumnos desarrollen competencias digitales en seguridad, no solo para dar continuidad a su aprendizaje en medio de una transición de emergencia sino también para que les permita emplear las TIC y otras plataformas digitales de una forma crítica y segura, lo cual puede interferir de manera significativa en su proceso académico y social.

La competencia digital vinculada con la seguridad permite adquirir conocimientos, capacidades y actitudes en los niños en torno a la protección de la información y comunicación a fin de que ellos puedan responder de manera significativa a los problemas que genera el uso de las TIC (Gallego, Torres, Pessoa, 2019). Asimismo, el Marco Europeo de la Competencia Digital de la Comisión Europea (Carretero, Vourikari & Punie, 2017) a través del área de seguridad busca el desarrollo de cuatro competencias: protecting devices, protecting personal data and privacy, protecting health and well-being y protecting the environment. Mediante estas competencias los niños pueden ser más conscientes de los riesgos que se encuentran en el mundo digital, así como también puedan usar de forma responsable y segura las TIC (Castillejos, Torres y Lagunes, 2016).

En base a una revisión bibliográfica, se encontró trabajos investigativos internacionales que abordan este tema, tal como el estudio desarrollado en España por Martínez, Gewerc, Rodríguez (2019), el cual tuvo como objetivo identificar, analizar, comprender y evaluar las competencias digitales (del modelo DigComp, Digital Competences) que poseen 764 alumnos del sexto grado del nivel primario de la comunidad autónoma de Galicia-España. Los hallazgos obtenidos en esta investigación, específicamente, con relación a la competencia vinculada con la seguridad concluyeron que, el 17,6% de los estudiantes de esta comunidad de España se encuentran en un nivel bajo, mientras el 48,8% presentan un nivel intermedio y solo el 31,1% se encuentran en un nivel avanzado.

En el contexto peruano, podemos describir el estudio realizado por Orosco, Gómez, Pomasunco, Salgado y Álvarez (2020), el cual tuvo como objetivo identificar las competencias digitales de 665 estudiantes del nivel secundaria de los colegios públicos de una provincia de la región central del Perú, concluyeron que el 61, 8% de los alumnos presentan un nivel de logro esperado en el área de seguridad, pues

el 48% obtuvo un nivel de logro esperado en las competencias sobre protección de dispositivos, de datos personales e identidad digital, de la salud y protección del entorno. Cabe señalar que los estudios realizados con relación a competencias digitales en seguridad en nivel primario en el Perú son escasos.

En esa línea, está investigación tiene como finalidad dar a conocer las percepciones de los estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad y el respectivo nivel de dominio (básico, intermedio y avanzado), pues a partir del reconocimiento de estas, podrán buscar estrategias para adquirir o fortalecer aquellas competencias que no han desarrollado. De esta manera, no solo se busca responder a los riesgos o desafíos que presentan las TIC, sino también a que puedan ser cibernautas competentes y responsables.

A partir de lo expuesto, este estudio está enfocado en responder la pregunta ¿Cuáles son las percepciones de los estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana? Las competencias que se evaluaron son parte del área de seguridad que conforma la competencia digital perteneciente al marco europeo de competencia digital (DIGCOMP).

Los objetivos que se han planteado para dicho estudio son los siguientes: en primer lugar, el objetivo general es analizar las percepciones de los estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana; en segundo lugar, se formularon dos objetivos específicos, por un lado, describir las percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad y, por otro lado, describir el nivel de competencias digitales en seguridad.

El enfoque metodológico de esta investigación es cualitativo del tipo descriptivo, ya que según Quecedo y Castaño (2002), su propósito es evitar la cuantificación y basarse principalmente en generar datos descriptivos de los fenómenos o eventos que son estudiados, para ello, emplea una serie de técnicas e instrumentos que generan datos descriptivos.

Las técnicas que se emplearon para la investigación fue la entrevista semiestructurada y una encuesta virtual dirigida a 10 estudiantes del 6to grado “A” del turno mañana, la cual permitió obtener información necesaria para responder a la pregunta de investigación como a los objetivos planteados.

Teniendo en cuenta lo descrito, la presente investigación se estructura en dos partes. En la primera, se presenta el marco teórico. Este expone dos capítulos, el primero relacionado con la percepción de los estudiantes sobre las competencias digitales en seguridad. En el segundo capítulo, se desarrolla la seguridad como competencia digital del siglo XXI en una educación no presencial. En la segunda parte, se presenta la parte de investigación, el cual expone en primer lugar, el diseño metodológico y, en segundo lugar, el análisis e interpretación de resultados. Luego de ello, se presentan las conclusiones, recomendaciones, referencias y anexos.

Finalmente, dentro de las limitaciones que se presentaron en este estudio se precisan básicamente dos: la primera relacionada con los criterios seleccionados para definir el nivel de percepción de cada estudiante sobre sus competencias en seguridad, pues las descripciones de los niveles son más precisas y claras; mientras que la segunda limitación que se registró fue en torno a las dificultades que mostraron los estudiantes al responder tanto las preguntas de la entrevista como la encuesta, lo cual puede interferir de alguna manera en la definición de sus niveles de percepción.

PRIMERA PARTE: MARCO TEÓRICO

Capítulo 1: Percepciones de los estudiantes sobre las competencias digitales en seguridad

Hoy en día, la tecnología y las tecnologías de la información y de la comunicación [en adelante TIC] mediados por el Internet se han transformado en una herramienta esencial en la sociedad, pues los servicios y beneficios que ofrecen a la ciudadanía facilitan el desarrollo óptimo de las diversas actividades sociales, de esta manera, contribuyen con la mejora de los diferentes ámbitos sociales. En el ámbito educativo, las TIC se han ido incorporando gradualmente como un complemento que contribuye en el desarrollo académico de los niños, así como en la gestión de las instituciones educativas y las relaciones interpersonales de la comunidad educativa, pero no como una herramienta indispensable.

Sin embargo, la actual coyuntura a causa del coronavirus (COVID-19) ha generado un cambio repentino en las actividades sociales, económicas y, sobre todo, educativas, debido al confinamiento social adoptado como estrategia por los diferentes países del mundo con el objetivo de evitar la propagación del virus (Naciones Unidas, 2020). Esta situación ha exigido a los estudiantes emplear las TIC para dar continuidad a su aprendizaje remoto, así como para realizar diversas actividades de entretenimiento digital, acceso a la información y comunicación. Todo ello, hace que ahora permanezcan más tiempo de lo usual frente a las pantallas. Por tal motivo, las TIC, hoy en día, han pasado de ser consideradas como una posibilidad a convertirse en una necesidad indispensable en tiempos de emergencia.

Este nuevo contexto de la tecnología, si bien puede representar mayores oportunidades y beneficios de aprendizaje en los niños, también puede significar una mayor exposición a los riesgos en las redes sociales y en el Internet por el acceso libre y poco control por parte de los padres sobre el uso de estos (Gonzáles, 2013). Frente a ello, el Fondo de las Naciones Unidas para la Infancia (UNICEF, 2020) manifiesta que resulta necesario dotar en habilidades digitales a los estudiantes con el fin de que puedan interactuar de forma segura y significativa en el

Internet; es decir, se requiere trabajar en la adquisición y fortalecimientos de competencias digitales en materia seguridad, ya que el desarrollo adecuado de estos puede prevenir futuros problemas en torno al uso excesivo e indebido del Internet (García-Umaña, 2017; García-Umaña y Tirado-Morueta, 2018, como se citó en García, Salvador, Casillas y Basilotta, 2019).

Debido a ello, el desarrollo de las competencias en seguridad resulta esencial en un contexto donde utilizan constantemente las TIC y están más propensos a sufrir algún tipo de riesgos cibernéticos. No obstante, para el desarrollo significativo y eficaz de estas competencias se requiere que existan marcos de referencia que precisen las competencias que deben desarrollar todo estudiante al término de su formación educativa y, de esta forma, sirva de base a los sistemas educativos para contar con estándares que concierne a las competencias digitales.

En ese sentido, en el presente capítulo se analizan los conceptos vinculados con la percepción y la competencia digital a la luz de diferentes autores. Asimismo, para los objetivos de este estudio, así como para tener una mejor comprensión del tema a tratar, se describen dos marcos de referencia entorno a las competencias digitales, tales como el marco europeo de competencias digitales para estudiantes (DIGCOMP) y la matriz de habilidades TIC para el Aprendizaje (HTPA). Cabe mencionar que el énfasis se centra en las competencias que presentan cada uno de estos marcos en materia de seguridad.

1.1. Definición de percepción desde la dimensión educativa

La percepción, según Fuenmayor y Villasmil (2008) es la parte esencial de la conciencia del ser humano, puesto que con ella definimos nuestra realidad en base a la interpretación de nuestras experiencias y cultura. Por tanto, la percepción se puede definir como el resultado del primer conocimiento o información que provienen de determinadas experiencias del ser humano.

Barthey (1982, como se citó en Arias, 2006), sostiene que la percepción es un proceso cognitivo de conocimiento de objetos, interpretación, hechos o verdades para la elaboración de juicios en torno a la experiencia sensorial y el pensamiento

obtenidas en el ambiente físico y social. Por su parte, Tolosa (2017) señala que la percepción es un proceso que forma parte del procesamiento de la información en el que la persona, antes de procesar las nuevas experiencias vividas que se almacenan en su conciencia, construye un gráfico informativo anticipatorio, que le permite contrastar organizar, interpretar y codificar el estímulo o datos sensorial con el objetivo de aceptarlo o rechazarlo según el propósito del gráfico.

La percepción desde la educación, en concreto desde la visión del estudiante, es como la primera imagen que se forma en el sujeto sobre un determinado estímulo cuando éste todavía no posee la información suficiente para la comprensión y para dar sentido a la información que quiere procesar e interpretar (Aguilar, 2010). Así pues, la percepción se define como la primera imagen mental que se desarrolla con la experiencia del niño. En otras palabras, es un proceso cognitivo que ayuda a seleccionar e interpretar la información que obtienen en los ambientes mediante estímulos físicos y sensaciones que son causados por los sistemas sensoriales.

En esa línea, esa línea, Pineda (2018) sostiene que la percepción tiene como objetivo precisar información con respecto a las experiencias que haya vivido en el medio ambiente para mantener la supervivencia, así como actuar en relación con el ambiente; dicho de otro modo, se centra en señalar determinada información sobre algún tema determinado a partir de la interacción y experiencias que desarrolla en el entorno, por lo cual estos pueden ser positivas o negativas.

En definitiva, la percepción es un proceso que permite crear distintas interpretaciones de la realidad de lo que ocurre en un ambiente a causa de los estímulos y sensaciones que provienen de las experiencias y recuerdos previos de cada sujeto, es decir de los órganos sensoriales. En tal sentido, la percepción que el estudiante posee sobre sus competencias digitales en seguridad va a influenciar de forma directa o indirecta las experiencias y recuerdos positivos y negativos que haya vivido durante el uso de las TIC y el Internet.

1.2. Definición de competencias digitales desde la dimensión educativa

Los avances de las nuevas tecnologías han conllevado al progreso de la sociedad del siglo XXI. Por ende, las TIC se han convertido en un recurso esencial para el crecimiento de las diferentes actividades académicas y sociales. Esta situación ha representado un desafío en los estudiantes para adaptarse a estos contextos, por lo que requieren contar con nuevas habilidades técnicas y cognitivas que les permita usar y aprovechar los beneficios que propicia esta herramienta y contrarrestar los nuevos retos que conlleva su uso. En respuesta a este contexto, la competencia digital adquiere un rol protagónico para la inserción en la sociedad digital, ya que permite emplear las TIC de forma significativa (Gisbert et al., 2016, como se citó en Chiecher, 2020).

Según la Organización para la Cooperación y el Desarrollo Económicos (OCDE,2020), la competencia digital en la sociedad del conocimiento es un elemento esencial que deben de desarrollar los estudiantes para que les permita adquirir habilidades, actitudes y conocimientos, y, de esa manera, mejorar el acceso a mejores oportunidades de enseñanza y aprendizaje en un espacio virtual, así como enfrentar los retos posteriores a los nuevos desarrollos tecnológicos. En el 2006, la Unión Europea definió y adoptó un marco de referencia que sustenta la necesidad de mejorar las aptitudes y competencias de los estudiantes, jóvenes y adultos para que puedan ejercer una ciudadanía activa e incluirse en las actividades sociales y laborales en la sociedad del conocimiento (Egido, 2011).

Para ello, propone ocho competencias claves y elementos transversales que deben adquirir todo estudiante durante su paso por la educación; ya que, estas son un conjunto de conocimientos, capacidades y destrezas que permite acceder a oportunidades para incorporarse al mundo académico, social y profesional, así como contribuye a la realización de los proyectos personales (Herreros, 2014). Para Rychen y Salganik (2003, como se citó en Coll, 2007) son competencias individuales que contribuyen al desarrollo integral de todo niño a fin de que aporten y participen de forma eficaz en el desarrollo de la sociedad y, de esa forma, tener éxito en la vida.

En esa línea, las ocho competencias que propone la Unión Europea podemos agruparlas en dos grupos, por un lado, competencias transversales, tales como sociales y cívicas; aprender a aprender; sentido de la iniciativa para el desarrollo empresarial y, finalmente, conciencia y expresión cultural. Por otro lado, competencias esenciales, tales como competencia en comunicación en la lengua materna y extranjera; en matemática; ciencia y tecnología, y "competencia digital" (Comisión Europea, 2007). Esta última competencia, para Cobo Romaní (2009, como se citó en García, 2013)," es una competencia transversal que contribuye a potenciar todas las demás competencias" (p. 12-13), pues integra conocimientos, habilidades y actitudes que se constituyen como elementos fundamentales para el bienestar de los alumnos. De esta manera, dicha competencia se transforma en una competencia clave y necesaria en la formación de los ciudadanos, en especial de los niños.

Así, a causa de este reconocimiento de las competencias digitales, en el 2006 la European Parliament and the Council introduce (como se citó en Ala Mutka, 2011), modifica su definición del 2004, indicando que implies the safe and critical use of ICT for work, leisure and communication, which is based on basic skills of technology for the use of computers in the development of activities such as recovering, evaluating, produce, present and exchange information, and communicate and participate in collaborative networks through the Internet.

En esta nueva definición de competencia digital, establece que las destrezas, conocimientos, capacidades y actitudes contribuyen a utilizar de forma responsable, segura y crítica el Internet y las TIC a fin de que puedan conseguir los objetivos vinculados al ámbito laboral, educativo, social, comunicativo y ocio (Muñoz, 2019).

Según Alonso (2011), la competencia digital comprende tres procesos: en primer lugar, el conocimiento, el cual permite comprender las aplicaciones y las oportunidades que brinda las TIC y el Internet; en segundo lugar, las habilidades para poder usar de manera apropiada los recursos digitales para desarrollar actividades como producir, comunicar, presentar, comprender, buscar y recoger información, asimismo, como para usar ordenadores tecnológicos como computadora, laptop, teléfono, entre otros. Por último, las actitudes para el manejo

de las TIC de forma independiente, crítica, reflexiva, significativa y responsable en la valoración de la información y los medios digitales. Es decir, para este autor la competencia digital está relacionada con las destrezas para el manejo de las TIC y el Internet y con el pensamiento lógico y crítico

En tal sentido, Gutiérrez (2014), sostiene que la definición de competencia puede clasificarse con relación a dos grandes perspectivas, por un lado, las que se enfocan la dimensión tecnológica y, por otro lado, las que enfatizan en la dimensión informacional o comunicativa, educativa y laboral (como se citó en González, Román, Prendes, 2018). Por esta razón, la competencia digital presenta diferentes conceptos de acuerdo a sus características y perspectivas de cada sector social, y que se modifica a medida que surgen las nuevas tecnologías, por lo que el concepto de esta competencia es interdisciplinar, pues se concibe desde la dimensión instrumental, psicológica, educativa y social.

En la esfera educativa, la competencia digital es entendida como un conjunto de destrezas y conocimientos que permite al estudiante emplear las TIC de una forma responsable y consciente para trabajar de manera colaborativa en la mejora de su aprendizaje y contribuir en el aprendizaje de los otros (Orosco, Gómez, Pomasunco, Salgado y Álvarez, 2021; Chavéz, Cantú y Rodríguez, 2016). En efecto, esto implica que pueden acceder, seleccionar y recuperar información digital de manera autónoma para realizar actividades educativas, así como crear y compartir contenidos educativos, resolver problemas digitales e iniciarse en los procesos de comunicación mediados por las redes sociales.

Para Mehboobe, Heidari, Farrokhnia y Noroozi (2021) They are multidimensional skills, knowledge and techniques on technology that allow the use of ICT in a meaningful way in the teaching and learning process. Por su parte, Marza y Cruz (2018, como se citó en Levano, Sanchez, Guillén, Tello, Herrera y Collantes, 2019) mencionan que dicha competencia son habilidades cognitivas, procedimentales y actitudinales que facilitan utilizar las TIC para mejorar su proceso académico de los alumnos, pues los recursos que brindan estos espacios pueden ayudar a consolidar o fortalecer ciertos aprendizajes.

Estas definiciones desarrolladas hacen hincapié en las habilidades, conocimientos y actividades para el uso y aplicación de las TIC para aportar de forma significativa en la mejora de sus actividades académicas en torno a las comunicativas, lingüísticas, matemáticas o científicas.

Sin embargo, otros autores como Orosco, Gómez, Pomasunco, Salgado y Álvarez (2021), sostienen que las competencias digitales no solo aportan habilidades o conocimientos para el manejo de las TIC y, por consiguiente, para colaborar a mejorar el aprendizaje de los estudiantes, sino también integran aspectos sociales y emocionales, los cuales contribuyen a adquirir habilidades intrapersonales e interpersonales, de escucha, gestión y expresión de las emociones, empatía, la capacidad de negociación y la creación de vínculos con sus pares.

En definitiva, la competencia digital entendida desde el panorama educativo es el conjunto de habilidades, actitudes y conocimientos que implican la capacidad de acceder y usar las TIC de forma significativa y segura para fortalecer su aprendizaje de los estudiantes, para comunicarse, investigar, analizar y transformar la información en conocimientos; por esa razón, esta competencia les debe facilitar en un futuro incorporarse al mundo social, académico, profesional y laboral.

A medida que los estudiantes desarrollan esta competencia, se van convirtiendo en un sujetos digitalmente competente, por lo que significa que estos deben being able and willing to keep up with the emergence of new technologies (Ferrari, Neza & Punie, 2014); además, have the ability to understand the media, adopt a critical, safe and responsible attitude towards the information, pages and technological resources that are accessed to enrich new skills (Ferrari, 2013, como se citó en Hazar, 2018).

Así pues, la competencia digital desempeña un papel indispensable en el aprendizaje sujeto a nuevos paradigmas mediados por los medios digitales y las TIC, por lo que la adquisición de estos debe comenzar desde una edad temprana en la educación formal (Caccuri, 2018). No obstante, el desarrollo de dicha competencia en los niños es un reto que no solo involucra a la educación, sino

también a la sociedad y, sobre todo, a la familia; ya que, de esta manera, es más probable una mayor aproximación al desarrollo integral de los estudiantes.

Por lo tanto, el sector educativo, tiene la misión de [..] “teach students how to use information effectively, interpret and use technology effectively, to benefit from technology in classrooms by supporting technology, and teaching the correct use of technology as a learning tool” (Kaware & Sain, 2015, como se citó en Hazar, 2018, p. 443). Como resultado de ello, se contribuye con el desarrollo y fortalecimiento de esta competencia, considerada necesaria y para afrontar los nuevos retos en torno al aprendizaje.

Por su parte, las familias son conscientes de la importancia de la tecnología para la formación integral y el proceso de aprendizaje. Por ello, su función, a fin de que los niños puedan adquirir o desarrollar esta competencia, se enfoca básicamente en la predisposición, por un lado, de adoptar el rol de guía para incentivar a los niños a emplear las TIC de forma responsable y, por otro lado, incorporar los recursos y dispositivos digitales y el internet en el hogar para acceder a las herramientas e información que proporciona las TIC (Sánchez, Andrés y Paredes, 2018). Sin embargo, Levano, Sanchez, Guillén. Tello, Herrera y Collantes (2019) consideran que para el desarrollo de las competencias digitales los estudiantes deben pasar por un proceso de formación respaldado por la alfabetización digital.

Cuando se aborda el término de alfabetización digital genera ciertas confusiones con respecto a la competencia digital en lo que respecta a sus conceptos, importancia, características y objetivos; de ahí que, es importante diferenciarlos.

El término de alfabetización digital presenta una gran diversidad de definiciones en relación al contexto cultural y tecnológico de acuerdo con cada época. Para Peñalva, Napal y Mendioros (2018) la alfabetización digital es la obtención de destrezas y dominios orientadas a emplear la información y comunicación, y no tanto en las habilidades para emplear las TIC. Mientras, Arrieta y Montes (2011), afirman que este término se define desde tres principios basado,

en primer lugar, en el uso de tecnología, el cual implica el manejo de programas y herramientas digitales por medio y uso de recursos tecnológicos como teléfonos, computadoras y tablets; en segundo lugar, la comprensión crítica de la misma, es decir, la capacidad para entender, analizar y evaluar los medios y contenidos digitales que se emplea. Finalmente, la creación y comunicación de contenido digital por medio de herramientas tecnológicas como páginas Web.

El objetivo de la alfabetización digital, se centra en la adquisición de habilidades con el propósito de que los niños puedan utilizar en su vida cotidiana las TIC, así como navegar en el Internet mediante ordenadores, y utilizar diversos recursos digitales en línea (Area, 2015). En otras palabras, la función de la alfabetización digital se enfoca en educar y adiestrar para utilizar el hardware y el software en un ambiente digital, por ello, es el punto de partida y factor clave para integrar las TIC.

Por las consideraciones anteriores, a diferencia de estos términos, desde la perspectiva de Ferrari et al. (2014, como se citó en Hazar, 2018), is that digital literacy is what provides the skills and knowledge to use ICT and, in this way, allows achieving digital competence. Vale decir, la alfabetización es el medio que permite adquirir la competencia digital. De la misma forma, la Fundación Telefónica (2015) sostiene que la alfabetización es la habilidad que contribuye, por medio de las competencias, utilizar las TIC de manera segura, responsable y crítica para alcanzar objetivos personales y sociales.

Es evidente entonces que estos dos términos se puede diferenciar con relación a la función que desempeñan cada uno en los entornos digitales; dicho de otra manera, la alfabetización digital tiene la función de desarrollar destrezas y dominios para el uso del internet y las TIC, incluidas las habilidades operativas y creativas; mientras la competencia digital tiene la función, a partir de esas habilidades, dominios, conocimiento y actitudes, contribuir en el manejo y uso de las TIC y el Internet de forma responsable, autónoma, segura, crítica y, sobre todo, mitigando los riesgos y optimizando las oportunidades para mejorar los diferentes sectores sociales, educativos, económicos y laborales.

1.3. Marco de referencias de competencias digitales en seguridad y niveles de dominio

Con el desarrollo y surgimiento de nuevas tecnologías digitales, el acceso a las TIC y al Internet por parte de los niños se viene produciendo desde tempranas edades, por lo que muchos de ellos necesitan contar con competencias, capacidades, conocimientos y habilidades a fin de que puedan utilizar forma segura, crítica y responsable, así como contrarrestar la exposición a una serie de riesgo cibernéticos. Frente a ello, la formación de los alumnos no puede quedar al margen de la nueva sociedad del conocimiento, por ende, surge la necesidad de que los estudiantes puedan ser competentes en el mundo digital por medio de la adquisición de desarrollo de diferentes competencias digitales, entre ellas la competencia digital vinculada a la seguridad (Gros y Contreras, 2006).

Esta competencia es considerada clave y transversal, por lo que todo niño, joven y adulto debería adquirirla no solo para poder acceder a las TIC, sino también para garantizar su utilización de forma adecuada y segura en el desarrollo académico y en otras actividades de la vida cotidiana. Alcanzar esta competencia significa poseer habilidades, conocimientos y actitudes para hacer frente a los riesgos que genera el mundo digital.

En ese sentido, la necesidad de educar y formar a los estudiantes en competencia digital en materia de seguridad es indispensable para mitigar los riesgos y mejorar las oportunidades que brinda las TIC. Al tratarse de una competencia transversal es tarea del sistema educativo poner los medios y recursos tecnológicos y humanos que posibiliten el desarrollo o fortalecimiento de dicha competencia. No obstante, para que las instituciones educativas puedan trabajar mediante el desarrollo de actividades diversificadas y contextualizadas, es importante que exista marcos de referencia sobre la competencia con relación a la seguridad, con el fin de que pueda servir como modelos de formación, diagnóstico o mejora de esta competencia.

Dadas las necesidades que anteceden, durante las últimas décadas se han desarrollado modelos para evaluar, acreditar y medir las competencias en seguridad

de las personas, alumnos y maestros. A nivel internacional podemos encontrar el marco europeo de competencias digitales (DIGCOMP). El surgimiento de dicho marco nace a partir del marco de referencia de competencias claves para el aprendizaje permanente y esencial presentado por la Unión Europea en 2006, con el objetivo de que los ciudadanos puedan participar de forma activa en la sociedad globalizada (Comisión Europea, 2007). Este marco presentó ocho competencias clave para la inclusión en los ámbitos sociales, laborales, económicos y académicos; entre estas se encuentra la competencia digital, siendo un elemento esencial para el manejo y uso de las TIC (Instituto Nacional de Tecnología Educativas y de Formación del Profesorado [INTEF], 2015).

A raíz de ello, en 2010, el Instituto de Prospectiva Tecnológica (IPTS) de la Comisión Europea, presentó por primera vez el borrador de la propuesta de marco de referencias de competencias digitales para la ciudadanía. En 2011, dicho marco se consolida a nivel europeo como parte del proyecto DIGCOMP, con el propósito de ayudar a que la población pueda comprender y desarrollar la competencia digital (González Fernández, 2015). Este marco según Punie, Neza & Ferrari, (2014), can serve as a reference for the development of educational curricula, certification and training programs and workshops around digital competence, where through a series of adaptation and diversification according to the social, cultural and cognitive context of students and people can be implemented this frame.

El modelo DIGCOMP proporciona detalladamente la descripción de todas las habilidades, conocimientos y actitudes que deben desarrollar los niños, jóvenes y adultos para ser competentes en los entornos digitales (Castillejos, Torres y Lagunes, 2016; Henriquez, Gisbert y Fernández, 2018). En esa línea, según García Varcárcel (2016) este marco tiene como objetivos:

- Identificar los conocimientos, habilidades y actitudes que contribuyen al sujeto a ser competente digitalmente.
- Proponer los descriptores por cada competencia a fin de formular un marco teórico general y poder validar los niveles de cada competencia.
- Desarrollar un plan de trabajo para determinar las acciones de monitoreo.

Desde la presentación del proyecto DIGCOMP, se han desarrollado cuatro informes que describen las áreas y competencias que conforman la competencia digital, y que podría funcionar como un modelo de referencia para diferentes iniciativas, proyectos, programas y currículos a nivel europeo. El último informe que presenta al marco de referencia de manera oficial es el DIGCOMP: a Framework for Developing and Understanding Digital Competence in Europe elaborada por Anusca Ferrari en el 2013 (González Fernández, 2015; García Valcárcel, 2016).

Dicho modelo establece cinco áreas competenciales que estructuran a la competencia digital: comunicación, información, creación de contenidos, resolución de problemas y seguridad. Además, por cada área se presenta una serie de competencias, siendo en total 21 competencias que todo ciudadano debe desarrollar para que se considere digitalmente competente; asimismo, se detallan tres niveles de dominio por cada área: básico, intermedio y avanzado (Comisión Europea, 2020; Ikanos, s.f).

Cada una de estas áreas constituye un elemento esencial para el desarrollo de la competencia digital, sin embargo, the areas of information, communication and content creation are specific competencies, so they need to be developed through activities that involve ICT mediated by the educational system, while security and problem solving are more transversal competences, which means that these can be developed in non-formal spaces; In other words, students are the main actor in their learning process where they can develop this competence naturally or work on them through participation in digital spaces (Punie, Neza & Ferrari, 2014).

Como resultado de ello, el marco DIGCOMP con relación al área de seguridad, aspecto central de este trabajo, propone el desarrollo de cuatro competencias. En la siguiente tabla se puede evidenciar con más detalle.

Tabla N° 1.
Áreas de seguridad del proyecto DIGCOMP.

	Competencias:
Área de seguridad	Proteger dispositivos
	Proteger datos personales y la privacidad
	Proteger la salud y el bienestar
	Proteger el medio ambiente

Fuente: Adaptado de la Comisión Europea, 2020; Ikano, s.f.

Cada competencia del área de seguridad se desarrolla por medio de tres niveles de dominio. En el dominio básico tenemos los niveles A1 y A2; en el intermedio se encuentran los niveles B1 y B2 y, por último, para el dominio avanzado se presentan los niveles C1 y C2. Cabe señalar que partes de estos tres niveles también presentan un dominio especializado a partir de los niveles D1 y D2. Para fines de este estudio, nos enfocaremos en desarrollar de manera específica dos de las cuatro competencias del área de seguridad considerando sus niveles de dominios: básico, intermedio y avanzado.

Las competencias que se presentan a continuación fueron seleccionadas debido a que estas responden a las problemáticas que generan mayor impacto en los estudiantes de 6to grado de primaria de una institución educativa de Lima Metropolitana cuando utilizan las redes sociales y el internet, por lo que conocer en qué nivel de dominio de sus percepciones se encuentran es una prioridad para plantear actividades y recursos que puedan contribuir al desarrollo de conocimientos, habilidades y actitudes en materia de seguridad.

- **Proteger datos personales y la privacidad:** Esta competencia se define como la capacidad para comprender cómo emplear y compartir datos personales o sensibles sin exponerse a sí mismo y a otros. Los niveles de esta competencia se pueden describir en la siguiente tabla:

Tabla N° 2.
Niveles de dominio

Básico	- Soy consciente de que sólo puedo compartir cierto tipo de información sobre mí mismo/a y sobre otras personas. - Conocimiento sobre qué tipos de información personal no se debe compartir en Internet. - Conocimiento de riesgos y consecuencias que puede generar utilizar inadecuadamente las redes sociales y el internet (como compartir información personal y de los demás). - Conocimientos sobre formas básicas para proteger su información personal y privacidad en los espacios digitales, garantizando su autoprotección y de terceros de peligros digitales. - Capacidades básicas para seleccionar qué tipo de información personal no se debe publicar en las redes sociales para proteger la identidad. - Actitud de prudencia en relación con los aspectos de privacidad hacia sí mismo y hacia los demás.
Intermedio	- Puede proteger mi propia privacidad y la de otras personas en internet y las redes sociales. - Comprendo de forma general sobre las cuestiones de privacidad tengo un conocimiento básico de cómo se guardan y utilizan mis datos. - Conocimiento sobre la importancia de la huella digital en las redes sociales e internet y el uso que pueden hacer terceras personas. - Conocimiento sobre el uso que pueden hacer terceras personas de su identidad digital. - Capacidad para localizar información en Internet y las redes sociales sobre sí mismo. - Conocimiento de estrategias para proteger la identidad en las redes sociales y de los riesgos en internet. - Actitud respetuosa de los principios de privacidad en internet y la red social, tanto la personal como la de otros.
Avanzado	- A menudo cambio la configuración de privacidad predeterminada por defecto de los servicios en línea para mejorar la protección de mi privacidad. Comprendo de forma amplia sobre los problemas de privacidad y sé cómo se guardan y utilizan mis datos. - Conocimiento de las ventajas de tener múltiples perfiles digitales para diferentes usos de la Red. - Conocimiento de estrategias para proteger los datos de otras personas que se aplican en su propio contexto. - Capacidad de cuidar y mejorar la identidad digital - Capacidad de modificar o eliminar información sobre sí mismo o de otras personas de los que es responsable en el internet y las redes sociales. en el mundo digital. - Actitud crítica cuando muestra información en línea sobre sí mismo y de otras personas. - Conocimiento sobre el uso de datos personales por los proveedores de servicios online con fines comerciales.

Fuente: Adaptado de Ikano (s.f, como se citó en Comisión Europea, 2020); Valcárcel, Salvador, Casillas y Gómez (2019).

- **Proteger la salud y el bienestar:** Esta competencia se define como la capacidad de evitar peligros que afecten la salud y el bienestar físico y psicológico del niño cuando emplea las TIC, así como la capacidad de

protegerse a uno mismo y a los demás frente a riesgos en los entornos digitales; además, se entiende como habilidad para conocer las nuevas tecnologías que permite la inclusión y el bienestar social. Los niveles de esta competencia se pueden describir en la siguiente tabla:

Tabla N° 3.
Niveles de dominio

Básico	- Prevenir riesgos que afecte a la salud, en específico, a la integridad física y el bienestar psicológico, ocasionados por el ciber-acoso y el uso de la tecnología. - Capacidad para emplear medidas básicas preventivas para protegerse a sí mismo del ciberacoso. - Conocimiento de las consecuencias por el uso constante de las tecnológicas (tiempo invertido en uso de internet, problemas auditivos y visuales, posturas). - Conocimiento de las consecuencias y causas del ciber-acoso. - Capacidad de establecer relaciones interpersonales por medio de las redes sociales. - Actitud de respeto, tolerancia y aceptación de las diferencias entre los usuarios.
Intermedio	- Sé cómo protegerme a mí mismo y a otras personas del ciberacoso y comprendo los riesgos que afecta a la salud originados por el uso de tecnologías (desde los aspectos ergonómicos hasta la adicción a las tecnologías). - Conocimiento sobre medidas preventivas para protegerse a sí mismo y a otros del ciberacoso - Conocimiento de los riesgos que genera el uso de tecnologías digitales para la salud. - Conocimientos de pautas saludables (ejemplo: ergonómicas, visuales, tiempos, auditivos. etc.) para el uso correcto de las tecnologías. - Capacidad para actuar preventivamente en relación con el ciber-acoso. - Actitud de prevención para evitar el ciberacoso.
Avanzado	- Estoy al tanto del uso correcto de las tecnologías para evitar problemas de salud. Sé cómo encontrar un buen equilibrio entre el mundo en línea y el mundo tradicional. - Capacidad para evitar los elementos distractores que generan pérdida de tiempo cuando navegan por el internet. - Capacidad para emplear estrategias que permitan evitar consecuencias dañinas del uso de las tecnologías. - Actitud crítica frente al uso inadecuado de las tecnologías (tipo de información que se consulta, contenidos inapropiados, dispositivos, etc. - Capacidad para emplear conductas saludables en el uso de dispositivos tecnológicos (volumen adecuado de altavoces, tamaño adecuado del texto, iluminación del dispositivo, etc.). - Actitud de comprensión frente a las estrategias que emplean los padres y maestros en el uso de las tecnologías.

Fuente: Adaptado de Ikano (s.f, como se citó en Comisión Europea, 2020); Valcárcel, Salvador, Casillas y Gómez (2019).

En contraste, a nivel Latinoamérica, debido a la falta de un marco de referencia de competencias digitales que pueda ser utilizado en todo el continente,

cada país ha desarrollado sus propias iniciativas (Henriquez, Gisbert y Fernández, 2018). Entre ellas se encuentra Chile, quien en el 2008 por medio del Centro de Educación y Tecnología del Ministerio de Educación propuso la matriz de Habilidades TIC para el Aprendizaje (HTPA), el cual se define como la habilidad y capacidad de solucionar problemas, por un lado, con relación a la información, comunicación y conocimiento y, por otro lado, dilemas sociales, legales y éticos en entornos digitales (Ministerio de Educación de Chile [MINEDUC], 2013).

En 2013, esta matriz pasó por un proceso de actualización, donde se definió un nuevo objetivo, el cual se basa en orientar y alinear el diseño de la política educativa orientada a la medición y desarrollo de un conjunto de habilidades en TIC, con el propósito de que los sistemas escolares puedan emplearlos para fortalecer el desarrollo académico de los estudiantes (Ascencio, 2017; Mineduc, 2013). Esta propuesta define cuatro dimensiones organizadas en 9 subdimensiones, 20 habilidades y definiciones operacional, que todo alumno debe desarrollar durante su pasó por la educación básica regular para que le permita emplear las TIC de forma significativa en el mundo digital. Dichas dimensiones son: información; comunicación y colaboración; convivencia digital, y tecnología.

En relación con las competencias digitales en seguridad, la dimensión que aborda dichas competencias es la convivencia digital. Esta dimensión propone la adquisición de destrezas con el objetivo de contribuir a la formación ética de los niños; asimismo, mediante ello se busca que los alumnos puedan aprender e interactuar con otros en entorno digitales y contrarrestar las situaciones riesgosas que se genera en esos espacios (Gasser, Maclay, & Palfrey, 2010, como se citó en Mineduc, 2013).

Las subdimensiones que se presentan en esa dimensión son: TIC y sociedad y ética y autocuidado. Esta última, es la que se centra más en la seguridad, pues la habilidades, conocimientos y actitudes que se deben desarrollar permiten reconocer ventajas y peligros en internet, aplicar y definir estrategias que garanticen la protección de la identidad y datos personales, así como respetar la propiedad intelectual de los otros (Salinas, Jara, San Martín, Claro y Cortés, 2016; Mineduc, 2013).

A diferencia del proyecto DIGCOMP, el HTPA no presenta niveles de dominio por cada subdimensión, es decir, solo describe de manera general qué habilidades deben desarrollar los estudiantes en materia de seguridad. Por tal motivo, para fines de este estudio investigativo se utiliza el marco de referencia de competencias digitales, pues nos permite identificar en qué nivel de las dos competencias seleccionadas del área de seguridad se encuentran las percepciones de los estudiantes del nivel primaria.

Capítulo 2: La seguridad como competencia digital del siglo XXI en una educación no presencial

La competencia digital en seguridad se presenta en la actualidad como respuesta a los nuevos desafíos tecnológicos y a las diferentes posturas tanto positivas como negativas que se tiene con respecto al uso del Internet y las TIC. Desde una perspectiva general, la seguridad se define como el medio por el cual permite reducir o mitigar todo tipo de peligro, daño o cualquier otro riesgo, con la finalidad de proporcionar un estado de bienestar en las personas.

En materia de seguridad digital, es entendida como la capacidad que se enfoca en detectar, proteger y prevenir las amenazas de información e informáticas en los entornos digitales, con el fin de entender y conocer estrategias y herramientas de seguridad para la protección de datos. Es decir, mediante ello se busca prevenir, limitar y gestionar todo tipo de riesgo y amenaza en línea (García, 2017; Figueroa, Rodríguez, Bone y Saltos, 2017).

El núcleo de la seguridad digital, para Sequera, Toledo y Ucciferri (2018), se centra en la protección de los niños que utilizan las tecnologías para fines laborales, académicos, comunicacionales, entretenimiento o científico. Por esa razón, en la actualidad el internet y las TIC tienen vínculos directos con la Convención sobre los Derechos del Niño (CDN), pues si bien estos pueden representar oportunidades para su desarrollo integral, también originan riesgos que pueden afectar a su integridad, por lo que asegurar su acceso a las TIC de forma segura y proteger su integridad frente a los peligros o riesgos digitales es un derecho humano que se

tiene que garantizar para promover su libertad y seguridad. Ya que, este involucra la dignidad, integridad y autonomía para desarrollarse integralmente y libre de peligros (Comisión Económica para América Latina y el Caribe [CEPAL], 2014; Maqueo, Moreno y Recio, 2017).

No obstante, para garantizar el derecho a la integridad de los alumnos en los ambientes digitales se necesitan, por un lado, leyes y políticas que regulen y garanticen el acceso seguro a estos espacios tecnológicos y, por otro lado, mediante el empoderamiento y desarrollo de competencias, habilidades y conocimiento en temas de seguridad digital que les permita ejecutar actividades en la red y mitigar todo tipo de riegos que conlleva a una amenaza a sus derechos fundamentales (Pavez, 2014).

Es así como, el desarrollo de competencias digitales vinculadas con la seguridad adopta un rol importante en los entornos digitales, ya que este busca reducir los potenciales riesgos que conlleva su uso a través del desarrollo de conocimiento y habilidades, así como una actitud activa y crítica frente a las TIC. Asimismo, esta competencia se ha transformado en una de las competencias del siglo XXI, ya que permite responder de forma eficaz a los nuevos retos que origina la sociedad del conocimiento. Por tanto, es una necesidad formativa garantizar la seguridad de los estudiantes mediante el desarrollo de la competencia en seguridad, a fin de que estos puedan utilizar de forma crítica, responsable y segura las TIC.

A partir de lo descrito, en este capítulo se abordan temas centrales orientados a la importancia del desarrollo de competencias digitales en seguridad en los estudiantes del nivel primario. Después, se explica de forma concreta la dimensión de la competencia sobre protección de datos personales y privacidad, pues mientras los estudiantes permanecen más tiempo utilizando diferentes medios digitales exponen una serie de información personal, por lo que garantizar que esta información no sea compartida para fines ilegales implica que desarrollen dicha competencia a fin de para prevenir consecuencias en la vida privada, salud e integridad. Finalmente, se describen algunos riesgos que se encuentran en Internet y estrategias de protección para la salud y bienestar, haciendo relación a la segunda competencia seleccionada.

2.1. Importancia del desarrollo de competencias digitales en seguridad

Abordar el tema sobre la tecnología y las TIC en la educación conlleva a reflexionar sobre los beneficios que aporta en el aprendizaje y sobre los riesgos que genera su uso, puesto que desde que un niño se conecta al internet y por consiguiente utiliza las TIC, genera ciertas preocupaciones sobre los peligros que pueden enfrentar en estos espacios (Fondo de las Naciones Unidas para la Infancia [UNICEF], 2017).

Según Cervera (2009, como se citó en Sánchez, y Robles, 2016) esta realidad de las tecnologías genera diferentes posturas en los padres de familia con respecto a los desafíos que plantea el Internet en materia de protección y seguridad, pues, por un lado, algunos adoptan posturas positivas, viendo los potenciales beneficios que ofrecen a los estudiantes, mientras que otros no lo consideran así, incluso creen que existen beneficios que pueden aportar más como riesgos.

En esa línea, aquellos padres que adoptan posturas positivas frente a las TIC son en su mayoría los que consideran que sus hijos pertenecen a los denominados nativos digitales, es decir, tienen conocimientos para manejar diferentes de dispositivos electrónicos, plataformas digitales y acceder a todo tipo de información en línea, por lo que permiten el acceso libre y tienen poco control sobre ellos cuando utilizan el Internet, debido a que tienden a sobrevalorar las oportunidades que brinda y, en muchos casos, subestiman los riesgos que puede traer. Por su parte, los que adoptan actitudes negativas, son aquellos que reconocen e identifican los peligros a los que están expuestos y el daño que puede causar su uso, por lo que prefieren proteger a los niños adoptando estrategias que, en ocasiones, son extremas a tal punto de evitar y alejarlos de las TIC y las tecnologías (Fondo de las Naciones Unidas para la Infancia [UNICEF], 2020).

Esta situación, para el Fondo de las Naciones Unidas para la Infancia (UNICEF, 2012), se debe a que los padres de familia no son conscientes sobre el uso que le dan los niños a las TIC y las consecuencias que pueden representar ciertas prácticas, por lo que genera diversas percepciones e inquietud social, los

cuales ocasionan que adopten estrategias inadecuadas. Sin embargo, no solo se debe a que los padres de familia no tienen conciencia sobre los riesgos que generan las TIC, sino también no cuentan con información confiable y adecuada sobre cuál es la mejor estrategia o forma que puedan utilizar para preparar a los niños en el uso responsable y seguro de estas herramientas; asimismo, desconocen qué competencias deben desarrollar durante su paso por la educación para minimizar los posibles riesgos que conlleva su uso (UNICEF, 2020; Sánchez y Robles, 2016).

Para evitar estos dilemas de los padres sobre el mismo fenómeno, así como evitar discursos tecnofóbicos con respecto a los efectos positivos como negativos a nivel físico, emocional y psicológico que pueden determinar ciertas prácticas digitales y, sobre todo, mitigar la vulnerabilidad y riesgos (Castillejos, Torres y Lagunes, 2016), las TIC deben emplearse por parte de los estudiantes con criterio, conciencia, responsabilidad e inteligencia. Esto supone que los niños necesitan desarrollar habilidades digitales, conocimientos y actitudes en materia de seguridad, es decir, necesitan el desarrollo de competencias digitales en seguridad (Garmendia, Garitaonandia, Martínez y Casado, 2012; Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado [INTEF], s.f.); debido a que estas competencias están vinculadas estrechamente con el respeto a la privacidad, la integridad y la eficiencia en el uso de las TIC (Anderson, 2003, como se citó en Gallego, Torres y Pessoa, 2019).

Mediante el área en seguridad propuesto por el proyecto DIGCOMP se busca adquirir habilidades, conocimientos y actitudes en los estudiantes para que puedan desarrollar competencias con relación a la protección de su identidad digital y privacidad, salud física y psicológica, así como protección de todo tipo de dispositivos y del impacto que causa el manejo de las tecnologías en el medio ambiente.

De esa manera, contribuye a crear mejores oportunidades de aprendizaje en los espacios digitales a través del uso sostenible, responsable y seguro de las TIC, asimismo, permite comprender los riesgos y amenazas digitales y conocer qué medidas de protección y seguridad puedan garantizar la protección de su integridad y salud de los niños (Comisión Europea, 2020; Castillejos, Torres y Lagunes, 2016).

Por su parte, Fernández (2018) sostiene que esta competencia facilita el desarrollo de adoptar una actitud crítica y realista hacia las TIC, reconociendo su ventajas y desventajas y respetando principios éticos y morales en su uso.

La importancia de la adquisición de las competencias en seguridad no solo radica en que los alumnos puedan usar las TIC, las redes sociales y páginas de entretenimiento de forma segura y significativa cuando navegan en el internet mediante el desarrollo de diferentes habilidades y capacidades, sino también busca generar conciencia y sensibilización en los estudiantes para que les permita comprender e identificar con precisión la naturaleza y magnitud del riesgo que conlleva su uso (Punie, Neza & Ferrari, 2014). Por tal motivo, cultivar en los niños una cultura de prevención mediante el desarrollo de las competencias en seguridad con el objetivo de responder a los retos de las tecnologías, representa un desafío sin precedentes en la educación.

Teniendo en cuenta que la competencia digital y, en específico, las competencias, capacidades, conocimientos y actitudes que aporta el área de seguridad en la protección de dispositivos digitales, de información personales, de la salud y del medio ambiente, se debe promover su desarrollo desde la educación básica, con el fin de formar niños capaces de usar de forma eficaz y productiva las TIC y navegar de forma segura en los entornos virtuales (Valcárcel, Salvador, Casillas y Gómez, 2019).

En tal sentido, si bien las competencias del área de seguridad son competencias transversales, para su desarrollo eficaz se necesita la predisposición de todos los actores para aportar en el desarrollo integral de los estudiantes. Es así que, los sistemas educativos deben incluir las competencias del área de seguridad dentro de su currículo, ya que muchos no lo hacen. Por ejemplo, en el programa curricular de Educación Primaria de nuestro país, si bien, propone el desarrollo de dos competencias transversales en torno a lo digital, ninguno de ellos busca desarrollar capacidades o desempeños en materia de seguridad (Ministerio de Educación, 2016).

Por tal motivo, incluir dichas competencias constituye un aspecto clave para contribuir a los niños a convertirse en cibernautas seguros y responsables de las TIC, especialmente si se les enseña a utilizar, comprender, afrontar y controlar en lugar de evitar los riesgos en línea (Represa, 2020). Para ello, se necesita preparar y formar a los profesores en estos temas para que adopten un rol de guía, mediador, catalizador y facilitador de información con el objetivo de orientar a concientizar a los estudiantes de la importancia del uso responsable y seguro de las TIC (Instituto tecnológico InGenio Learning, 2021).

Desde esta perspectiva, si bien el profesorado es un elemento indispensable para educar y sensibilizar a los alumnos sobre la importancia de la seguridad, esta tarea debe ser compartida con los padres, pues el rol de estos es fundamental para concientizar a los niños sobre los riesgos y consecuencias que puede conllevar determinadas prácticas digitales. En efecto, la labor de los padres, docentes e institución educativa en la adquisición de las competencias en seguridad es una tarea que debe ser atendida, ya que todo estudiante que egrese de la educación básica debe ser capaz de desplegar estas competencias, y, con ello, contribuir a cerrar las brechas digitales y riesgos que conlleva su uso.

2.2. Protección de datos personales y privacidad en una educación no presencial

A causa de la crisis sanitaria por la pandemia del Covid-19, el Ministerio de Educación y el Estado ordenaron el aislamiento social a toda la población; por tanto, los colegios a nivel nacional tuvieron que paralizar el desarrollo de sus actividades presenciales, por lo que ahora han adoptó una nueva modalidad denominado la educación no presencial, con el objetivo de dar continuidad al proceso académico. Esta modalidad educativa se entiende como el desarrollo de las actividades educativas a través del ciberespacio, donde puede efectuarse desde los distintos espacios del hogar tan solo con contar con un recurso tecnológico que tenga conexión y acceso al internet (Bonilla, 2016, como se citó en Expósito y Marsolier, 2020).

Desde el punto de vista de Patiño (2020), es una modalidad que se centra en

la comunicación e interacción bidireccional y diferenciada entre maestros y alumnos en ambientes físicamente separados, facilitada por herramientas tecnológicas para el aprendizaje, tales como la radio, televisión, teléfono u otro dispositivo electrónico con conexión a internet. Esta situación conlleva a que uno de los requisitos principales para acceder a esta modalidad de enseñanza sea contar con herramientas tecnológicas, distinto al esquema presencial.

Entre las principales características de la educación no presencial destaca el desarrollo académico, ya que este se da a través de un entorno digital mediados por los recursos tecnológicos, donde la información que se transmite se lleva a cabo por medio de materiales educativos en línea, así como la comunicación e interacción es virtual y, sobre todo, las clases pueden desarrollarse de forma sincrónica o asincrónica, por lo que los horarios son abiertos y flexibles (Martínez, 2008). Por su parte Chaves (2017), señala que en estos espacios los alumnos son más autodidacta, pues se fomenta el autoaprendizaje y la autorregulación a través del rol de apoyo y guía que adopta el docente, es decir, en esta modalidad el protagónico y el centro del proceso educativo lo tiene el niño.

Este escenario de la no presencialidad educativa representa un aumento significativo de la presencia de los niños en Internet. Durante el primer trimestre del 2020, en el Perú, se ha registrado el 60,3% de niños entre 6 a 11 años que utilizan el Internet (Instituto Nacional de Estadística e Informática [INEI], 2020]. Al respecto, en 2021, hubo un aumento significativo de los 6,5 puntos porcentuales al pasar de 60,3% a 66,8%, asimismo, el 86,6% lo utiliza diariamente (Instituto Nacional de Estadística e Informática [INEI], 2021).

La Comisión Económica para América Latina y el Caribe (CEPAL, 2014), manifiesta que muchos de los alumnos emplean las TIC para comunicarse y obtener información para fines educativos y de entretenimiento como descargar música, películas y para acceder a videojuegos en línea. En el Perú, el 80,9% recurre a esta herramienta con el objetivo de acceder a información, mientras el 83,8% utiliza para realizar actividades de entretenimiento en línea y el 94,3% de los estudiantes la utilizan para comunicarse mediante las redes sociales (INEI, 2021).

Esto último, se origina debido a que las redes sociales se han convertido en un espacio de interacción donde las personas, incluyendo a los niños, socializan y establecen relaciones interpersonales con amigos, familiares, personas conocidas y hasta desconocidas que integran el mundo de la red social. En dicha interacción surge un intercambio en donde se envía y recibe todo tipo de información personal y recreativa (Astorg Y Schmidt, 2019).

Sin embargo, según la Universidad de Alicante (s.f.), las redes sociales es el espacio donde los estudiantes, al interactuar, comparten y hacen público datos personales, tales como dirección de su domicilio y de sus correos electrónicos, fotografías, gustos, intereses, debilidades, números telefónicos, edad y la institución educativa donde estudian. Igualmente, cuando ingresan a diferentes páginas web para buscar información o realizar actividades con fines educativos se difunde información personal, pues el principal requisito para acceder a estos espacios es la identificación personal. Todo ello, representa, por tanto, una mayor exposición de su seguridad y privacidad en los entornos digitales, pues al acceder a ellos son más vulnerables a mostrar un conjunto de datos personales.

Agregando a lo anterior, toda información que se publica en las redes sociales no se puede controlar o proteger, debido a que este espacio permite que todo usuario navegue y realice alguna acción que pueda dañar a alguien sin restricción alguna. Al respecto Chango (2018), indica que la información personal que se publica es vulnerable, puesto que las redes sociales como Facebook, Instagram, Telegram, etc., sin bien cuentan con programas diseñados para proteger nuestros datos personales, son muy pocos de los cibernautas que conocen y aplican. Del mismo modo, estas mismas plataformas no garantizan la protección y privacidad de los datos personales, pues estos también proveen información a terceros, quienes la usan para diferentes fines sin el consentimiento de sus usuarios, perjudicando su identidad e integridad.

Esta situación conlleva a que personas con ciertos intereses personales pueden usar la información personal del alumno para causar daños físicos y psicológicos y para utilizar con fines ilícitos como la suplantación de identidad, pérdida de datos o acoso cibernético (García, 2012-2013), puesto que en muchos

casos los estudiantes lo hacen de forma voluntaria, es decir, no son conscientes de las consecuencias que pueden tener determinadas prácticas digitales, como es el caso de compartir información personal. Al respecto, Troncoso (2010, como se citó en Ordoñez y Calva, 2020), sostiene que cuando una persona, niño o adolescente comparte información de carácter personal puede afectar en su proceso interpersonal en la sociedad, así como se puede construir identidades negativas del sujeto.

De acuerdo con INTEF (s.f) los peligros más graves originados por el acceso y manejo de las TIC son aquellos que afecta a la identidad, privacidad e integridad de los estudiantes causados por revelar datos personales y por no respetar la privacidad del otro. Por tal motivo, la atención y prevención frente a esta problemática social debe ser una prioridad que concierne a todos los agentes educativos y públicos, pues toda información de carácter personal debe ser protegida.

Debido a ello, con el objetivo de impedir que se divulguen características de su vida privada de los usuarios, la protección de información personal y privacidad en Internet, entendida como la facultad que tiene toda persona de controlar y decidir sobre el uso y destino de su información personal (Garrida, 2015, como se citó en Zúñiga, 2018), es un tema que ha tenido especial atención por diferentes organizaciones internacionales desde la defensa de los derechos del niño estipulado en normas jurídicas. Dicho de otro modo, la protección de información personal y privacidad es un derecho que tiene toda persona, por tanto, queda a disposición de los Estados e instituciones responsables garantizar este derecho, especialmente, en los estudiantes que son los más vulnerables.

Lo mencionado podemos encontrar tanto en el artículo 34.1 de la Carta de Derechos Humanos como en el artículo 57.1 del Reglamento de la Unión Europea, donde señalan que todo niño tiene derecho a la protección de sus datos personales y a los cuidados necesarios para su bienestar (Ordoñez y Calva, 2020). Del mismo modo, en el artículo 16.1 de la Convención Internacional sobre los Derechos del Niño (CIDN), se indica que todo niño tiene derecho a no ser objeto de injerencias arbitrarias o ilegales en todo lo que concierne al aspecto de su vida privada, familiar

y social, así como a no ser deslegitimado su honra y reputación (Fondo de las Naciones Unidas para la Infancia [UNICEF], 2006).

Al respecto, en Perú, en materia de protección de datos y privacidad de los niños, encontramos como referencia la Ley 29733, el cual tiene como objetivo garantizar el derecho a la protección de información de carácter personal y privado. Para ello, mediante su reglamento en el artículo 13 plantea ciertas medidas para garantizar dicho derecho bajo el principio del interés superior del niño de la CIDN.

Es así como, a través de estas normas jurídicas la protección de datos personales y privacidad en el espacio digital se ha convertido en un derecho fundamental que protege la vida privada e identidad de los estudiantes cuando ingresan a los diferentes espacios tecnológicos. Sin embargo, si bien los niños son sujetos de derechos, no garantiza que estos sean efectivamente ejercidos cuando hay un desconocimiento de la existencia de estas legislaciones por parte de la población y, en especial, de los padres de familia, lo que conlleva a generar un replanteamiento de las medidas que se toman en materia de protección de información de carácter personal y privado.

Autores como Acedo y Platero (2016) y Pérez (2009), sostienen que para garantizar dicho derecho no solo se necesita de normas legales que protegen y sanciones acciones que perjudiquen la vida privada de los niños, sino también es importante educar para la adquisición de competencias y habilidades necesarias que les permita tomar decisiones más adecuadas sobre qué información y dónde pueden exponer o proporcionar.

Frente a ello, desde el área de seguridad del proyecto DIGCOMP se propone el desarrollo de la competencia protección de datos personales y privacidad, puesto que mediante ello se busca dotar de conocimientos, capacidades, habilidades y actitudes en los alumnos, con el fin de afrontar los riesgos que afectan a la protección de su identidad e integridad (Comisión Europea, 2020).

En tal sentido, esta competencia se define como la capacidad de proteger activamente todo tipo de información personal y la privacidad en ambientes

digitales, donde le permita al niño entender y ser más consciente cuando comparte información personal mientras respeta la privacidad de otros y se protege a sí mismo de peligros, fraudes o suplantación de identidad (Comisión Europea, 2020). En otras palabras, por medio de ello se pretende empoderar a los niños a conocer pautas de autoprotección, así como para decidir cuándo, cómo y en qué medida su información personal debe proporcionar y quiénes pueden compartir (Vitale, 2014, como se citó en Chango, 2018).

En esa misma línea, Astorga y Schmidt (2019) sostienen que cuando los niños poseen conocimientos sobre seguridad digital pueden decidir qué tipo de información deben o no de compartir, además saben cómo usar sus datos personales, de tal manera que cuidan y protegen su identidad y la de los otros. Asimismo, mientras estos tienen desarrolladas capacidades para discernir qué información no deben proporcionar reducen su exposición a una serie de riesgos y peligros cibernéticos, contribuyendo, de esa manera, a que puedan aprovechar y beneficiarse de las múltiples oportunidades que brinda las TIC y las redes sociales de forma responsable y segura.

En suma, considerando que los niños son un sector de población que requiere mayor atención y protección por lo vulnerable que se encuentran frente a toda forma de delito y riesgos en Internet, el desarrollo de la competencia en protección de datos personales y privacidad se posiciona como un medio que busca responder a esos peligros que generan la exposición de información personal durante la educación no presencial o cuando se navega en el internet; así como también garantizar el ejercicio de este como un derecho fundamental que protege la vida privada e integridad, pues la protección es un aspecto esencial del desarrollo integral.

2.3. Riesgos digitales en internet y estrategias de protección para la salud y bienestar

A medida que las TIC se usan más a diario para el desarrollo del aprendizaje y otras actividades, la exposición y vulnerabilidad de los niños aumenta continuamente frente a una serie de riesgos cibernéticos. Una de ellas tiene que ver

con el acceso a contenidos inapropiados para su edad, tales como violencia, drogas, alcohol, abusos o suicidios, así como a imágenes sexuales o pornográficas, contenidos de juegos y apuestas donde el lenguaje que se emplea es inadecuado (García, 2008). Todo ello, puede traer como consecuencia cambios en su comportamiento y personalidad del niño, ya que estos pueden adoptar ciertas conductas inapropiadas como acosar, difundir imágenes o contenidos ilegales o sustraer contenidos inapropiados (Fondo de las Naciones Unidas para la Infancia [UNICEF], 2016).

Asimismo, cuando los docentes dejan como actividad de extensión para investigar sobre algún tema determinado, los niños pueden estar propensos al acceso de información poco confiable o falsa, pues no se registra parámetros de restricción para subir información, lo que significa que los textos científicos, artículos o informes que se tome puede ser errónea, el cual puede afectar a su desarrollo cognitivo y afectivo por el modo que abordan los temas (Pere, 2008).

Por otro lado, el mal manejo de datos personales y privacidad en las redes sociales o en las diferentes páginas web, puede perjudicar la integridad y la vida privada del niño. Cuando esta situación ocurre, los niños pueden estar expuestos a diferentes peligros o amenazas que van de acuerdo a la vulnerabilidad que se permite o a la seguridad a la que no se accede, tales como acosos cibernéticos (grooming, el ciberbullying y sexting), intimidación, odio y suplantación de identidad digital (Chango, 2018). Una idea similar es la que plantea García (2012-2013), quien señala que los riesgos que pueden encontrar los niños son el ciberbullying, sextorsión, sexting y adicción.

De los riesgos presentados, los acosos cibernéticos son los que generan mayores consecuencias a nivel físico y psicológico. Por ejemplo, el grooming, entendida como la captación de niños mediante el uso de las TIC, tiene como objetivo generar confianza por parte de un adulto en los niños para obtener a cambio contenidos personales inapropiados como imágenes o videos íntimos, es decir, son prácticas que conlleva a establecer conexiones emocionales con el fin de acosar o realizar abusos sexuales (Palmer, 2017). Esta situación según la UNICEF

(2012) sucede cuando un niño brinda información en las redes sociales o para acceder alguna plataforma sin ser conscientes de las consecuencias que puede traer esas acciones, personas con intenciones sexuales pueden adoptar la identidad del niño para captar a otros.

Al respecto, el ciberacoso es una forma de someter, intimidar, acosar psicológicamente y humillar de manera agresiva a un niño o adolescente mediante mensajes, videos o imágenes que se envían a por medio del internet y las redes sociales, su principal función es atomizar y llevarle a un quiebre emocional a quien es víctima (Lloret, 2014). Además, este es considerado como un medio para ejercer violencia frente a un niño, a través de la intimidación, burlas, chantajes o limitación del derecho a la libertad que afectan significativamente a la privacidad, intimidad e identidad (García, Joffre, Martínez y Llanes, 2011).

Todos estos riesgos que se han descrito pueden traer como consecuencia daños físicos o psicológicos, problemas psicológicos, conducta de suicidio, baja autoestima, desconfía, depresión y cambios de comportamientos, los cuales se trasladan de manera significativa en el bajo rendimiento académico de los niños (Mendoza, 2012).

Si bien el acceso a las TIC en ocasiones puede representar temores por los peligros que conlleva su uso, esto no significa que deben dejar de lado o prohibir su uso en los niños. Para ello, es importante conocer las siguientes estrategias presentadas por diferentes organizaciones que buscan garantizar el acceso seguro y confiable a los diferentes espacios que proporcionan las TIC, así como prevenir todo tipo de daño físico y psicológico.

Una de las estrategias de protección y prevención que sostiene la UNICEF (s.f.) tiene que ver con la actitud y predisposición por parte de los padres para acompañar a los niños cuando hacen uso de las TIC, pues mediante ello pueden tener mayor confianza para compartir sus experiencias en el internet o las redes sociales, es decir, brindar la confianza a sus hijos para que puedan acudir cuando se sienten vulnerados.

Para que exista esa confianza, el Ministerio del Interior (2021), sostiene que debe existir una buena comunicación que permita compartir dudas, problemas u orientación con respecto al uso del internet; asimismo, indica que cuando los padres muestran predisposición para acompañar en los espacios digitales, crean un ambiente familiar basado en la confianza que facilita abordar temas que se vinculan con los peligros en las redes sociales o páginas web; sin embargo, es importante señalar que, esto no garantiza que las medidas que adoptan para ayudar a sus hijos sean las más adecuadas y eficaces, ya que existen una falta de información por parte de ellos en materia de seguridad.

Por el contrario, el Fondo de las Naciones Unidas para la Infancia (UNICEF, 2016) recomienda que es importante habilitar espacios que fomenten la sensibilización sobre la seguridad, pues mediante ello se promueve el empoderamiento y formación de los niños y padres de familia con respecto al uso responsables y seguro de las TIC.

En relación a la protección de información personal en las redes sociales, es importante orientar a los niños sobre qué información puede compartir en modo público y cuál no, ya que pueden ser víctimas de los diversos riesgos digitales. Por su parte, la Agencia Española de Protección de Datos (s.f), indica que la información como los nombre y apellidos, domicilio, número de DNI, número de teléfono, fotografía, datos de salud y datos laborales son de carácter personal, por lo que no se deben de compartir en el mundo digital.

Desde la perspectiva de Vitale (2014, como se citó en Chango, 2018) para proteger su privacidad y seguridad, los niños deben plantearse qué información personal pueden publicar y cuál no. Para ello, recomienda que los datos como nombre del colegio, información financiera familiar no deben publicarse, así como para evitar usar su nombre y apellidos reales es necesario utilizar pseudónimos. A ello se suma Moreno y Rueda (2013, como se citó en Astorga y Schmidt, 2019), quienes señalan que mientras menos información personal se ofrezca en las redes sociales el nivel de seguridad y protección de su identidad digital aumenta.

En esa línea, en la actualidad todo niño o niña que navegue por las redes

sociales y otras plataformas digitales necesita mantener segura su privacidad e información personal, por ello, es importante que conozca de una manera clara y sencilla, una serie de estrategias o medidas que deben emplear para garantizar su protección. Al respecto, El Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales (INAI, s.f.), menciona que una de las formas de proteger toda información personal que se publica o se sube a las diferentes redes sociales es utilizando las funciones de privacidad, con el fin de evitar que personas desconocidas tengan acceso a sus datos personales.

Otra forma de proteger nuestros datos personales, según la Comisión Federal de Comercio (s.f.), es navegar por los diversos entornos digitales utilizando la opción de modo incógnito para prevenir que nuestra información personal no se quede guardado; del mismo modo, recomienda no almacenar de forma predeterminada información o contraseñas en los navegadores. Por su parte, Garcia (2012-2013), sostiene que para mantener la privacidad de los niños se deben usar contraseñas seguras y difíciles de adivinar, además deben cambiarlas con frecuencia para prevenir el robo de información.

Asimismo, cuando investiga sobre algún tema determinado de las actividades académicas, es necesario que se les proporcione estrategias de cómo darse cuenta de que la información que tomará es confiable o falsa (UNICEF, s.f.). Del mismo modo, el Ministerio del Interior (2021), en su función de garantizar la protección del niño recomienda que es importante que los padres tengan acceso a los espacios que vistan sus hijos en el internet, con la finalidad de verificar a qué tipo de información están accediendo y qué información está compartiendo y a quienes.

Con relación a una de las estrategias que deben aplicar todos los niños para mitigar los riesgos que pueden generar ser víctima de suplantación de identidad es comunicarse directamente con los gestores de la propia red, con el fin de denunciar este delito (Ministerio del Interior y Seguridad Pública de Chile, 2020). De esa manera, se previene todo tipo de riesgo que afecte a la integridad e identidad digital.

Por último, cuando se utiliza algún tipo de dispositivos tecnológicos es importante que se tengan en cuenta los siguientes aspectos: mantener una distancia

de 30 o 40 cm con relación a la pantalla; utilizar la iluminación natural de los dispositivos; mantener una posición correcta y cómoda; cuando se utiliza audífonos mantener el volumen recomendado por los dispositivos y, finalmente, efectuar descansos cortos con frecuencia (Confederación de Empresarios de Lugo, 2015). Todo ello, con el objetivo de prevenir enfermedades que afectan a la salud y bienestar de quienes utilizan estos dispositivos.

Es importante enfatizar que, si bien estas estrategias pueden ser propuestas desde un enfoque preventivo, sin embargo, para su efectividad e impacto en los estudiantes es esencial que se trabaje desde el objetivo de desarrollar competencias en seguridad, dicho de otro modo, desde la adquisición de las competencias sobre protección de datos personales y privacidad y protección de la salud y bienestar. Esta última, es una competencia con un valor determinado para velar por la estabilidad emocional, física y psicológica, pues como se indicó anteriormente busca evitar riesgos y peligros para la salud por el uso de las tecnologías y el mal manejo de plataformas digitales (Comisión Europea, 2020).

En síntesis, a partir de lo desarrollado en este apartado, podemos determinar que el desarrollo de las competencias en seguridad en los alumnos es un reto que exige la participación de las familias, educadores, colegios, sociedad y Estado, pues mediante estos agentes se puede educar y formar a los niños para prevenir y proteger frente a todo tipo de riesgo cibernético que dañe la integridad física y psicológica y, de esa manera, garantizar su acceso seguro y confiable. Por ello, dicha competencia es una de las alternativas que no tiene que ser dejada de lado cuando se busca desarrollar en los niños capacidades, habilidades, conocimientos y actitudes a fin de crear una cultura de prevención digital.

Si bien una de las competencias del área de seguridad (protección de datos personales y privacidad) es un derecho legítimo respaldados por marcos jurídicos nacionales e internacionales, este no es ejercido con eficacia, pues existe un desconocimiento en la sociedad. Ante ello, es importante generar un balance entre el aprovechamiento y la protección mediante espacios donde se permita a los estudiantes no solo conocer ciertos derechos y deberes en los entornos digitales, sino también desarrollar habilidades y competencias en materia de seguridad.

SEGUNDA PARTE: INVESTIGACIÓN

Capítulo 3: Diseño metodológico

En este apartado se presenta y sustenta el diseño metodológico utilizado para responder a la pregunta de investigación. Primero, se inicia con la delimitación del enfoque y tipo de investigación que orienta la presente investigación; segundo, se define el objetivo general y los objetivos específicos, los cuales detallan las acciones necesarias para cumplir con el propósito final, asimismo, se detalla las categorías y subcategorías propuestas; tercero, se describen los informantes seleccionados quienes brindan datos necesarios para realizar esta investigación, además se explican los criterios de inclusión y exclusión; cuarto, se definen las técnicas e instrumentos empleados para obtener información y validación de los mismos garantizando la confiabilidad, validez y objetividad. Finalmente, se presentan las técnicas de organización, procesamiento y análisis de la información teniendo en cuenta los principios de ética propuestos por la Pontificia Universidad Católica del Perú.

3.1. Enfoque y tipo de investigación

El presente estudio requiere ser desarrollado desde la dimensión de la realidad educativa en torno a las competencias en seguridad. Por tal motivo, el enfoque metodológico de este estudio es cualitativo, puesto que su propósito es evitar la cuantificación y basarse principalmente en generar datos descriptivos de los fenómenos o eventos que son estudiados, para ello, emplea una serie de técnicas e instrumentos que generan datos descriptivos Quecedo y Castaño, 2002). Por su parte, Hernández, Fernández y Baptista (2014) sostienen que este enfoque se centra en comprender los fenómenos desde la visión y perspectiva de los participantes estudiados con relación a su ambiente natural y contexto. Dicha perspectiva toma en cuenta las experiencias, actitudes, creencias, pensamientos y reflexiones de los informantes (Gegeo 1988, como se citó en Pérez, 2007).

En ese sentido, el fenómeno que se analizó es sobre qué percepciones y niveles de competencias en seguridad del modelo DIGCOMP consideran que

poseen y han desarrollado los niños de 6to grado del nivel primaria de un colegio público de Lima Metropolitana.

Teniendo en cuenta los alcances de este estudio, el nivel de esta investigación cualitativa es descriptiva, puesto que busca “describir sistemáticamente hechos y características de una población dada o área de interés de forma objetiva y comprobable” (Colás y Buendía, 1990, como se citó en Díaz, Suárez y Flores, 2016, p.39). Su objetivo principal se orienta en medir, buscar y evaluar propiedades y características importantes del fenómeno que se someten a un análisis (Hernández, Fernández y Baptista, 2006). Es así que, mediante el estudio descriptivo, nos permitió, desde un panorama más cercano, conocer, describir y responder a la pregunta de investigación y contrastar con la teoría la realidad educativa sobre las competencias en seguridad que poseen los estudiantes para que puedan proteger su identidad digital, salud y el medio ambiente frente a riesgos que genera el manejo de las TIC, las redes sociales y otros espacios digitales.

3.2. Objetivos y categoría de la investigación

Para el presente estudio se planteó la siguiente pregunta problemática: ¿Cuáles son las percepciones de los estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana? A raíz de la problemática formulada, el objetivo general de esta investigación es:

- Analizar las percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana.

Para alcanzar el objetivo general, se definieron los siguientes objetivos específicos:

- Describir las percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana.

- Describir el nivel de competencias digitales en seguridad de estudiantes de 6to grado de primaria en una institución educativa pública de Lima Metropolitana.

En respuesta al tema de investigación y los objetivos planteados, se proponen la siguiente categoría con sus respectivas subcategorías, las cuales se sustentan en la matriz de consistencia (ver anexo 1).

Según Romero (2005) las categorías permiten asignar grupos de conceptos y subcategorías a un nivel más abstracto, las cuales orientan el proceso de obtención, análisis e interpretación de la información de la investigación. En tal sentido, teniendo en cuenta los objetivos específicos se propone la siguiente categoría y subcategorías, las cuales contribuyeron en la realización del análisis. A continuación, se muestra en la tabla N° 4 cada una de ellas.

Tabla N°4:
Categorías y subcategorías de investigación

Categoría	Subcategorías
Competencias en seguridad	Protección de datos personales y privacidad
	Protección de la salud y bienestar

Es importante resaltar que dicha categoría y subcategorías presentadas fueron utilizadas para responder a los dos objetivos específicos planteados.

3.3. Fuentes informantes

De acuerdo con Arias, Villasis y Miranda (2016), las fuentes informantes son un conjunto de individuos de interés, que formarán el referente para la elección de la muestra, y que estos surgen de los objetivos planteados. Debido a ello, para la presente investigación, se ha seleccionado una muestra representativa, puesto que permite seleccionar con la mayor precisión posible a un grupo pequeño de informantes que reflejan o representan a un grupo más grande; es decir, el grupo seleccionado representa las mismas características de toda la población objetivo, por lo que los resultados pueden ser aplicados a dicha población (Monje, 2011).

A raíz de lo descrito, los informantes de este estudio se encuentran conformados por 25 estudiantes del 6to grado “A” del nivel primaria de una

institución educativa pública ubicada en el distrito de Pueblo Libre, provincia de Lima Metropolitana del departamento de Lima, la cual atiende los niveles de educación inicial y primaria en los turnos de mañana y tarde. Asimismo, dicha institución alberga a 190 estudiantes del nivel inicial a cargo de 8 docentes y 301 de primaria a cargo de 17 docentes.

La muestra seleccionada ha sido de **tipo no probabilístico por conveniencia**, el cual es entendida como un procedimiento de selección de forma arbitraria de la muestra, en otras palabras, se elige a los informantes en base a las características específicas de la propia investigación y, sobre todo, teniendo en cuenta los objetivos planteados del estudio (Sayago, 2014, como se citó en Muñoz, 2018). Al respecto, Otzen y Manterola (2017) sostienen que este tipo de selección otorga al investigador la potestad de seleccionar a los informantes de acuerdo a sus intereses o que cumplan con ciertos criterios determinados de selección, reduciendo, de tal forma, un posible sesgo cuando responden a una técnica o instrumento. Por tanto, para fines de este estudio, los informantes seleccionados fueron 10 de los 25 estudiantes seleccionados entre 11 a 12 años del sexto grado “A" del turno mañana, quienes contribuyeron con la generalización de datos e información para la investigación.

Cabe señalar que, la selección de los informantes se debe a que el investigador se ha desempeñado como docente practicante en el marco de sus prácticas-pre profesionales; por tal motivo, existe cierta cercanía y confianza con los informantes, lo cual permitió obtener información verídica sobre las percepciones y el nivel que tienen sobre sus competencias digitales en seguridad. Los criterios de muestra que se tuvieron en cuenta para la selección y exclusión se ubican en la siguiente tabla.

Tabla N°5:
Criterios de muestra

Criterios de inclusión	Criterios de exclusión
- Ser estudiantes del 6to grado “A”	- No ser estudiantes del 6to grado “A”
- Tener acceso a internet y a las TIC para el desarrollo de su proceso de aprendizaje y para realizar otras actividades	- No contar con redes sociales como facebook, instagram, WhatsApp, etc.

- Utilizar las redes sociales como facebook, instagram, WhatsApp, etc.

Es necesario enfatizar que los informantes seleccionados tuvieron que completar un formulario (ver anexo 2) que tuvo como objetivo determinar quiénes cumplen los criterios mencionados. De esa manera, se logró una selección objetiva y significativa.

3.4. Técnicas e instrumentos para la recolección de datos

Para lograr los objetivos específicos planteados, esta investigación cualitativa-descriptiva empleó dos técnicas e instrumentos que fueron aplicados a los 10 estudiantes seleccionados.

Es importante aclarar que, para el desarrollo de este estudio se evaluaron dos de las cuatro competencias del área de seguridad del modelo DigComp: protección de datos personales y privacidad y protección de la salud.

En tal sentido, con el propósito de describir las percepciones de los estudiantes sobre sus competencias digitales en seguridad se utilizó la entrevista del tipo semiestructurada como una de las técnicas más usadas en los estudios educacionales cualitativos (ver anexo 3), pues permite “the interviewer to ask each respondent the same questions in the same way. A tightly structured schedule of questions is used, very much like a questionnaire” (Mathers, Fox y Hunn, 2002, p.2). Para Diáz, Torruco, Martínez y Varela (2013) es una técnica que se caracteriza por el intercambio de ideas mediante el diálogo entre el entrevistador y el entrevistado, el cual se desarrolla por medio de preguntas y respuestas con el fin de obtener una información determinada. Mediante ello, el investigador tiene la posibilidad de aclarar dudas o reformular ciertas preguntas durante el proceso de la entrevista, lo cual asegura respuestas más apropiadas y beneficiosas para la investigación.

Dicha técnica se aplicó por medio del instrumento de guion de entrevista semiestructurada, el cual se basa en plantear una serie de preguntas abiertas que pueden modificarse o ampliarse a partir de las respuestas que brinda el entrevistado (Díaz y Sime, 2009). Cabe destacar que esta técnica e instrumento se ejecutó a través de sesiones por la plataforma Zoom con una duración de 20 minutos por

estudiantes. Dicha entrevista se realizó con previa autorización de la docente y padres de familia.

Por otro lado, para describir los niveles de dominio de las competencias del área de seguridad se empleó la técnica de encuesta en línea (ver anexo 4), ya que esta “utiliza un conjunto de procedimientos estandarizados de investigación mediante los cuales se recoge y analiza una serie de datos de una muestra de casos representativa de una población [..]” (García, s.f, como se citó en Casas, Repullo y Donado (2003). Esta técnica se caracteriza por permitir recolectar datos tanto cualitativos como cuantitativos de forma rápida, ya que se pueden recolectar datos de varias personas en simultáneo

Para la técnica presentada se utilizó un cuestionario como instrumento, ya que este se basa en la formulación de un listado de preguntas estandarizadas y estructuradas sobre los hechos que interesan en una investigación y, de esa manera, permite obtener información de la población estudiada (García, 2003).

Para la elaboración del cuestionario, se tomó como base la prueba de evaluación elaborado por García, Salvador, Casillas y Basilotta (2019), el cual tuvo como objetivo construir y analizar una prueba de evaluación para medir los conocimientos, capacidades y actitudes de 600 alumnos de 12 a 14 años de las competencias en seguridad del proyecto DigComp.

Las preguntas que se plantearon en el cuestionario son a través de ítems que presentan situaciones en las que los niños tienen que seleccionar una opción de respuesta correcta. Las opciones de respuesta que se les proporcionó son acciones que realizan para proteger sus datos personales y salud.

Para realizar el proceso de validación de los instrumentos, se recurre a la técnica de los juicios de expertos que poseen experiencia y conocimiento en el tema del presente estudio. En tal sentido se contó con el apoyo de la magister Sylvana Mariella Valdivia Cañote y la licenciada Rossangel Cuentas Ramírez. Para ello, previamente se envió un correo adjuntando una carta formal para solicitar su apoyo en la revisión y posterior validación de los instrumentos, el cual se muestra en el anexo 5. Después de haber aceptado la invitación los especialistas, enviaron el

guion de entrevista y el cuestionario, la matriz de consistencia y la ficha de validación de los instrumentos (ver anexo 6) por medio del correo electrónico.

3.5. Técnicas para la organización, procedimiento y análisis

Con el propósito de procesar y organizar los datos obtenidos a partir de la aplicación de los instrumentos señalados en los párrafos anteriores, se elaboraron matrices, en las cuales se separa la información obtenida acorde a las categorías y técnicas para de esa manera analizar e interpretar la información encontrada.

Para analizar la información se empleó el diseño sistemático propuesto por Hernández, Fernández y Baptista (2014), ya que presenta un proceso estructurado que inicia con la recolección de información por medio de los instrumentos propuestos. Segundo, en el proceso de codificación abierta se clasifican y codifican la información pertinente de cada instrumento. Tercero, en este proceso (codificación axial) se agrupan la información con relación a las categorías y subcategorías. Cuarto, en el proceso selectivo, se asigna un código al extracto más importante de la información para poder diferenciarlo entre ellos. Finalmente, mediante el proceso de visualización de la teoría, se relaciona la información obtenida por medio de los instrumentos con la teoría que se tiene para el desarrollo del análisis.

3.6. Principios de la ética de la investigación

La presente investigación considera el cumplimiento de cinco principios éticos de la investigación (respeto por las personas, beneficencia y no maleficencia, integridad científica, justicia y responsabilidad) que promueve el Comité de Ética de la Investigación de la Pontificia Universidad Católica del Perú (2019).

En cuanto al principio de respeto por las personas, la investigación se desarrolla a partir de los consentimientos informados y participación voluntaria de los participantes, donde se incluye la opción de dejar de participar si en caso lo desean. Para ello, los apoderados de los estudiantes autorizaron la participación de sus hijos en la investigación mediante el protocolo de consentimiento informado (ver anexo 7). Con relación al principio de beneficencia y no maleficencia, se protege la identidad y anonimato de los informantes a fin de resguardar su seguridad.

Finalmente, para los principios de integridad científica, justicia y responsabilidad, se promueve una acción honesta, equitativa y veraz, así como también, la información obtenida de la investigación responde exclusivamente para fines de este estudio y, sobre todo, se garantiza a los informantes el derecho de acceder a los resultados obtenidos del estudio.

Capítulo 4: Análisis e interpretación de resultados

En este bloque se presenta el análisis e interpretación de los resultados obtenidos a partir de los instrumentos aplicados a 10 estudiantes del nivel primaria, con el propósito de responder a los objetivos planteados en esta investigación con relación a las percepciones y niveles de dominio de las competencias digitales en materia de seguridad. Todo ello, se llevó a cabo siguiendo los aspectos a considerar en los procesos de análisis e interpretación, por un lado, la organización de respuestas brindadas por cada entrevista y encuesta en la matriz de procesamiento y organización de la información diseñada para cada subcategoría. Por otro lado, realizar el contraste entre los resultados obtenidos con la información brindada por los autores en el marco de la investigación. Cabe resaltar que se asignó un código para cada respuesta brindada por los informantes.

4.1. Competencias digitales en seguridad

La presente investigación empleó como marco de referencia el Marco Europeo de Competencias Digitales, conocido como DIGCOMP, con la finalidad de analizar las percepciones de los estudiantes de sexto grado del nivel primaria sobre sus competencias en el área de seguridad. Dicho marco fue adoptado debido a que busca un aprendizaje que implica el empoderamiento en términos de los conocimientos, habilidades y actitudes que son necesarias para poder hacer frente a los diferentes riesgos y peligros cibernéticos y navegar de forma responsable y segura en los entornos digitales.

Los resultados que se presentan a continuación se encuentran procesados en función a los códigos emergentes que se definieron a partir de los hallazgos tanto de la entrevista como de la encuesta. Para definir el nivel de percepción sobre sus

competencias se utilizó se utilizó la matriz de triangulación (ver anexo 9), teniendo en cuenta las descripciones de dominio (básico, intermedio y avanzado) que corresponden a lo propuesto por Ikano (s.f, como se citó en Comisión Europea, 2020) y Valcárcel, Salvador, Casillas y Gómez (2019). Es decir, para describir las percepciones de los estudiantes sobre su competencia en protección de datos personales y privacidad, se presentan los resultados de la entrevista, mientras que, para describir el nivel de dominio sobre dicha competencia, se presentan los resultados de la encuesta. A través del contraste de estos se define el nivel de percepción.

Dicha dinámica, también se adopta para presentar los resultados de la subcategoría sobre protección de la salud y seguridad. Cabe señalar que los resultados finales también atienden al objetivo general.

4.1.1. Protección de datos personales y privacidad

La competencia digital sobre protección y privacidad tiene como objetivo dotar a los niños de conocimiento, habilidades y actitudes para saber cómo emplear y compartir información personal sin exponerse a sí mismo y a terceros de cualquier posible daño o riesgo.

Teniendo en cuenta lo señalado, para analizar los resultados sobre las percepciones de los estudiantes en seguridad fue necesario utilizar los códigos emergentes tales como publicación de información personal, datos personales que no deben ser compartidos, protección de datos personales, respeto a la privacidad de otros y acciones frente a la suplantación de identidad. A continuación, se describen de forma detallada.

Para el mejor desarrollo del análisis es importante conocer a los informantes seleccionados de este estudio; es por ello por lo que se describe de forma detallada los datos generales más importantes de cada uno de ellos. Cabe señalar que para poder presentar mejor la información brindada por los participantes se utilizó códigos de identificación, donde ENT significa entrevistado(a), E representa encuestados(a), H indica hombre, M denota mujer y E indica la edad.

En ese sentido, los participantes seleccionados fueron 10 estudiantes del sexto grado “A" del turno mañana de una institución educativa de Lima Metropolitana, de los cuales dos de ellos son de sexo masculino y poseen 12 años edad; igualmente, tres del mismo sexo tienen 11 años; mientras tres informantes son del sexo femenino, una de 11 años y dos de 12 años de edad.

Teniendo en cuenta las características de los participantes, se presentan los resultados y análisis correspondientes a esta subcategoría. No obstante, para analizar tanto las percepciones y niveles de dominios sobre la competencia protección de datos y privacidad, fue necesario conocer las redes sociales que utilizan y la frecuencia de uso de estos. Respecto a ello, los entrevistados E1HE12, E3HE12, E5ME11, E9ME11, E10ME11 y E7HE11 manifestaron que utilizan las redes sociales como Facebook, Instagram y WhatsApp. Sin embargo, los participantes E6ME12, E4HE11 y E8HE11 señalaron que emplean Facebook y WhatsApp; mientras la entrevistada E7HE11 indicó usar Instagram y WhatsApp.

En esa línea, los entrevistados E3HE12, E2ME12, E6ME12 y E7HE11 mencionaron que utilizan diario WhatsApp. Asimismo, los informantes E1HE12, E4HE11 y E8HE11 emplean Facebook y WhatsApp a diario. Los participantes E6ME12, E7HE11 y E10ME11 usan Facebook dos veces a la semana. Los entrevistados E1HE12 y E2ME12 emplean Instagram interdiario. Por el contrario, el informante E7HE11 usa Instagram una vez a la semana. Por su parte, el entrevistado E3HE12 indicó que utiliza Facebook e Instagram una vez a la semana. La entrevistada E5ME11 manifestó que emplea Facebook, WhatsApp e Instagram 4 a 5 veces por semana; mientras la entrevista E9ME11 utiliza Facebook, Instagram y WhatsApp interdiario. Finalmente, la participante E10ME11 señaló que usa Instagram a diario

Todo lo descrito ratifica que este grupo está permanentemente conectado a cualquier dispositivo electrónico para acceder a las diversas redes sociales, ya que este es un espacio de interacción donde las personas, incluyendo a los niños, socializan y establecen relaciones interpersonales con amigos, familiares, personas conocidas y hasta desconocidas que integran el mundo de la red social. En dicha

interacción surge un intercambio en donde se envía y recibe todo tipo de información personal y recreativa (Astorg Y Schmidt, 2019).

Sin embargo, para la Universidad de Alicante (s.f.), las redes sociales es el espacio donde más los estudiantes, al interactuar, comparten y hacen público datos personales, tales como dirección de sus domicilios y de sus correos electrónicos, fotografías, gustos, intereses, debilidades, números telefónicos, edad y la institución educativa donde estudian. Todo ello, representa una mayor exposición de su seguridad y privacidad en los entornos digitales, pues al acceder a ellos son más vulnerables a mostrar un conjunto de datos personales, lo que aumenta la posibilidad de sufrir algún tipo de daño cibernético

Con relación al código emergente sobre si los estudiantes publican o no información personal, y sobre el conocimiento que poseen con respecto a si tienen el control de todo lo que publican en las redes sociales y el internet, los resultados muestran que los entrevistados ENT2ME12, ENT4HE11 y ENT8HE11 manifiestan que no publican información personal en las redes sociales. En cambio, los participantes ENT1HE12, ENT6ME12, ENT7HE11 y ENT10ME11 señalan que publican información como fotos familiares y propias de las redes sociales. Por su parte, el estudiante ENT3HE12 declaró: ***"Público información personal, como el colegio donde estudió, fotos personales y familiares y mi número de teléfono"***. En tanto, otro participante mencionó: ***"Público la ubicación de donde estamos con mis amigos, así como la ubicación de donde estamos con mis familiares cuando viajamos. También, fotos de mis familiares y mías, y el nombre del colegio donde estudio"*** [ENT5ME11]. Mientras la entrevistada ENT9ME11 indicó: ***"Publicó fotos mías y mis contraseñas, pero utilizo una aplicación para guardar notas de forma privada"***.

Por el contrario, de acuerdo con los resultados de la encuesta podemos contrastar que, tres de los cuatro participantes (E1HE12, E6ME12 y E10ME11) que indicaron que solo publican fotos familiares y propias en las redes sociales, consideran la opción que indica que: ***"La información la controlo yo y la puedo borrar cuando quiera"*** [E1HE12, E6ME12 y E10ME11]. Asimismo, las informantes EN5ME11 y EN9ME11 que publican aparte de fotos otras informaciones personales,

piensan que: ***"Su publicación no afectará en ningún caso a mi futuro ni al de mi familia"*** [E5ME11 y E9ME1].

Ante lo señalado, se puede evidenciar que dichos participantes poseen una percepción básica con respecto al conocimiento que deben de tener sobre el internet y las redes sociales, pues ninguna persona, incluyendo los niños, tiene la posibilidad de controlar la información personal que publican; ya que este espacio permite que todo usuario navegue y realice alguna acción que pueda dañar a alguien sin restricción alguna. Al respecto Chango (2018), indica que la información personal que se publica es vulnerable, ya que las redes sociales como Facebook, Instagram, Telegram, etc., si bien cuentan con programas diseñados para proteger nuestros datos personales, son muy pocos los cibernautas que conocen y aplican. Del mismo modo, estas mismas plataformas no garantizan la protección y privacidad de los datos personales, pues estos también proveen información a terceros, quienes la usan para diferentes fines sin el consentimiento de sus usuarios.

Todo ello, una vez más, expone la identidad e integridad de los niños en el mundo digital. Frente a ello, es importante que las TIC, las redes sociales y otras plataformas digitales se usen con criterio, conciencia, responsabilidad e inteligencia. Por tanto, es necesario que los niños desarrollen habilidades digitales, conocimientos y actitudes en materia de seguridad, en otras palabras, requieren el desarrollo de competencias digitales en el área seguridad (Garmendia, Garitaonandia, Martínez y Casado, 2012; Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado [INTEF], s.f.); puesto que, dicha competencia constituye un aspecto clave para ayudar a los niños a convertirse en cibernautas seguros y responsables de las TIC y las redes sociales, especialmente si se les enseña a utilizar, comprender, afrontar y controlar en lugar de evitar los riesgos en línea (Represa, 2020).

Por el contrario, a pesar de que los entrevistados ENT2ME12, ENT4HE11 y ENT8HE11 manifiestan que no publican información personal en las redes sociales, estos tienen conocimiento de que: ***"Una vez que publican algo en Internet pierden el control sobre ello"*** [E2ME12, E4HE11 y E8HE11]. Mientras que el participante EN7HE11 que indicaron que solo publican fotos familiares y propias en

las redes sociales, consideran, en la encuesta demostró que sabe que: ***"Una vez que publico algo en Internet pierdo el control sobre ello"*** [E7HE11]. Asimismo, el entrevistado EN3HE12, quien si bien pública información como el nombre de su colegio, número de teléfono y fotos propias y familiares, sabe que: ***"Una vez que publican algo en Internet pierden el control sobre ello"*** [E3HE12].

Al respecto, se puede evidenciar que los informantes descritos en el párrafo anterior poseen una percepción intermedia con respecto al conocimiento que deben tener sobre el Internet y las redes sociales; pues a pesar de que comparten información personal en las redes sociales tienen en cuenta que no pueden controlar y resguardar dichas informaciones.

Esto supone que han desarrollado competencias en materia de seguridad, en específico la competencia sobre protección de datos personales y privacidad, puesto que mediante ello se busca dotar de conocimientos, capacidades, habilidades y actitudes en los alumnos con el fin de afrontar los riesgos que afecta a la protección de su identidad e integridad, así como también proteger su información personal. Desde la perspectiva de la Comisión Europea (2020), dicha competencia permite que el niño entienda y sea más consciente cuando comparte información personal mientras respeta la privacidad de los demás y se protege a sí mismo de amenazas, fraudes o suplantación de identidad.

Por su parte, Vitale (2014, como se citó en Chango, 2018), señala que mediante ello se pretende empoderar a los niños a conocer pautas de autoprotección, así como para decidir si debe o no publicar sus datos personales o cuándo, cómo y en qué medida sus datos personales se deben proporcionar y con quiénes puede compartir, con el propósito de aprovechar las oportunidades que brindan las TIC, las redes sociales y otras páginas de forma segura.

Por otro lado, la Agencia Española de Protección de Datos (s.f), indica que la información como los nombre y apellidos, domicilio, número de DNI, número de teléfono, fotografía, datos de salud y datos laborales son de carácter personal, por lo que no se deben de compartir en el mundo digital. Desde la perspectiva de Vitale (2014, como se citó en Chango, 2018) para proteger su privacidad y seguridad, los

niños deben de plantearse qué información personal deben publicar y cuáles es conveniente que no lo hagan, por ello, recomienda que los datos como nombre del colegio, información financiera familiar no deben publicarse, así como para evitar usar su nombre y apellidos reales es necesario utilizar pseudónimos. A lo presentado, se suma Moreno y Rueda (2013, como se citó en Astorga y Schmidt, 2019), quienes señalan que mientras menos información personal se ofrezca en las redes sociales el nivel de seguridad y protección de su identidad digital aumenta.

Teniendo en cuenta lo descrito en el párrafo anterior, los resultados revelan que los entrevistados ENT1HE12, ENT2ME12, ENT3HE12 y ENT8HE11 mencionan que datos como la dirección de domicilio, número de teléfono, fotos propias y familiares, nombre completo, número de DNI de los padres, ubicación del lugar donde me encuentro y el oficio de sus padres no se debe publicar en las redes sociales y el internet; asimismo, la entrevista señala que no se debe compartir: ***"La dirección de mi casa, la dirección de donde trabajan mis padres, el colegio donde estudio o fotos mías"***.

En tanto, la informante ENT9ME11 afirma que las informaciones que no deben ser publicadas son: ***"La ubicación de donde me encuentro, el número de DNI de mis padres, fotos mías y de mis familiares"***. Todo ello, nos permite determinar que dichos participantes conocen qué información personal no debe ser compartida o publicada, por lo que poseen conocimiento sobre la importancia de la huella digital en las redes sociales e internet, y el uso que pueden hacer terceras personas, lo que significa que en este código emergente sus percepciones se encuentran en un nivel de dominio intermedio. Esto se puede sustentar con los resultados de la encuesta, ya que indicaron que: ***"Un comentario personal sobre una noticia que he leído en el periódico"*** no pone en peligro su identidad [E1HE12, E2ME12, E3HE12, E8HE11 y E9ME11].

Ante lo señalado, Astorga y Schmidt (2019) manifiestan que cuando los niños poseen conocimientos sobre seguridad digital pueden decidir qué tipo de información deben o no de compartir, así como saben cómo usar sus datos personales, de tal manera que cuida y protege su identidad y la de los otros. Asimismo, mientras los participantes mencionados tienen desarrolladas

capacidades para discernir qué información no deben proporcionar reducen su exposición a una serie de riesgos y peligros cibernéticos, contribuyendo, de esa manera, a que puedan aprovechar y beneficiarse de las múltiples oportunidades que brinda el internet y las redes sociales de forma segura y responsable.

Sin embargo, los participantes ENT4HE11, ENT6ME12, ENT5ME11, ENT7HE11 y ENT10ME11 si bien conocen qué tipos de información personal no debe ser publicada, contrastando con los resultados de la encuesta estos afirman que: ***"Una fotografía en la puerta de mi casa en la que aparece el número y nombre de la calle"*** [E4HE11, E6ME12, E5ME11, E7HE11 y E10ME11] no pone en peligro su identidad. Por ende, sus percepciones se encuentran en un nivel básico, ya que no poseen conocimiento sobre la importancia de la huella digital en las redes sociales e internet, y el uso que pueden hacer terceras personas.

Frente a ello, a causa del mal manejo de sus datos personales y privacidad en las redes sociales o en las diferentes páginas web, se exponen a personas que pueden atentar la integridad y la vida privada del niño. Cuando esta situación ocurre pueden estar expuestos a diferentes peligros o amenazas que van de acuerdo con la vulnerabilidad que se permite o a la seguridad a la que no se accede, tales como acosos cibernéticos (grooming, el ciberbullying y sexting), intimidación, odio y suplantación de identidad digital (Chango, 2018).

Esto se puede ejemplificar con los resultados de la informante ENT5ME11, quién al formularle la pregunta si había tenido algún episodio que considere una violación a su privacidad por compartir datos personales indico lo siguiente: ***"Una vez, cuando utilizaba el aplicativo TikTok, estaba grabando un video y de la nada no me dí cuenta que había publicado mi número de celular, y me empezaron a escribir personas que no conocía"***. Mientras los participantes ENT1HE12, ENT2ME12, EN3HE12, ENT4HE11, ENT6ME12, ENT7HE11, ENT8HE11, ENT9ME11 y ENT10ME11 señalaron que por el momento no han tenido un episodio que consideren una violación a su privacidad.

Por tanto, queda en evidencia que cuando una información personal es compartida por el mal manejo de cualquier tipo de plataformas y herramientas

digitales puede traer ciertas consecuencias a sus usuarios. Al respecto, Troncoso (2010, como se citó en Ordoñez y Calva, 2020), sostiene que cuando una persona, niño o adolescente comparte información de carácter personal puede afectar en su proceso interpersonal en la sociedad, así como se puede construir identidades negativas del sujeto.

Toda esta situación, y tomando como ejemplo los resultados de la informante ENT5ME11, se desarrolla debido a que los estudiantes no son conscientes de las consecuencias que pueden tener determinadas prácticas digitales, como es el caso de compartir información personal.

Es importante señalar que en la actualidad la protección de datos personales y privacidad están planteados desde la defensa de los derechos del niño; por esta razón, cuando los datos personales se comparten o publican por las redes sociales, no solo se exponen a sufrir algún tipo de riesgo o peligros digital, sino también se vulnera el derecho a la protección de la información personal y a los cuidados necesarios para su bienestar, estipulado en el artículo 16.1 de la Convención Internacional sobre los Derechos del Niño (CIDN), que indica que todo niño tiene derecho a no ser objeto de injerencias arbitrarias o ilegales en todo lo que concierne al aspecto de su vida privada, familiar y social, así como a no ser deslegitimado su honra y reputación (Fondo de las Naciones Unidas para la Infancia [UNICEF], 2006). En Perú la Ley que regula es la 29733, la cual tiene como objetivo garantizar el derecho a la protección de los datos de carácter personal y privado.

Por otro lado, respecto a la categoría sobre medidas que emplea para proteger su información personal cuando acceden a las redes sociales o páginas web, los entrevistados ENT1HE12, ENT2ME12, 3NTHE12, ENT4HE11, ENT5ME11, ENT6ME12, ENT7HE11, ENT8HE11, ENT9ME11 y ENT10ME11, mencionan que protegen sus datos personales configurando en privacidad sus redes sociales. En cambio, la participante ENT5ME11 señala que: ***”Suelo cambiar muchas veces la contraseña de mis cuentas de redes sociales”***. Es decir, los informantes emplean acciones como configurar sus redes sociales mediante la opción de privacidad, así como cambian constantemente la contraseña de estos.

Por su parte, los resultados de la encuesta revelan que los estudiantes E1HE12, E2ME12, E3HE12 E4HE11, E5ME11, E6ME12, E7HE11, E8HE11, E9ME11 y E10ME11, manifiestan que cuando acceden a las redes sociales o páginas web protegen su información personal a través de "***utilizo la opción de modo incógnito, reviso las opciones de seguridad y privacidad del navegador y no almaceno contraseñas de forma predeterminada en los navegadores"***, así como ***configuro la opción de privacidad; utilizo contraseñas seguras y configuro la opción sobre qué personas solo pueden observar todo lo que subo (todas las anteriores)***.

Los hallazgos de esta categorización nos permiten señalar que los participantes poseen una percepción de nivel intermedio sobre medidas de protección de datos personales, puesto que tienen conocimientos de estrategias para proteger su identidad en las redes sociales y de los riesgos en internet, así como son conscientes de los principios de privacidad en internet. Asimismo, las acciones que emplean resultan ser las que recomiendan instituciones que velan por la protección de los usuarios en el mundo digital, tales como, el Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales (INAI, S.F.), quien menciona que una de las formas de proteger toda información personal que se publica o se sube a las diferentes redes sociales es utilizando las funciones de privacidad, con el fin de evitar que personas desconocidas tengan acceso a sus datos personales.

Otra forma de proteger nuestros datos personales, según la Comisión Federal de Comercio (s.f.), es navegar por los diversos entornos digitales utilizando la opción de modo incógnito para prevenir que nuestra información personal no se quede guardado; del mismo modo, recomienda no almacenar de forma predeterminada información o contraseñas en los navegadores. Una idea similar puede encontrarse en García (2012-2013), quien sostiene que para mantener la privacidad de los niños deben de usar contraseñas seguras y difíciles de adivinar, así como deben cambiarla con frecuencia para prevenir el robo de información.

Este último, nos ayuda a sustentar el nivel de percepción que se ha designado para esta categoría, pues la informante ENT5ME11 indicó que: ***"Suelo***

cambiar muchas veces la contraseña de mis cuentas de redes sociales", lo cual queda en evidencia el conocimiento que posee con respecto a medidas de protección de información personal. Sin embargo, es importante aclarar que, si bien para utilizar las redes sociales u otras plataformas de forma segura y responsable es importante conocer dichas medidas de seguridad, estas no garantizan al 100% la protección de nuestros datos personales. Pero en cierta medida reduce y previene que nuestra información se exponga a riesgos cibernéticos, así como a personas no autorizadas

Respecto a la categoría de qué manera ***respetan la privacidad de terceras personas*** cuando acceden a las redes sociales, los resultados muestran que los informantes ENT1HE12, ENT2ME12, 3NTHE12, ENT4HE11, ENT5ME11, ENT6ME12, ENT7HE11, ENT8HE11, ENT9ME11 y ENT10ME11, manifiestan que no comparten los datos personales que suben a las redes sociales, debido a que no cuentan con su consentimiento. Por su parte, los resultados de la encuesta, revela que los encuestados E1HE12, E2ME12, 3HE12, E4HE11, E5ME11, E6ME12, E7HE11, E8HE11, E9ME11 y E10ME11 menciona que, en el caso de que hayan recibido una información personal de uno de sus amigos sin su consentimiento: ***"Lo elimino e informo a dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios"***.

Estos resultados nos permiten identificar que los participantes en esta categoría tienen una percepción avanzada, pues cuentan con la capacidad y conocimiento de estrategias para proteger los datos de otras personas que se aplican en su propio contexto. También, poseen actitudes críticas sobre los principios de privacidad. Cuando dicha competencia se desarrolla en los estudiantes les permite tener la capacidad y actitud de proteger activamente todo tipo de información personal y la privacidad en ambientes digitales, donde el niño entiende y es más consciente cuando comparte información personal mientras respeta la privacidad de los demás y se protege a sí mismo de amenazas, fraudes o suplantación de identidad (Comisión Europea, 2020).

En cambio, cuando no poseen esta capacidad y actitudes de proteger y respetar cualquier información de otras personas puede generar riesgos que afectan

la identidad y reputación digital de terceros. Por ello, formar a los niños en cuestiones vinculadas con la privacidad tanto propia como de otros es de suma importancia, considerando que la privacidad es planteada desde el derecho a la intimidad a una vida privada, por lo que transgredir es un delito que conlleva a ser sujeto de sanciones reguladas por legislaciones de cada país. En el Perú estos están legislados por la Ley 29733.

Finalmente, en lo que concierne a medidas que emplean si descubren que una persona utiliza tu identidad para cometer delitos, los resultados de la entrevista exponen que los participantes ENT3HE12 y ENT7HE11 mencionan que las acciones que realizan es enviar un mensaje a las redes sociales denunciando la existencia de un perfil falso. Por su parte, los entrevistados ENT1HE12, ENT8HE11 y ENT9ME11 señalan que las medidas que emplean son informar a sus padres de familia y enviar un mensaje a las redes sociales denunciando la existencia de un perfil falso. Mientras que los estudiantes ENT2ME12, ENT4HE11 y ENT5ME11 indican que envían un mensaje a sus contactos y envían un mensaje a las redes sociales denunciando la existencia de un perfil falso. Por último, el entrevistado ENT6ME12, afirma que las acciones que realiza es: ***" Enviar un mensaje a la persona que ha creado el perfil falso"***. En contraste con los resultados de la encuesta este revela que esto mismos participantes señalaron que: ***"Envió un mensaje a la red social denunciando la existencia de un perfil falso para que lo eliminen"*** [E1HE12, E3HE12, E4HE11, E6ME12, E7HE11, E8HE11 y E9ME11].

Al respecto, los hallazgos determinan que en esta categoría las percepciones de estos participantes se encuentran en un nivel de dominio intermedio, ya que las estrategias que deben de aplicar para mitigar los riesgos que puede generar ser víctima de suplantación de identidad son comunicarse directamente con los gestores de la propia red con el fin de denunciar este delito, usar contraseñas seguras y complejas y hacer privado sus perfiles en las redes sociales (Ministerio del Interior y Seguridad Pública de Chile, 2020). Por tal motivo, estos participantes cuentan con conocimientos de estrategias para proteger su identidad en las redes sociales y de los riesgos en internet, pues esto involucra tener habilidades para decir qué hacer cuando su identidad ha sido suplantada en las redes sociales o en otros espacios digitales.

Sin embargo, a pesar de que los informantes ENT2ME12 y ENT5ME11, indican que envían un mensaje a sus contactos y envían un mensaje a las redes sociales denunciando la existencia de un perfil falso, los resultados de la encuesta revelan que ellos emplean la siguiente estrategia: ***"Envío un mensaje a mis contactos por medio de una publicación informando que han creado un perfil falso con mis datos personales para que eviten responder a ese perfil"***. Asimismo, la participante ENT10ME11 en la entrevista señala que: "Le comunicaría a mis padres que han creado un perfil falso con mis datos personales", mientras que en los resultados de la encuesta indicó que: ***"Envío un mensaje a mis contactos por medio de una publicación informando que han creado un perfil falso con mis datos personales para que eviten responder a ese perfil"***.

Este último resultado evidencia en los participantes la falta de congruencia entre lo que creen, lo que realmente saben y lo que deben hacer si son víctimas de la suplantación de identidad. Por tal motivo, la percepción de estos informantes se encuentra en un nivel básico, pues la falta de conocimientos y capacidades en materia de seguridad puede generar que sean víctimas de este delito que, en muchas ocasiones, se dan para cometer actos relacionados con el ciberacoso o la ciberdelincuencia.

4.1.2. Protección a la salud y bienestar

Todo tipo de entorno digital donde interactúan y desarrollan diversas actividades académicas y de entretenimiento, genera una serie de peligros que afecta a la salud y bienestar de las personas, incluyendo a los niños. Por tal motivo, la competencia sobre protección a la salud y bienestar se propone como una de las medidas que previene los efectos generados por utilizar las TIC. Esta competencia se define como la capacidad de evitar peligros que afecten la salud y al bienestar físico y psicológico del niño cuando emplean las TIC, así como la capacidad de protegerse a uno mismo y a los demás frente a riesgos de los espacios digitales.

A partir de lo mencionado anteriormente, para analizar los resultados sobre las percepciones de los participantes en relación a esta competencia, se aplicó la misma metodología, es decir, el análisis se desarrolla teniendo en cuenta los

códigos emergentes identificados en los hallazgos de la información obtenida de los instrumentos.

Con respecto al código emergente sobre consecuencias que genera el uso inadecuado de las redes sociales y la navegación en las páginas web en su salud, los informantes ENT1HE12, ENT3HE12, ENT4HE11, ENT5ME11, ENT6ME12, ENT8HE11 y ENT10ME11 manifiestan que pueden ser víctimas de algún tipo de acoso cibernético. Por el contrario, incluyendo al acoso cibernético, el entrevistado ENT7HE11 señaló que también puede causar: ***"Cuando observas videos que fomentan la violencia contra los animales o las personas puede que sufres algún daño psicológico, ya que puedes replicar los que hicieron en el video"***. Asimismo, la estudiante ENT9ME11 mencionó: ***"También podemos encontrar contenidos que no son propios de nuestra edad, como vídeos pornográficos, de violencia e información que nos pueda afectar psicológicamente"***. Mientras, la participante ENT2ME12 expresó que: ***"Una consecuencia sería la adicción a las redes sociales o las páginas web, ya que sobrepasamos su uso. También puede cambiar mi comportamiento o daños psicológicos si observamos algún video que tiene contenidos de violencia, asesinatos u otros"***.

Como se puede observar, en su mayoría los participantes están considerando al acoso cibernético como una de las principales consecuencias que afecta a su salud, pero no especifican los efectos en sí que genera estos. Por tal motivo, se les ha planteado una pregunta con respecto a si conocen los riesgos y consecuencias de los diferentes acosos cibernéticos. Al respecto, los entrevistados ENT2ME12 y ENT5ME11 indicaron que las consecuencias que generan son la baja autoestima. De igual manera, teniendo en cuenta la baja autoestima como una consecuencia, los informantes ENT1HE12, ENT4HE11, ENT6ME12, ENT7HE11, ENT8HE11, ENT9ME11 y ENT10ME11 indicaron que las consecuencias que generan son la depresión, bajo rendimiento académico y aislamiento por miedo y vergüenza; mientras el estudiante ENT3HE12 expuso que: ***"Puede ser víctima de algún secuestro por contactarse con personas que conoces"***.

En esa línea, para poder definir mejor el nivel de percepción que poseen, se les planteó otra pregunta sobre de qué manera pueden evitar dichas consecuencias

mencionadas. Ante ello, los estudiantes ENT1HE12, ENT3HE12, ENT4HE11, ENT5ME11, ENT6ME12, ENT8HE11 mencionaron que las acciones que adoptarán para prevenir es no compartir y/o publicar información personal en redes sociales y otras plataformas digitales. En cambio, la participante ENT7HE11 expresó que: ***"Lo que haría es consultarles a mis padres qué es lo que puedo y lo qué no puedo ver en YouTube"***. De la misma manera, la entrevistada ENT10ME11 señaló que: ***"Mis padres me dicen que no debo de utilizar mucho el internet, y creo que eso es lo que debo hacer para no afectar a mi salud y bienestar"***. En tanto, la entrevistada ENT2ME12 manifestó que: ***"Evitaría realizando otras actividades, tales como hacer deporte, salir a caminar y otras cosas"***. Finalmente, la estudiante ENT9ME11 manifestó que: ***"No debemos de acceder a contenidos que nos para nuestra edad porque puede afectar a nuestra salud***".

Estos resultados nos permiten exponer que las percepciones de los participantes ENT1HE12, E2ME12, ENT3HE12, ENT4HE11, E7HE11, ENT8HE11 y E9ME11 se encuentran en un nivel de dominio intermedio, dado que poseen conocimientos de las consecuencias y causas del ciberacoso, así como medidas preventivas para protegerse a sí mismo y a otros del ciberacoso. Lo mencionado anteriormente, se puede sustentar con los resultados de la encuesta, pues los estudiantes E1HE12, E3HE12, E4HE11 y E8HE11 indicaron que para evitar problemas de acoso cibernético: ***"Confío en personas que conozco y quieren contactarse conmigo"***.

A partir de los resultados se puede constatar que mientras los estudiantes poseen conocimientos y habilidades sobre los efectos y consecuencias que puede generar el uso inadecuado de las redes sociales y otras plataformas digitales en la salud, bienestar e integridad, aumenta la posibilidad de prevenirlos. Este punto de vista se apoya en Pávez (2014), quien sostiene que mediante el empoderamiento y desarrollo de competencias, habilidades y conocimiento en temas de seguridad digital contribuye a que les permita ejecutar actividades en la red de forma segura y mitigar todo tipo de riesgos que conlleva a una amenaza a sus derechos humanos y privacidad y, sobre a su salud y bienestar.

Asimismo, lo mencionado por los participantes guarda relación a lo manifestado por García (2012-2013), quien señala que, por el uso inadecuado de las redes sociales y otras páginas web, los riesgos que puede encontrar los niños son el ciberbullying, sextorsión, sexting grooming, adicción e infoxicación. Estos pueden traer como consecuencia daños físicos o psicológicos, sobrepeso, problemas psicológicos, conducta de suicidio, baja autoestima, desconfía, depresión y cambios de comportamientos, los cuales se trasladan de manera significativa en el bajo rendimiento académico de los niños (Mendoza, 2012).

Es importante aclarar que las estrategias preventivas que emplean las entrevistadas ENT7HE11 y ENT10ME11, el cual es acudir a sus padres, es una de las que recomienda la UNICEF (s.f), pues al existir una actitud y predisposición por parte de los padres para acompañar a los niños cuando hacen uso de las TIC, genera mayor confianza para compartir sus experiencias en el internet o las redes sociales, el cual permite que los niños puedan acudir cuando se sienten vulnerados. Está estrategia para el Ministerio de Interior (2021) no garantiza que las medidas que adoptan para ayudar a sus hijos sean las más adecuadas y eficaces, ya que existe un desconocimiento y falta de información por parte de ellos en materia de seguridad.

Por su parte, los estudiantes E5ME11 y E6ME12 poseen una percepción de nivel básico, pues tienen conocimientos de las consecuencias y causas que puede ocasionar el ciber-acoso, sin embargo, no cuentan con la capacidad para actuar preventivamente con relación al ciber-acoso. A esto se suma los resultados de la encuesta, el cual revela que la primera encuestada manifestó que: ***"Utilizo una falsa personalidad en la Red"***. Del mismo modo, la segunda informante sostiene que: ***"Solo me comunico con otros si es presencialmente"***. Por lo tanto, no existe una coherencia entre lo que señalan (con respecto a las consecuencias que genera el uso inadecuado de las TIC, las consecuencias que genera los diferentes acosos cibernéticos y qué acciones emplean para evitarlas) y lo que realmente saben y realizan.

Esta misma situación ocurre con la participante E10ME11, si bien señala que conocen las consecuencias que genera el uso inadecuado de redes sociales en la

salud, así como estrategias para evitarlos, estos no se reflejan de manera significativa en los resultados de la encuesta, porque indica que: ***"Utilizo una falsa personalidad en la Red"***. Esto significa que tiene una percepción de nivel básico. La información brindada por estos informantes muestra la falta de habilidades, capacidades y competencias en materia de protección a su salud y bienestar, por lo que promover el desarrollo de esta competencia es indispensable si se busca mitigar o prevenir algún tipo de riesgo digital que afecte a su salud, con el fin de garantizar el acceso seguro al mundo digital. El desarrollo de esta competencia se propone debido a que vela por la estabilidad emocional, física y psicológica, es decir, busca evitar riesgos y peligros que afecte a la salud por el uso de las tecnologías y el mal manejo de plataformas digitales (Comisión Europea, 2020).

Por último, en relación al cuidado de aspecto ergonómicos cuando utiliza algún dispositivo, los resultados delata que todos los entrevistados E1HE12, ENT2ME12, ENT3HE12, ENT4HE11, ENTE5ME11, ENT6ME12, ENT7HE11 ENT8HE1 y ENT9ME11 tiene cuida en estos. Las medidas que emplean son mantener una buena postura, escuchan música con el volumen adecuado y utilizan la iluminación recomendada por el dispositivo. Sin embargo, la participante ENT10ME11 manifiesta que: ***"Muchas veces no tengo cuidado cuando utilizo mi celular y la computadora. Por ejemplo, cuando utilizo audífono, como está malogrado, escucho solo con uno y en alto volumen. Yo lo utilizo echada en el sofá y suelo bajar el brillo del celular"***.

En contraste con los resultados de la encuesta, esta muestra que los informantes E3HE12, E7HE11, E8HE11, E9ME11 sostiene que: ***"Me siento correctamente en una silla, sofá, sillón, etc. y empleo trípode para sostener el equipo tecnológico"*** cuando hacen uso del ordenador, celular, Tablet, entro otros dispositivos. A consecuencia de ello, se puede señalar que estos poseen una percepción intermedia sobre riesgos que afecta a la salud originados por el uso de las tecnologías (desde los aspectos ergonómicos hasta la adicción a las tecnologías), puesto que cuentan con conocimientos claros de pautas saludables (ejemplo: ergonómicas, visuales, tiempos, auditivos. etc.) para el uso correcto de las tecnologías.

Lo mencionado se puede sustentar con la propuesta de la Conferencia de Empresarios de Lugo (2015), que señala que para prevenir enfermedades o riesgos que afectan la salud y bienestar de quienes utilizan diferentes dispositivos de aparatos tecnológicos es importante que consideren los siguientes aspectos: mantener una distancia de 30 0 40 cm con relación a la pantalla, utilizar la iluminación natural de los dispositivos, mantener una posición correcta y cómoda, así como cuando se utiliza audífonos mantener el volumen recomendado por los dispositivos y, por último, efectuar descansos cortos pero con frecuencia.

Sin embargo, los participantes E1HE12, E2ME12, E4HE11, E5ME11, E6ME12 y E10ME11, tienen una percepción básica sobre riesgos que afecta a la salud originados por el uso de las tecnologías, pues estos manifestaron en la encuesta que: ***"Muchas veces me terminan doliendo la espalda, piernas o cuello"***, lo que significa que estos no cuentan con conocimientos claros de pautas saludables (ejemplo: ergonómicas, visuales, tiempos, auditivos. etc.) para el uso correcto de las tecnologías.

Los hallazgos presentados muestran que no existe una cohesión entre lo que dicen y lo que realmente saben, lo que conlleva a que los informantes señalados presenten carencias para adoptar las mejores estrategias y cuidados que garanticen su protección de su salud y bienestar cuando utilizan dispositivos tecnológicos. Debido a ello, es importante que los estudiantes desarrollen la competencia sobre protección de su salud y bienestar, dado que este no solo busca prevenir los riesgos que genera el mal manejo de las plataformas digitales en la salud, sino también se enfoca que evitar que se haga un mal uso de los dispositivos tecnológicos (Comisión Europea, 2020).

Los resultados obtenidos de esta competencia ponen en evidencia que en una sociedad cada vez más globalizada las oportunidades que brindan las TIC y los espacios digitales deben ser aprovechados por todos los niños sin ninguna excepción, para ello, se debe garantizar la protección a la salud física y emocional por medio del desarrollo de competencias en materia de seguridad, con el propósito de promover una cultura de hábitos mediáticos saludables.

CONCLUSIONES

Por medio del presente estudio, se exponen las siguientes conclusiones:

1. El área de seguridad y sus competencias se presentan como respuesta a los nuevos desafíos que genera el uso de las TIC, las redes sociales y otros espacios digitales, puesto que su objetivo principal es que los estudiantes adquieran habilidades, conocimientos y actitudes para identificar, evitar y enfrentar con precisión la naturaleza de posibles riesgos y peligros que afectan a su identidad digital, integridad y salud, así como buscar el uso sostenible con el fin de proteger el medio ambiente; asimismo, contribuye a crear mejores oportunidades de aprendizaje a través del uso crítico, responsable y seguro de las TIC.

2. De acuerdo con resultados obtenidos se evidencia que los conocimientos y capacidades que dicen y creen tener los estudiantes del 6to grado del nivel primaria son en su mayoría consecuentes con lo que realmente saben y hacen cuando emplean e interactúan con las TIC y otras plataformas. Esto permite minimizar los posibles peligros que se encuentran en el mundo digital y maximizar las oportunidades que brinda para su formación.

3. Los estudiantes de 6to grado del nivel primaria poseen un nivel de percepción intermedio con relación a la competencia protección de datos personales y privacidad del área de seguridad, puesto que cuentan con conocimientos, actitudes y habilidades sobre qué tipo de información personal no deben publicar en las redes sociales y el internet, conocen los principios por el respeto de la privacidad de otros, saben de estrategias para proteger su información personal y adoptar acciones adecuadas para contrarrestar los efectos de la suplantación de identidad. Todo ello, les permite garantizar su seguridad en el mundo digital protegiendo su derecho a la privacidad e intimidad y navegando de forma segura, crítica y responsable. No obstante, es importante que se fortalezcan algunos conocimientos y habilidades en relación a la seguridad en las redes sociales, pues se evidencia que hay

algunos participantes que muestran conocimientos básicos sobre estos temas.

4. Respecto a la competencia sobre protección de la salud y bienestar, los estudiantes cuentan con un nivel de percepción intermedio, pues poseen conocimientos, habilidades y actitudes sobre las consecuencias que genera el uso inadecuado de las redes sociales y el internet en la salud emocional, física y psicológica; además, sobre los efectos que genera en la salud el uso de dispositivos electrónicos de forma inadecuada. Esto les permite ser más conscientes al navegar en el Internet y al usar cualquier tipo de dispositivo electrónico, considerando que su salud se expone a una serie de riesgos y peligros, por lo que al conocer sobre estos efectos podrán prevenirlos.

RECOMENDACIONES

A continuación, se presentan las siguientes recomendaciones:

1. Con el fin de contar con niños competentes y responsables en el mundo digital, se recomienda promover el desarrollo de las competencias del área de seguridad desde los colegios a través del área de Computación y otras afines a éstas como una cuestión de prioridad; para ello, es importante que estas competencias sean incluidas en el programa curricular de Educación Básica regular, ya que en actualidad si bien se propone el desarrollo de dos competencias transversales relacionadas a lo digital, ninguna de ellas busca desarrollar capacidades o desempeños en materia de seguridad.

2. Se sugiere que las competencias del área de seguridad se incluyan como un aspecto transversal en la formación de los docentes y padres, ya que son los protagonistas y actores principales en la formación integral de los niños, por tanto, deben de poseer conocimientos, habilidades y actitudes para que ayuden a estos cuando se encuentren en situaciones de vulnerabilidad, empleando estrategias y medidas que contribuyan al uso responsable y seguro, sin limitar las oportunidades que brindan las TIC.

3. Dado que los estudiantes se encuentren en constante interacción con las TIC y el Internet, se recomienda que se desarrolle una investigación de este tipo con mayor número de participantes, con el fin de contar con un panorama más claro de los niveles de dominio que poseen los estudiantes de la educación básica regular de nuestro país en materia de seguridad. Esto permitirá crear y promover políticas y programas educativos más eficaces, que faciliten el logro de mejores niveles de competencias digitales.

4. Se recomienda para futuras investigaciones evaluar las cuatro competencias del área de seguridad desde un enfoque cuantitativo para determinar con mayor exactitud los niveles de dominio que poseen los estudiantes y, por consiguiente, identificar aquellos que aún requieren fortalecer.

REFERENCIAS:

Aguilar, F. (2010). Percepción y meta-cognición en la educación: Una mirada desde América Latina. *Revista Sophia, Colección de Filosofía de la Educación*, (8), 148-190. https://www.redalyc.org/pdf/4418/441846105007.pdf

Agencia Española de Protección de Datos. (s.f). Los datos personales y la privacidad. Nuestros derechos y obligaciones. Principales riesgos en la red. https://www.tudecideseninternet.es/aepd/images/articulos/ficha-01.pdf

Alonso Ferreiro, A. (2011). El desarrollo del concepto de competencia digital en el currículum de las enseñanzas obligatorias de Galicia. *Revista Innovación Educativa*, (21), 152-158. https://minerva.usc.es/xmlui/bitstream/handle/10347/6230/1/pg_153-162_in21_1.pdf

Ala Mutka, K. (2011). *Mapping digital competence: Towards a conceptual understanding*. European Union. https://www.researchgate.net/publication/340375234_Mapping_Digital_Competence_Towards_a_Conceptual_Understanding

Area Moreira, M. (2015). La alfabetización digital y la formación de la ciudadanía del siglo XXI. *Revista Investigación Educativa*, 7(3). http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1997-40432014000300002

Arias Castilla, C. (2006). Enfoques teóricos sobre la percepción que tienen las personas. Revista Horizontes Pedagógicos, 8(1), 9-13. https://dokumen.tips/documents/enfoques-teoricos-sobre-la-percepcion-que-tienen-las-personas.html

Arias Gómez, J., Villasis Keever, M. y Miranda Novales, M. (2016). El protocolo de investigación III: la población de estudio. *Revista Alergia México,* 63(2), 201-206. https://www.redalyc.org/pdf/4867/486755023011.pdf

Ascencio Ojeda, P. (2017). *Estándar de competencia digital para estudiantes de educación superior de la Universidad de Magallanes de Chile* [Tesis doctoral, Universidad de Barcelona]. https://www.tdx.cat/handle/10803/460805#page=5

Astorga Aguilar, C. y Schmidt Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad*. Revista Electrónica Educare*, 23(3), 1-24. https://www.revistas.una.ac.cr/index.php/EDUCARE/article/view/10041/17750

Caccuri, V. (2018). C*ompetencias Digitales para la Educación del Siglo XXI [e-book].* https://www.academia.edu/36935871/Competencias_Digitales_para_la_Educaci%C3%B3n_del_Siglo_XXI

Casas Anguita, J., Repullo Labrador, J. y Donado Campos, J. (2003). La encuesta como técnica de investigación. *Revista Aten Primaria*, 31(8), 527-38. https://www.sciencedirect.com/science/article/pii/S0212656703707288

Castillejos López, B., Torres Gastelú, C. y Lagunes Domínguez. A. (2016). La seguridad en las competencias digitales de los millennials. *Revista de Apertura*, 8(2), 54-69. http://www.scielo.org.mx/pdf/apertura/v8n2/2007-1094-apertura-8-02-00054.pdf

Coll, C. (2007). *Competencia clave, competencias básicas: Una encrucijada para la educación escolar.* Universidad de Barcelona https://www.academia.edu/1137986/Competencias_clave_competencias_b%C3%A1sicas_una_encrucijada_para_la_educaci%C3%B3n_escolar

Comisión Europea. (2007). *Competencias clave para el aprendizaje permanente. Un Marco de Referencia Europeo.* https://www.educacionyfp.gob.es/dctm/ministerio/educacion/mecu/movilidad-europa/competenciasclave.pdf?documentId=0901e72b80685fb1

Comisión Federal de Comercio. (s.f.). NETCÉTERA Cómo charlar con sus hijos sobre su comportamiento en línea. https://www.consumidor.ftc.gov/articulos/spdf-0001-net-cetera.pdf

Comisión Europea. (16 de diciembre de 2020). Marco europeo de competencias digitales DIGCOMP. https://epale.ec.europa.eu/es/content/marco-europeo-de-competencias-digitales-digcomp

Comisión Económica para América Latina y el Caribe. (31 de octubre de 2014). *Uso seguro de las TIC puede ayudar a niños y adolescentes a ejercer mejor sus derechos*. https://www.cepal.org/es/comunicados/uso-seguro-de-las-tic-puede-ayudar-ninos-y-adolescentes-ejercer-mejor-sus-derechos

Confederación de Empresarios de Lugo. (26 de febrero, 2015). Recomendaciones preventivas en el uso de dispositivos electrónicos móviles. http://www.cel.es/es/actualidad/364/recomendaciones-preventivas-en-el-uso-de-dispositivos-electronicos-moviles/

Chango Jaya, S.(2018). *Competencias de seguridad-privacidad en internet y redes sociales en estudiantes de Tercero de Bachillerato General Unificado de una Unidad Educativa de Quito-Ecuador* [Tesis de maestría, Instituto Politécnico de Leiria].https://iconline.ipleiria.pt/bitstream/10400.8/3648/1/UPTIC_relatorio-final_Santiago%2BChango_06-08-2018.pdf

Chaves Torres, A. (2017). La educación a distancia como respuesta a las necesidades educativas del siglo XXI. *Revista Academia y Virtualidad*, 10(1), 23-41. http://dx.doi.org/10.18359/ravi.2241

Chávez Barquero, F., Cantú Valadez, M. y Rodríguez Pichardo, C. (2016). Competencias digitales y tratamiento de información desde la mirada

infantil. *Revista Electrónica de Investigación Educativa,* 18 (1), 210-216. http://www.scielo.org.mx/pdf/redie/v18n1/v18n1a15.pdf

Chiecher, A. (2020). Competencias digitales en estudiantes de nivel medio y universitario. ¿Homogéneas o heterogéneas? *Universidad Nacional de Río Cuarto Córdoba, CONICET, Argentina.* https://cerac.unlpam.edu.ar/index.php/praxis/article/view/4259/html

Díaz Bazo, C., Suárez Díaz, G. y Flores Flores, E. (2016). *Guía de investigación en educación.* Pontificia Universidad Católica del Perú. https://cdn02.pucp.education/investigacion/2016/06/21165057/GUIA-DE-INVESTIGACION-EN-EDUCACION_21_11_16.pdf

Diáz Bravo, L., Torruco García, U., Martínez Hernández, M. y Varela Ruíz, M. (2013). La entrevista, recurso flexible y dinámico. *Revista de Investigación en Educación Médica*, 2(7), 162-167. http://www.scielo.org.mx/pdf/iem/v2n7/v2n7a9.pdf

Díaz, C. y Sime, L. (2009). *Una mirada a las técnicas Una mirada a las técnicas e instrumentos de investigación*. Pontificia Universidad Católica del Perú. http://blog.pucp.edu.pe/blog/wp-content/uploads/sites/184/2009/02/bolet3.pdf

Egido Gálvez, I.(2011). Las competencias clave como elemento central del currículo de la enseñanza obligatoria: Un repaso a las experiencias europeas. *Revista Española de Educación Comparada,* (17), 239-262. https://www.researchgate.net/publication/307819596_Las_competencias_clave_como_elemento_central_delcurriculo_de_la_ensenanza_obligatoria_un_repaso_a_lasexperiencias_europeas

Expósito, D. y Marsolier, R. (2020). Virtualidad y educación en tiempos de COVID-19. Un estudio empírico en Argentina. *Revista Educación y Humanismo*, 22(39), 1-27. https://doi.org/10.17081/eduhum.22.39.4214

Fernández, P. (14 de septiembre de 2018). *La ciudadanía digital y la seguridad en educación.* https://ieducando.com/nuestro-blog/2018/09/14/la-ciudadania-digital-y-la-seguridad-en-educacion

Ferrari, A., Neza, B. & Punie Y. (2014). DIGCOMP: a Framework for Developing and Understanding Digital Competence in Europe. *eLearning Papers,* (38), 4- 14. https://www.academia.edu/7132885/DIGCOMP_a_Framework_for_Developing_and_Understanding_Digital_Competence_in_Europe

Figueroa Suárez, J., Rodríguez Andrade, R., Bone Obando, C. y Saltos Gómez, J. (2017). La seguridad informática y la seguridad de la información. *Revista Polo Conocimiento*, 2 (12), 145-155. https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf

Fondo de las Naciones Unidas para la Infancia. (2020). *Pantallas en casa: Guía para acompañar en el uso de internet*. https://www.unicef.org/uruguay/informes/pantallas-en-casa

Fondo de las Naciones Unidas para la Infancia. (2017). *Niños en un mundo digital.* https://www.unicef.org/peru/sites/unicef.org.peru/files/2019-01/Estado_Mundial_de_la_Infancia_2017._Ninos_y_ninas_en_un_mundo_digital._Resumen_Ejecutivo_-_UNICEF.PDF

Fondo de las Naciones Unidas para la Infancia. (2006). *Convención sobre los derechos del niño.* https://www.un.org/es/events/childrenday/pdf/derechos.pdf

Fondo de las Naciones Unidas para la Infancia. (2016). *Los derechos de la infancia y el internet.* https://sites.unicef.org/csr/files/Spanish_UNICEF_GUARDIAN_publication.pdf

Fondo de las Naciones Unidas para la Infancia. (s.f.). Niños, niñas y adolescentes en línea. Riesgos de las redes y herramientas para protegerse. https://www.unicef.org/chile/media/3096/file/lacro-en-linea.pdf

Fondo de las Naciones Unidas para la Infancia. (2012). *La seguridad de los niños en línea Retos y estrategias mundiales.* https://www.unicef-irc.org/publications/pdf/ict_spa.pdf

Fuenmayor, G. y Villasmil, Y. (2008). La percepción, la atención y la memoria como procesos cognitivos utilizados para la comprensión textual. *Revista de Artes y Humanidades UNICA*, 9(22), 189-200. https://www.redalyc.org/pdf/1701/170118859011.pdf

Fundación Telefónica. (2015). *Diagnóstico, diseño y desarrollo de contenidos para la Escuela TIC Familia en Colombia y sistematización del proceso.* https://www.fundaciontelefonica.co/wp-content/uploads/2016/05/Documento-Referenciaci%C3%B3n.pdf

Gallego Arrufat, M.,Torres Hernández, N. y Pessoa, T. (2019). Competencia de futuros docentes en el área de seguridad digital. *Revista Científica de Educomunicación*, 61(27). 57-67. https://www.revistacomunicar.com/index.php?contenido=revista&numero=61

García Aparici, J. (2012-2013). *Estudio sobre la privacidad en el uso de las redes sociales de Internet en el IES Emilio Jimeno de Calatayud* [Tesis de maestría, Universidad Nacional de Educación a Distancia]. http://e-spacio.uned.es/fez/eserv/bibliuned:masterComEdred-Jlgarcia/Documento.pdf

García Ávila, S. (2017). Alfabetización Digital. *Revista Razón y Palabra*, 21(98), 66-81. https://www.redalyc.org/pdf/1995/199553113006.pdf

García Maldonado, G., Joffre Velázquez, V., Martínez Salazar, G. y Llanes Castillo, A. (2011). Ciberbullying: forma virtual de intimidación escolar. *Revista Colombiana de Psiquiatría*, 40(1), 115-129. http://www.scielo.org.co/pdf/rcp/v40n1/v40n1a10.pdf

García Muños, T. (2003). El cuestionario como instrumento de

investigación/evaluación. Universitario Santa Ana. http://www.univsantana.com/sociologia/El_Cuestionario.pdf

García Piña, C. (2008). Riesgos del uso de internet por niños y adolescentes. Estrategias de seguridad. *Revista Acta Pediátrica de México*, 29(5), 272-278. https://www.redalyc.org/pdf/4236/423640313006.pdf

García Sandoval, C. (2013). Competencias digitales para los ciudadanos del siglo XXI. Universidad Femenina del Sagrado Corazón. *Revista de la Facultad de Ciencias de la Educación,* (19), 12-13. *https://revistas.unife.edu.pe/index.php/educacion/article/view/1015*

García Valcárcel, A. (2016). *Las competencias digitales en el ámbito educativo.* Universidad de Salamanca. https://gredos.usal.es/bitstream/handle/10366/130340/Las%20competencias%20digitales%20en%20el%20ambito%20eductivo.pdf?sequence=1

García Valcárcel, A., Salvador Blanco, L., Casillas Martín, S. y Basilotta Gómez, V. (2019). Evaluación de las competencias digitales sobre seguridad de los estudiantes de Educación Básica. *Revista de Educación a Distancia,* 19(61), 2-28. https://revistas.um.es/red/article/view/398031/273721

Garmendia, M., Garitaonandia, C., Martínez, G. y Casado, M. (2012). Los menores en internet. Usos y seguridad desde una perspectiva europea. *Revista Quaderns del CAC 38,* XV (1), 37-44. https://www.cac.cat/sites/default/files/2019-01/Q38_garmendia_et_al_ES.pdf

Gónzales Rodríguez, E. (2013) *Uso de internet en los estudiantes de la preparatoria NO.11* [Tesis de Maestría, Universidad Autónoma de Nuevo León]. http://eprints.uanl.mx/3490/1/1080256733.pdf{

Gonzáles, N. y Fernández, V. (2015). DigComp o la necesaria adecuación al marco común de referencia en competencias digitales. *Revista Anuario ThinkEPI*, 9, 30-35. https://recyt.fecyt.es/index.php/ThinkEPI/article/view/thinkepi.2015.04

González Calatayud, V., Román Garcia, M. y Prendes Espinoza, M. P. (2018). Formación en competencias digitales para estudiantes universitarios basada en el modelo DIGCOMP. *Revista Electrónica de Tecnología Educativa*, (65), 1-14. https://www.edutec.es/revista/index.php/edutec-e/article/view/1119/pdf

Gros, B. y Contreras, D. (2006). La alfabetización digital y el desarrollo de competencias ciudadanas. *Revista Iberoamericana de Educación*, (42). https://rieoei.org/historico/documentos/rie42a06.htm

Hazar, E. (2018). Digital competence in primary education: The case of Turkish language, mathematics and personal and social development courses. *International Online Journal of Education and Teaching* (IOJET), 5(2),443-458.https://files.eric.ed.gov/fulltext/ED592527.pdf

Henríquez Coronel, P., Gisbert Cervera, M. y Fernández Fernández, I. (2018). La

evaluación de la competencia digital de los estudiantes: una revisión al caso latinoamericano. Revista Latinoamericana de Comunicación, (137). 93-112. https://www.redalyc.org/journal/160/16057171013/html/

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la investigación (6° edición ed.). *México DF: Mc Graw Hill.* https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Hernández, R., Fernández, C., & Baptista, P. (2006). Metodología de la investigación (4° edición ed.). *México DF: Mc Graw Hill.* https://investigar1.files.wordpress.com/2010/05/1033525612mtis_sampieri_unidad_1-1.pdf

Herreros Martínez, P. J. (2014). Competencias clave para el aprendizaje permanente. Un marco de referencia europeo. *Revista Supervisión,* 21(34), 1-2. https://usie.es/supervision21/wp-content/uploads/sites/2/2020/01/SP-21-34-ESTUDIOS_Competencias_claves.pdf

Ikano. (s.f). *Marco europeo de competencias digitales DIGCOMP.* https://ikanos.eus/recursos/documentos-digcomp/

Instituto Nacional de Estadística e Informática. (25 de junio de 2020). *El 40,1% de los hogares del país tuvo acceso a Internet en el primer trimestre del 2020.* https://www.inei.gob.pe/prensa/noticias/el-401-de-los-hogares-del-pais-tuvo-acceso-a-internet-en-el-primer-trimestre-del-2020-12272/

Instituto Nacional de Estadística e Informática. (2021). *Estadística de las tecnologías de información y comunicación en los hogares.* https://www.inei.gob.pe/media/MenuRecursivo/boletines/02-informe-tecnico-tic-i-trimestre-2021.pdf

Instituto Nacional de Tecnología Educativas y de Formación del Profesorado. (2015). *Las competencias clave.* Formación en Red. http://formacion.intef.es/pluginfile.php/109467/mod_resource/content/1/Las%20competencias%20clave.pdf

Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado. (s.f.). *Seguridad del menor en internet*. https://intef.es/tecnologia-educativa/seguridad-del-menor-en-internet/

Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales. (s.f.). Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital. https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/5RecomendacionesPDP_Web.pdf

Instituto tecnológico InGenio Learning. (25 de enero de 2021). *Educación en ciberseguridad: Nuevos retos para educadores.* https://ingenio.edu.pe/educacion-en-ciberseguridad-nuevos-retos-para-ed

ucadores/

Laura Lloret, M. (2014). *Ciberbullying: entre operaciones, estadios y operatorias* [Tesis de Licenciatura, Universidad del Aconcagua]. http://190.183.61.20/objetos_digitales/600/tesis-3782-ciberbullying.pdf

Levano Francia, L., Sanchez Díaz, S., Guillén Aparicio, P., Tello Cabello, S. Herrera Paico, N. y Collantes Inga, Z. (2019). Competencias digitales y educación. *Revista Propósitos y Representaciones,* 7(2), 569-580. http://www.scielo.org.pe/pdf/pyr/v7n2/a22v7n2.pdf

Maqueo Ramírez, M., Moreno Gonzáles, J. y Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho*, 30(1). https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-09502017000100004

Martínez Uribe, C. (2008). La educación a distancia: sus características y necesidad en la educación actual. *Revista Educación, 17 (33)*, 7-27. https://revistas.pucp.edu.pe/index.php/educacion/article/view/1532

Mathers, N., Fox, N. y Hunn, A. (2002). Trent focus for research and development in primary health care. Trent Focus Group. http://web.simmons.edu/~tang2/courses/CUAcourses/lsc745/sp06/Interviews.pd

Mehboobe, M., Heidari, E. Farrokhnia, M. & Noroozi, O. (2021). The mediating role of digital informal learning in the relationship between students' digital competence and their academic performance. *Computing and Education Magazine,* 167, 2-7. https://www.sciencedirect.com/science/article/abs/pii/S0360131521000610?via%3Dihub

Mendoza López, E. (2012). Acoso cibernético o cyberbullying: Acoso con la tecnología electrónica. *Pediatría de México*, 14/3), 133-146. https://www.medigraphic.com/pdfs/conapeme/pm-2012/pm123g.pdf

Ministerio de Educación de Chile. (2013). *Matriz de Habilidades TIC para el Aprendizaje.* Centro de Educación y Tecnología, Enlaces.http://www.enlaces.cl/sobre-enlaces/habilidades-tic-en-estudiantes/

Ministerio de Educación. (2016). Programa curricular de Educación Primaria. http://www.minedu.gob.pe/curriculo/pdf/programa-curricular-educacion-primaria.pdf

Ministerio del Interior y Seguridad Pública de Chile. (2020). Procedimientos suplantación de identidad en R.R.S.S. https://www.csirt.gob.cl/media/2020/07/Procedimiento-para-denunciar-suplantaci%C3%B3n-de-identidad-en-redes-sociales.pdf

Ministerio del Interior. (03 de marzo de 2021). Recomendaciones de uso seguro de Internet para menores de edad.

https://www.gob.pe/12799-recomendaciones-de-uso-seguro-de-internet-para-

Monje Álvarez, C. (2011). *Metodología de la investigación cuantitativa y cualitativa.* Universidad Surcolombiana. https://www.uv.mx/rmipe/files/2017/02/Guia-didactica-metodologia-de-la-investigacion.pdf

Muñoz Loayza, B. (2018). *Ventajas y desventajas del muestreo probabilístico y no probabilístico en investigación científicas* [Tesis de licenciatura, Universidad Técnica de Machala]. http://repositorio.utmachala.edu.ec/bitstream/48000/12838/1/ECUACE-2018-CA-DE00859.pdf

Muñoz Recio, F. (2019). *La competencia digital: Un desafío para docentes y alumnos*. Universidad Nacional de Educación a Distancia (UNED). https://www.researchgate.net/publication/331984626_LA_COMPETENCIA_DIGITAL_UN_DESAFIO_PARA_DOCENTES_Y_ALUMNOS

Naciones Unidas. (2020). *Informe: El impacto del COVID-19 en América Latina y el Caribe.* https://peru.un.org/sites/default/files/2020-07/SG%20Policy%20brief%20COVID%20LAC%20%28Spanish%29_10%20July_0.pdf

Ordoñez Pineda, L. y Calva Jiménez, S. (2020). Amenazas a la privacidad de los menores de edad a partir del Sharenting. Revista Chilena de derecho y tecnología, 9(2). https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000200105

Organización para la Cooperación y el DesarrolloEconómicos. (2020). *Aprovechar al máximo la tecnología para el aprendizaje y la formación en América Latina.* Editorial OECD. https://www.oecd.org/skills/centre-for-skills/Aprovechar_al_m%C3%A1ximo_la_tecnolog%C3%ADa_para_el_aprendizaje_y_la_formaci%C3%B3n_en_Am%C3%A9rica_Latina.pdf

Orosco Fabian, J., Gómez Galindo, W., Pomasunco Huaytalla, R., Salgado Samaniego, E. y Álvarez Casabona, R. (2021). Competencias digitales en estudiantes de educación secundaria de una provincia del centro del Perú. *Revista Educación*, 45(1), 2-14. https://revistas.ucr.ac.cr/index.php/educacion/article/view/41296/45332

Otzen. T y Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *Revista Int. J. Morphol*, 35(1), 227-232. https://scielo.conicyt.cl/pdf/ijmorphol/v35n1/art37.pdf

Palmer Padilla, J. (2017). *Seguridad y riesgos: Cyberbullying, grooming y sexting.* http://openaccess.uoc.edu/webapps/o2/bitstream/10609/67105/6/fpalmerpTFM0617memoria.pdf

Patiño Rivera, A. (2020). Por una educación a distancia. https://tarea.org.pe/wp-content/uploads/2020/08/Tarea100_16_Alberto_Pa

tino_Rivera.pdf

Pavez, M. (2014). *Los derechos de la infancia en la era de Internet. América Latina y las nuevas tecnologías*. Comisión Económica para América Latina y el Caribe y Fondo de las Naciones Unidas para la Infancia. https://repositorio.cepal.org/bitstream/handle/11362/37049/1/S1420497_es.pdf

Peñalva Vélez, A., Napal Fraile, M. y Mendioros Lacambra, A. M. (2018). Competencia digital y alfabetización digital de los adultos (profesorado y familias). *Revista International Journal of New Education*, 1 (1), 3-8. https://dialnet.unirioja.es/servlet/articulo?codigo=6938587

Pere Marqués, G. (2008*). Los riesgos de internet. consejos para su uso seguro. Habilidades necesarias para utilizar internet*. https://ddd.uab.cat/pub/dim/16993748n2/16993748n2a4.pdf

Pérez, G. (2007). Desafíos de la investigación cualitativa. Universidad Nacional de Educación a Distancia (UNED). https://www.academia.edu/6457324/DESAF%C3%8DOS_DE_LA_INVESTIGACI%C3%93N_CUALITATIVA

Pineda Torres, L.F. (2018). Percepciones de los estudiantes sobre el uso de tic en el proceso de aprendizaje de una lengua extranjera como el inglés en la institución educativa San Antonio de Padua del municipio de Támesis, Antioquia [Tesis de Maestría, Universidad Pontificia Bolivariana]. https://repository.upb.edu.co/bitstream/handle/20.500.11912/4355/Percepciones%20de%20los%20estudiantes%20sobre%20el%20uso%20de%20TIC%20en%20el%20proceso%20de%20aprendizaje%20de%20una%20lengua%20extranjera%20como%20el%20ingl%C3%A9s.pdf?sequence=1&isAllowed=y

Pontificia Universidad Católica del Perú. (2019). Reglamento del comité de ética de la investigación de la Pontificia Universidad Católica del Perú. Pontificia Universidad Católica del Perú. https://departamento.pucp.edu.pe/psicologia/wp-content/uploads/2019/08/reglam

Quecedo, R. y Castaño, C. (2002). Introducción a la metodología de investigación cualitativa. *Revista de Psicodidáctica*, 14, 5-22. https://www.redalyc.org/pdf/175/17501402.pdf

Represa Estrada, C. (11 febrero de 2020). *Avanzando con seguridad en el futuro de la educación.* https://ieducando.com/nuestro-blog/2020/02/11/avanzando-con-seguridad-en-el-futuro-de-la-educacion

Romero Chaves, C. (2005). La categorización un aspecto crucial en la investigación cualitativa. *Revista de Investigaciones Cesmag,* 11(11), 1-4. *http://aprendeenlinea.udea.edu.co/lms/moodle/pluginfile.php/159995/mod_resource/content/0/LA_CATEGORIZACION_UN_ASPECTO_CRUCIAL_*

EN_LA_INVESTIGACIONCUALITATIVA.pdf

Salinas, A., Jara, I., San Martín, E. Claro, M. y Cortés, F. (2016). Nuevos desafíos pedagógicos: Estrategias de enseñanza para el manejo de TICs. *Revista Centro de Estudios de Políticas y Prácticas en Educación*, (12), 2-5. .http://ceppe.uc.cl/images/contenido/policy-briefs/CEPPE_N12-Nuevos_desafios_pedagogicos-Estrategias_de_ensenanza_para_el_manejo_de_TICs.pdf

Sánchez Antolín, P., Andrés Viloria, C. y Paredes Labra, J. (2018). El papel de la familia en el desarrollo de la competencia digital. Análisis de cuatro casos. *Revista* Digital *Education Review*, (34), 45-54. https://revistes.ub.edu/index.php/der/article/view/20750/pdf

Sánchez Teruel, D. y Robles Bello, M. (2016). Riesgos y potencialidades de la era digital para la infancia y la adolescencia. *Revista Educación y Humanismo*, 18(31), 186-204. http://revistas.unisimon.edu.co/index.php/educacion/article/view/2358/2250

Sequera, M., Toledo, A. y Ucciferri, L. (2018). *Derechos humanos y seguridad digital: Una pareja perfecta.* https://privacyinternational.org/sites/default/files/2018-06/La-pareja-perfecta-DDHH-y-Seguridad-Digital.pdf

Tolosa Quintero, N. J. (2017). *Percepción de la calidad del proceso de enseñanza aprendizaje del curso virtual de salud pública de la universidad de los Llanos* [Tesis de especialidad, Universidad Cooperativa de Colombia]. https://repository.ucc.edu.co/bitstream/20.500.12494/8430/1/2019_percepcion_calidad_ensenanza.pdf

Universidad de Alicante. (s.f.). *Identidad digital.* https://rua.ua.es/dspace/bitstream/10045/79589/2/ci2_basico_2017-18_La_identidad_digital.pdf

Zuñiga Becerra, O. (2018). Educación y prevención en materia de protección de datos personales de niños, niñas y adolescentes en internet. *Revista Jurídica UNAM,* 5, 69-75. https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/12122/13806

ANEXOS

1. Matriz de consistencia

Título de la investigación	Percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana.			
Pregunta problema	¿Cuáles son las percepciones de los estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana?			
Objetivo general	Analizar las percepciones de los estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana.			
Objetivos específicos	Categorías	Subcategorías	Técnicas e Instrumentos	Fuente de información
Describir las percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana.	Competencias digitales en seguridad	Protección de datos personales y privacidad. Protección de salud y bienestar	Técnica: Entrevista Instrumento: Guía de entrevista semiestructurada	Alumno del sexto grado "A"
Describir el nivel de competencias digitales en seguridad de estudiantes de 6to grado de primaria en una institución educativa pública de Lima Metropolitana.			Técnica: Encuesta Instrumento: cuestionario	Alumno del sexto grado "A"

2. Formulario de selección de informantes

Criterios de selección	Opciones de respuesta	
Nombres y apellido:		
Pertenecen al sexto grado "A"	SI	NO
Utilizas internet para realizar actividades académicas y de entretenimiento.	SI	NO
Utilizas las redes sociales como facebook, instagram, WhatsApp, etc.	SI	NO

3. Diseño de la guía de entrevista

Objetivo	Describir las percepciones de los estudiantes sobre sus competencias digitales en seguridad
Código del entrevistado	
Datos personales	

<table>
<tr><td>Sexo</td><td>Varón</td><td>Edad</td><td>12</td></tr>
<tr><td>Fecha</td><td>5/11/21</td><td>Hora</td><td>2:00 p.m</td></tr>
<tr><td>Recurso para la realización de la entrevista</td><td colspan="3">Videoconferencia por medio de la plataforma online de ZOOM</td></tr>
<tr><td>Protocolo a seguir en la entrevista</td><td colspan="3">- Se inicia la entrevista con un saludo y agradecimiento por participar.
- Presentación del investigador.
- Presentación del tema de investigación y los objetivos de la misma.
- Se indica que la investigación es de carácter privado y académico, y no se dará a conocer los nombre de los entrevistados.
- Se menciona que para recolectar la información se grabará la sesión del Zoom.
- Se le solicitará la carta de consentimiento informado firmado por su apoderado.
- Se realizará la entrevista siguiendo el orden de las preguntas.
- Si el entrevistado/da desvié de la pregunta se tendrá que intervenir planteando de nuevo la pregunta, ya que es una entrevista semi estructurada.
- Se guardan todos los materiales usados en la entrevista y se agradece al entrevistado/da por habernos brindado su valioso tiempo.</td></tr>
<tr><td colspan="2">Aspectos sobre sobre los que se entrevistará</td><td colspan="2">Items de entrevista</td></tr>
<tr><td rowspan="9">Categoría: Competencias digitales en seguridad</td><td rowspan="6">Subcategoría 1: Protección de datos personales y privacidad</td><td colspan="2">Usas redes sociales, como por ejemplo Facebook, Instagram, Telegram, etc. ¿Cuáles empleas? ¿Con qué frecuencia?
¿Públicas información personal en las redes sociales?
¿Qué tipo de información compartes?</td></tr>
<tr><td colspan="2">¿Conoces qué información personal no debes compartir cuando navegas en páginas de internet o redes sociales?</td></tr>
<tr><td colspan="2">¿De qué manera proteges tu información personal cuando accedes a las redes sociales o a páginas web?</td></tr>
<tr><td colspan="2">Cuando ingresas a las redes sociales, ¿de qué manera respetas la privacidad de los otros?</td></tr>
<tr><td colspan="2">¿Has tenido algún episodio que consideras una violación a tu privacidad en internet en los últimos tres años?</td></tr>
<tr><td colspan="2">¿Qué acciones o medidas empleas si descubres que una persona utiliza tu identidad para delitos</td></tr>
<tr><td rowspan="3">Subcategoría 2: Protección de salud y bienestar</td><td colspan="2">¿Conoces los riesgos y sus consecuencias de los diferentes acosos cibernéticos?</td></tr>
<tr><td colspan="2">¿Tienes cuidado con los aspectos de postura o cuidado de la salud (iluminación, audífonos en alto volumen, pantalla, sedentarismo, postura, etc.) al usar algún dispositivo?
¿Qué acciones realizas?</td></tr>
<tr><td colspan="2">¿Qué consecuencias puede generar el uso inadecuado de las redes sociales y la navegación en las páginas web a tu salud? ¿Cómo evitas?</td></tr>
</table>

4. Diseño del cuestionario de la encuesta

<table>
<tr><td>Objetivo</td><td colspan="3">Describir el nivel de competencias digitales en seguridad.</td></tr>
<tr><td>Código del encuestado</td><td colspan="3"></td></tr>
<tr><td>Sexo</td><td></td><td>Edad</td><td></td></tr>
<tr><td>Recurso para la realización de la encuesta</td><td colspan="3">Formulario del google gmail</td></tr>
<tr><td>Protocolo a seguir en la encuesta</td><td colspan="3">Saludo y agradecimiento:
Estimado (a) estudiante, de antemano se agradece su disposición y tiempo para participar en la investigación titulada “Percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana”, así como para responder a este cuestionario.

Objetivo del cuestionario
El presente cuestionario tiene como finalidad conocer el nivel de competencias digitales en seguridad del modelo DigComp (protección de datos personales, de la salud y del medioambiente) que posee. Su participación es voluntaria y anónima, y la información recogida será estrictamente confidencial, por lo que se utilizará solamente para fines de este trabajo de investigación. Siéntase libre de preguntar si tiene alguna duda, o de finalizar su participación en cualquier momento.

Recomendaciones
Es importante que complete todos sus datos personales.
Los ítems presentan situaciones en las que debes de seleccionar la respuesta correcta.
El cuestionario puede ser desarrollado en el tiempo que considere necesario.</td></tr>
<tr><td colspan="2">Aspectos sobre sobre los que se encuesto</td><td colspan="2">Items de entrevista</td></tr>
<tr><td rowspan="3">Categoría: Competencias digitales en seguridad</td><td rowspan="3">Subcategoría 1: Protección de datos personales y privacidad</td><td colspan="2">1. Si publico fotos o datos sobre mi familia, como fotos de mi casa, la profesión de mis padres, el colegio donde estudió, la dirección de mi casa, número de celular, en Internet:

a) La información la controlo yo y la puedo borrar cuando quiera.
b) Una vez que publico algo en Internet pierdo el control sobre ello (correcta).
c) La información no afectará en ningún caso a mi futuro ni al de mi familia.</td></tr>
<tr><td colspan="2">2. Si descubro que una persona ha creado un perfil falso con mis datos personales y sobre mi familia en mi red social:

a) Le envió un mensaje a la persona solicitando que elimine el perfil creado.
b) Envío un mensaje a mis contactos por medio de una publicación informando que han creado un perfil falso con mis datos personales para que eviten responder a ese perfil.
c) Envió un mensaje a la red social denunciando la existencia de un perfil falso para que lo eliminen (correcta)..</td></tr>
<tr><td colspan="2">3. ¿Cuáles de las siguientes publicaciones no pondría en peligro la protección de mi identidad?

a) Una fotografía en la puerta de mi casa en la que aparece el número y nombre de la calle.
b) Una fotografía de las vacaciones del último verano con mi familia.</td></tr>
</table>

		c) Un comentario personal sobre una noticia que he leído en el periódico (correcta).
		4. Cuando accedes a las redes sociales u otras páginas web ¿de qué manera proteges tu información personal? a) Si un compañero de clase descubre la contraseña de mi correo electrónico o redes sociales podría: b) Utilizo la opción de modo incógnito, reviso las opciones de seguridad y privacidad del navegador y no almaceno contraseñas de forma predeterminada en los navegadores. c) Configuro la opción de privacidad; utilizo contraseñas seguras y configuro la opción sobre que personas solo pueden observar todo lo que subo. Todas las anteriores (correcta).
		5. En el caso de que haya recibido una información personal de uno de mis amigos(as) sin su consentimiento, ¿qué debería hacer? a) Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios (correcta). b) Sigo compartiendo esa información con el resto de mis amigos. c) Lo guardo en la galería de cualquier dispositivo tecnológico para luego publicarlo en las redes sociales.
	Subcategoría 2: Protección de salud y bienestar	6. Para evitar problemas de acoso a través de Internet: a) Confío en personas que conozco y quieren contactarse conmigo (correcta). b) Solo me comunico con otros si es presencialmente. c) Utilizo una falsa personalidad en la Red.
		7. Cuando uso el ordenador, tablet, celular, TV, consola de videojuegos... en mi casa: a) Me siento correctamente en una silla, sofá, sillón, etc. y empleo trípode para sostener el equipo tecnológico (correcta). b) Muchas veces me terminan doliendo la espalda, piernas o cuello. c) Suelo sentir cansancio rápidamente.

5. Carta de solicitud para la validación de los instrumentos

CARTA DE PRESENTACIÓN

Mag. Sylvana Mariella Valdivia Cañotte

Presente

Asunto: **Validación de instrumentos por juicio de experto**

Me es grato comunicarme con usted para expresarle mi saludo y así mismo, hacer de su conocimiento que, siendo estudiante de la Facultad de Educación primaria en la Pontificia Universidad Católica del Perú, me permito solicitar su atención, en calidad de experto(a), debido a que tengo referencia de su larga trayectoria en temas educativos y en investigación educativa.

Actualmente, estoy desarrollando el trabajo de investigación para optar por el título de licenciado en Educación Primaria**,** el cual se denomina "Percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana".

En esa línea, me encuentro en el proceso del planteamiento del diseño metodológico y elaboración de instrumentos, para lo cual he considerado las técnicas de entrevista y encuesta, con la finalidad de recoger la información de los estudiantes en relación a sus competencias digitales en seguridad basada en el **modelo DigComp.** Por ello, he considerado conveniente recurrir a usted a fin de que pueda emitir valoraciones, comentarios y juicios sobre la claridad, coherencia y relevancia de los instrumentos diseñados; con lo cual se garantice que las preguntas y/o ítems formulados guarden relación con los objetivos, categorías y subcategorías que conforman la investigación.

Adjunto:
1. Matriz de consistencia
2. Instrumentos
3. Ficha de validación de los instrumentos

Expresando mi respeto y consideración a usted, me despido no sin antes agradecerle por la atención y su pronta respuesta.

Atentamente
Michael Santiago Bautista Altamirano
Código: 20162474

CARTA DE PRESENTACIÓN

Lic. Rossangel Cuentas Ramírez

Presente

Asunto: **Validación de instrumentos por juicio de experto**

Me es grato comunicarme con usted para expresarle mi saludo y así mismo, hacer de su conocimiento que, siendo estudiante de la Facultad de Educación primaria en la Pontificia Universidad Católica del Perú, me permito solicitar su atención, en calidad de experto(a), debido a que tengo referencia de su larga trayectoria en temas educativos y en investigación educativa.

Actualmente, estoy desarrollando el trabajo de investigación para optar por el título de licenciado en Educación Primaria***,*** el cual se denomina “Percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana".

En esa línea, me encuentro en el proceso del planteamiento del diseño metodológico y elaboración de instrumentos, para lo cual he considerado las técnicas de entrevista y encuesta, con la finalidad de recoger la información de los estudiantes en relación a sus competencias digitales en seguridad basada en el **modelo DigComp.** Por ello, he considerado conveniente recurrir a usted a fin de que pueda emitir valoraciones, comentarios y juicios sobre la claridad, coherencia y relevancia de los instrumentos diseñados; con lo cual se garantice que las preguntas y/o ítems formulados guarden relación con los objetivos, categorías y subcategorías que conforman la investigación.

Adjunto:
1. Matriz de consistencia
2. Instrumentos
3. Ficha de validación de los instrumentos

Expresando mi respeto y consideración a usted, me despido no sin antes agradecerle por la atención y su pronta respuesta.

Atentamente
Michael Santiago Bautista Altamirano
Código: 20162474

6. Ficha de validación de instrumentos

Instrumento N° 1: Guía de entrevista semiestructurada

Datos del investigador: Michael Santiago Bautista Altamirano, estudiante de la Facultad de Educación de la Pontificia Universidad Católica del Perú.

Criterios de validación: Los criterios de validación son claridad, coherencia y relevancia, considerando la definición de estos de acuerdo con el siguiente cuadro.

Criterio	Claridad	Coherencia	Relevancia
Definición	El ítem elaborado se llega a comprender sin dificultad, es decir, la redacción garantiza propiedad sintáctica y gramatical.	El ítem elaborado tiene relación lógica con la categoría y subcategoría.	El ítem planteado resulta pertinente y relevante, teniendo en cuenta la categoría y subcategoría y los objetivos de la investigación.

Categoría	subcategorías	Preguntas	Claridad		Coherencia		Relevancia		Comentario/ Sugerencia
			SÍ	NO	SÍ	NO	SÍ	NO	
Competencias digitales en seguridad	**Subcategoría 1:** Protección de datos personales y privacidad	Usas redes sociales, como por ejemplo Facebook, Instagram, Telegram, etc. ¿Cuáles empleas? ¿Con qué frecuencia? ¿Públicas información personal en las redes sociales? ¿Qué tipo de información compartes?							
		¿Conoces qué información personal no debes compartir cuando navegas en páginas de internet o redes sociales?							
		¿De qué manera proteges tu información personal cuando accedes a las redes sociales o a páginas web?							
		Cuando ingresas a las redes sociales, ¿de qué manera respetas la privacidad de los otros?							
		¿Has tenido algún episodio que consideras una violación a tu privacidad en internet en los últimos tres años?							
		¿Qué acciones o medidas empleas si descubres que una persona utiliza tu identidad para cometer delitos?							
	Subcategoría 2: Protección de la salud y bienestar	¿Conoces los riesgos y sus consecuencias de los diferentes acosos cibernéticos?							
		¿Tienes cuidado con los aspectos de postura o cuidado de la salud (iluminación, audífonos en alto volumen, pantalla, sedentarismo, postura, etc.) al usar algún dispositivo? ¿Qué acciones realizas?							

		¿Qué consecuencias puede generar el uso inadecuado de las redes sociales y la navegación en las páginas web a tu salud? ¿Cómo evitas?							

Instrumento N° 2: Cuestionario

Criterios de validación: Los criterios de validación son claridad, coherencia y relevancia, considerando la definición de estos de acuerdo con el siguiente cuadro.

Criterio	Claridad	Coherencia	Relevancia
Definición	El ítem elaborado se llega a comprender sin dificultad, es decir, la redacción garantiza propiedad sintáctica y gramatical.	El ítem elaborado tiene relación lógica con la categoría y subcategoría.	El ítem planteado resulta pertinente y relevante, teniendo en cuenta la categoría y subcategoría y los objetivos de la investigación.

Categoría	subcategorías	Preguntas	Claridad		Coherencia		Relevancia		Comentario/sugerencia
			SI	NO	SI	NO	SI	NO	
Competencias digitales en seguridad	Subcategoría 1: Protección de datos personales y privacidad	1. Si publico fotos o datos sobre mi familia, como fotos de mi casa, la profesión de mis padres, el colegio donde estudió, la dirección de mi casa, número de celular, etc. en Internet: a) La información la controlo yo y la puedo borrar cuando quiera. b) Una vez que publico algo en Internet pierdo el control sobre ello (correcta). c) La información no afectará en ningún caso a mi futuro ni al de mi familia.							
		2. Si descubro que una persona ha creado un perfil falso con mis datos personales y sobre mi familia en mi red social: a) Le envió un mensaje a la persona solicitando que elimine el perfil creado. b) Envío un mensaje a mis contactos por medio de una publicación informando que han creado un perfil falso con mis datos personales para que eviten responder a ese perfil. c) Envió un mensaje a la red social denunciando la existencia de un perfil falso para que lo eliminen (correcta).							

		3. ¿Cuáles de las siguientes publicaciones no pondría en peligro la protección de mi identidad? a) Una fotografía en la puerta de mi casa en la que aparece el número y nombre de la calle. b) Una fotografía de las vacaciones del último verano con mi familia. c) Un comentario personal sobre una noticia que he leído en el periódico (correcta).							
		4.Cuando accedes a las redes sociales u otras páginas web ¿de qué manera proteges tu información personal? a) Utilizo la opción de modo incógnito, reviso las opciones de seguridad y privacidad del navegador y no almaceno contraseñas de forma predeterminada en los navegadores. b) Configuro la opción de privacidad; utilizo contraseñas seguras y configuro la opción sobre que personas solo pueden observar todo lo que subo. c) Todas las anteriores (correcta).							
		5. En el caso de que haya recibido una información personal de uno de mis amigos(as) sin su consentimiento, ¿qué debería hacer? a) Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios (correcta). b) Sigo compartiendo esa información con el resto de mis amigos. c) Lo guardo en la galería de cualquier dispositivo tecnológico para luego publicarlo en las redes sociales.							
	Subcategoría 2: Protección de salud y bienestar	6. Para evitar problemas de acoso a través de Internet:							

		a) Confío en personas que conozco y quieren contactarse conmigo (correcta). b) Solo me comunico con otros si presencialmente. c) Utilizo una falsa personalidad en la Red.							
		7. Cuando uso el ordenador, tablet, celular, TV, consola de videojuegos... en mi casa: a) Me siento correctamente en una silla, sofá, sillón, etc. y empleo trípode para sostener el equipo tecnológico (correcta). b) Muchas veces me terminan doliendo la espalda, piernas o cuello. c) Suelo sentir cansancio rápidamente.							

7. Consentimiento informado

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAR A LOS PARTICIPANTES

Estimado/a participante:
Le pedimos su apoyo en la realización de una investigación conducida por Michael Santiago Bautista Altamirano, estudiante de la Facultad de Educación de la Pontificia Universidad Católica del Perú, en la especialidad de Educación Primaria. La investigación, denominada "Percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana", tiene como propósito "analizar las percepciones de los estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana".
Su aporte como estudiante del sexto grado "A" del turno mañana de educación primaria, será de gran valor. Si usted accede a participar en esta encuesta, se le solicitará responder diversas preguntas sobre el tema antes mencionado, lo que le tomará aproximadamente entre 20 a 30 minutos. Debe saber que, la información obtenida será utilizada únicamente en el marco del presente estudio y su identidad será guardada con rigurosidad, en coherencia con los principios éticos de la investigación.

Dada la emergencia sanitaria, la encuesta se enviará a su correo a través del Google Form para que pueda registrar con tranquilidad la información. La información será almacenada únicamente por la investigadora en su computadora personal, pero, luego de haber publicado la investigación, ésta será eliminada.
Su participación en la investigación es completamente voluntaria. Usted puede interrumpir la misma en cualquier momento, sin que ello genere ningún perjuicio. Además, si tuviera alguna consulta sobre la investigación, puede formularla cuando lo estime conveniente, a la dirección que compartimos más abajo, a fin de clarificarla oportunamente.
Al concluir la investigación, le enviaremos a su dirección electrónica, un resumen ejecutivo del informe de la investigación, donde compartiremos los principales resultados, conclusiones y sugerencias del estudio.
En caso de tener alguna duda sobre la investigación, no dude en comunicarse al siguiente correo electrónico: a20162474@pucp.edu.pe o al número 920731541.
Desde ya, gracias por sus valiosos aportes.

Yo,_____, doy mi consentimiento de mi menor hijo(a) para participar en el estudio titulado Percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana. Y que los resultados obtenidos se utilicen estrictamente en el marco de esta investigación. Asimismo, estoy de acuerdo que mi identidad sea tratada de manera confidencial, es decir, que en la investigación no se hará ninguna referencia expresa de mi nombre; en tal sentido, el investigador utilizará un código de identificación o pseudónimo. Finalmente, entiendo que recibiré una copia de este protocolo de consentimiento informado.

…….. ……. ……..
Nombre completo del (de la) participante Firma Fecha

Correo electrónico del participante: ……

Michael Santiago Bautista Altamirano …… ……..
Nombre del Investigador responsable Firma Fecha

Correo electrónico del investigador responsable: a20162474@pucp.edu.pe

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENTREVISTAS PARA PARTICIPANTES

Estimado/a participante,

Le pedimos su apoyo en la realización de una investigación conducida por Michael Santiago Bautista Altamirano, estudiante de la especialidad de Educación Primaria de la Facultad de Educación de la Pontificia Universidad Católica del Perú, asesorado por la docente Roxana Villa. La investigación, denominada "Percepciones de estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana", tiene como fin "analizar las percepciones de los estudiantes de 6to grado de primaria sobre sus competencias digitales en seguridad en una institución educativa pública de Lima Metropolitana".

Se le ha contactado a usted en calidad de estudiante del sexto grado "A" del nivel primaria del turno mañana. Si usted accede a participar en esta entrevista, se le solicitará responder diversas preguntas sobre el tema antes mencionado, a través de la aplicación videoconferencia Zoom, lo que tomará aproximadamente entre 30 y 45 minutos. La información obtenida será únicamente utilizada para la elaboración de una tesis. A fin de poder registrar apropiadamente la información, se solicita su autorización para grabar la conversación. La grabación y las notas de las entrevistas serán almacenadas únicamente por el investigador en su computadora personal por un periodo de 6 meses, luego de haber publicado la investigación, y solamente él y su asesora tendrán acceso a la misma. Al finalizar este periodo, la información será borrada.

Su participación en la investigación es completamente voluntaria. Además, si tuviera alguna consulta sobre la investigación, puede formularla cuando lo estime conveniente, a fin de clarificarla oportunamente. Por último, en caso de tener alguna duda sobre la investigación, puede comunicarse al siguiente correo electrónico: a20162474@pucp.edu.pe o al número 920731541.
Desde ya le agradecemos su participación.

Yo,_____, doy mi consentimiento de mi menor hijo(a) para participar en el estudio y autorizo que mi información se utilice en este.
Asimismo, estoy de acuerdo que mi identidad sea tratada de manera (marcar una de las siguientes opciones):

	Declarada, es decir, que en la tesis se hará referencia expresa de mi nombre.
	Confidencial, es decir, que en la tesis no se hará ninguna referencia expresa de mi nombre y la tesista utilizará un código de identificación o pseudónimo.

Finalmente, entiendo que recibiré una copia de este protocolo de consentimiento informado.

…….. …… ……..

Nombre completo del (de la) participante Firma Fecha

Correo electrónico del participante: ……..

Michael Santiago Bautista Altamirano …… ……..
Nombre del Investigador responsable Firma Fecha

Correo electrónico del investigador responsable: a20162474@pucp.edu.pe

8. Matriz de triangulación

Categoría		Competencia digital en seguridad			
Subcategoría		Protección de datos personales y privacidad			
Codificación emergente	**Hallazgos de instrumento 1: Entrevista**	**Hallazgos de instrumento 2: Encuesta**	**Competencia: Protección de datos personales y privacidad**		
			Básico	**Intermedio**	**Avanzado**
			Soy consciente de que sólo puedo compartir cierto tipo de información sobre mí mismo/a y sobre otras personas. ● Conocimiento sobre que una vez que se publica algo en Internet se pierde el control. ● Conocimiento sobre qué tipos de información personal no se debe compartir en Internet. (indica al menos cuatro tipos de información) ● Conocimiento de riesgos y consecuencias que puede generar utilizar inadecuadamente las redes sociales y el internet (compartir información personal y de los demás). ● Conocimientos sobre formas básicas para proteger su información personal y privacidad en los espacios digitales, garantizando su autoprotección y de terceros de peligros digitales. ● Capacidad para seleccionar qué tipo de información personal no se debe publicar en las redes sociales para proteger la identidad. (indica al menos cuatro tipos de información) ● Actitud de prudencia en relación con los aspectos de privacidad hacia sí	Puede proteger mi propia privacidad y la de otras personas en internet y las redes sociales. Comprendo de forma general sobre las cuestiones de privacidad tengo un conocimiento básico de cómo se guardan y utilizan mis datos. ● Conocimiento sobre la importancia de la huella digital en las redes sociales e internet y el uso que pueden hacer terceras personas. ● Conocimiento sobre el uso que pueden hacer terceras personas de su identidad digital. ● Capacidad para seleccionar qué tipo de información personal no se debe publicar en las redes sociales para proteger la identidad. ● Conocimiento de estrategias para proteger la identidad en las redes sociales y de los riesgos en internet. ● Es consciente de los principios de privacidad en internet y la red social, tanto personal como la de otros. ● Capacidad para localizar información en Internet y las	A menudo cambio la configuración de privacidad predeterminada por defecto de los servicios en línea para mejorar la protección de mi privacidad. Comprendo de forma amplia sobre los problemas de privacidad y sé cómo se guardan y utilizan mis datos. ● Conocimiento de las ventajas de tener múltiples perfiles digitales para diferentes usos de la Red. ● Conocimiento de estrategias para proteger los datos de otras personas que se aplican en su propio contexto. ● Capacidad de cuidar y mejorar la identidad digital ● Capacidad de modificar o eliminar información sobre sí mismo o de otras personas de los que es responsable en el internet y las redes sociales. ● Actitud crítica cuando muestra información en línea sobre sí mismo y de otras personas. ● Conocimiento sobre el uso de datos personales por los proveedores de servicios online

			mismo y hacia los demás.	redes sociales sobre sí mismo.	con fines comerciales.

Publicación de información personal	Solo subo fotos de mi familia o míos (ENT1HE12).	La información la controlo yo y la puedo borrar cuando quiera (respuesta incorrecta). E1HE12	B X	A	I
	No comparto mi información personal, la cuenta la tengo privada (ENT2ME12).	Una vez que publico algo en Internet pierdo el control sobre ello (respuesta correcta). E2ME12		X	
	El colegio donde estudió, fotos personales y familiares, mi número de teléfono (ENT3HE12).	Una vez que publico algo en Internet pierdo el control sobre ello (respuesta correcta). E3HE12		X	
	No publicó información personal (ENT4HE11).	Una vez que publico algo en Internet pierdo el control sobre ello. (respuesta correcta). E4HE11		X	
	La ubicación de donde estamos con mis familiares cuando viajamos. Asimismo, fotos de mis familiares y mías y el nombre del colegio donde estudio (ENT5ME11).	La información no afectará en ningún caso a mi futuro ni al de mi familia. (respuesta incorrecta). E5ME11	X		
	Lo único que público son fotos mías y de mis familiares (ENT6ME12).	La información la controlo yo y la puedo borrar cuando quiera. (respuesta incorrecta). E6ME12	X		
	Publicó fotos mías (ENT7HE11)	Una vez que publico algo en Internet pierdo el control sobre ello. (respuesta correcta)		X	
	No, no público nada de información personal (ENT8HE11).	Una vez que publico algo en Internet pierdo el control sobre ello (respuesta correcta). E8HE11		X	
	Publicó fotos mías y mis contraseñas, pero utilizo una aplicación para guardar notas de forma privada (ENT9ME11).	La información la controlo yo y la puedo borrar cuando quiera. (respuesta incorrecta). E9ME11	X		
	Instagram solo público fotos mías (ENT10ME11).	La información la controlo yo y la puedo borrar cuando quiera. (respuesta incorrecta). E10ME11	X		
Datos personales que no deben ser compartidos	Mi número de teléfono, la dirección de mi casa (ENT1HE12).	Un comentario personal sobre una noticia que he leído en el periódico (Respuesta correcta). E1HE12		X	
	Mi nombre completo, dirección de mi casa y fotos mías o de mis familiares (ENT2ME12).	Un comentario personal sobre una noticia que he leído en el periódico (Respuesta correcta). E2ME12		X	
	La dirección de mi casa, número de celular o a que se dedican mis familiares (ENT3HE12).	Un comentario personal sobre una noticia que he leído en el periódico (respuesta correcta). E3HE12		X	
	La dirección de mi casa, en que colegio estudio, fotos íntimas y en qué se dedican mis padres etc. (ENT4HE11).	Una fotografía en la puerta de mi casa en la que aparece el número y nombre de la calle (respuesta incorrecta). E4HE11	X		
	La dirección de mi casa, mi número de teléfono, tampoco a que se dedican mis padres (ENT5ME11).	Una fotografía en la puerta de mi casa en la que aparece el número y nombre de la calle (respuesta incorrecta). E5ME11	X		
	La dirección de mi casa, fotos, oficio de mis padres o del colegio donde estudio (ENT6ME12).	Una fotografía en la puerta de mi casa en la que aparece el número y nombre de la calle (respuesta incorrecta). E6ME12	X		
	La ubicación o dirección de mi casa, mi número de teléfono o el oficio de mis padres (ENT7HE11).	Una fotografía en la puerta de mi casa en la que aparece el número y nombre de la calle (respuesta incorrecta). E7HE11	X		
	La dirección de mi casa, la dirección de donde trabajan mis padres, el colegio donde estudio o fotos mías (ENT8HE11).	Un comentario personal sobre una noticia que he leído en el periódico (respuesta correcta). E8HE11		X	

	La ubicación de donde me encuentro, el número de DNI de mis padres, fotos mías y de mis familiares. (ENT9ME11)	Un comentario personal sobre una noticia que he leído en el periódico (respuesta correcta). E9ME11		X	
	Mi número de teléfono, correo electrónico, y la dirección de mi casa (ENT10ME11).	Una fotografía en la puerta de mi casa en la que aparece el número y nombre de la calle (respuesta incorrecta). E10ME11	X		
Protección de datos personales	Hay una opción para poner solo pueden ver mis amigos (ENT1HE12).	Todas las anteriores (respuesta correcta). E1HE12		X	
	Pongo en privado toda la información que he subido (ENT2ME12).	Todas las anteriores (respuesta correcta). E2ME12		X	
	Yo tengo mi Facebook en privado para que solo puedan ver mis amigos o amigas lo que subo (ENT3HE12).	Todas las anteriores (respuesta correcta). E3HE12		X	
	Lo que hago es poner en privado todas mis cuentas de redes sociales (ENT4HE11).	Todas las anteriores (respuesta correcta). E4HE11		X	
	Suelo cambiar muchas veces la contraseña de mis cuentas de redes sociales (ENT5ME11).	Todas las anteriores (respuesta correcta). E5ME11		X	
	Poner en privado para que solo puedan ver las cosas que subo mis amigos (ENT6ME12).	Todas las anteriores (respuesta correcta). E6ME12		X	
	Todas mis redes sociales las tengo en privado (ENT7HE11).	Todas las anteriores (respuesta correcta). E7HE11		X	
	Toda la información que subo, ya sea fotos o videos lo pongo en privacidad (ENT8HE11).	Todas las anteriores (respuesta correcta). E8HE11		X	
	Lo que hago yo es poner en privado para que solo lo puedan ver mis amigos y familiares. (ENT9ME11)	Todas las anteriores (respuesta correcta). E9ME11		X	
	La única medida que realizo es ponerlo en privacidad con el fin de que otras personas que no conozco puedan ver mis fotos (ENT10ME11).	Todas las anteriores (respuesta correcta). E10ME11		X	
Respeto a la privacidad de otros	No comparto sus datos personales, fotos, u otro tipo de información (ENT1HE12).	Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios (respuesta correcta). E1HE12			X
	Evito compartir su información de esa persona como sus fotos, videos entre otras cosas (ENT2ME12).	Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios (respuesta correcta). E2ME12			X
	No comparto nada de su información personal porque no tengo su consentimiento (ENT3HE12).	Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios (respuesta correcta). E3HE12			X
	No comparto sus fotos o lo que sube a las redes sociales (ENT4HE11).	Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios (respuesta correcta). E4HE11			X
	No lo comparto porque no quiero que le pase algo o a su familia (ENT5ME11).	Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios (respuesta correcta). E5ME11			X
	No comparto sus fotos u otra información sin su consentimiento (ENT6ME12).	Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios (respuesta correcta). E6ME12			X
	Si publican alguna información le digo que borre esa información y no los comparto (ENT7HE11).	Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios (respuesta correcta). E7HE11			X
	No comparto sus datos personales (ENT8HE11).	Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo			X

		compartida en las redes sociales y otros medios (respuesta correcta). E8HE11			
	Cuando mis amigos me envían fotos de los lugares que están, yo no los comparto y público (ENT9ME11).	Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios (respuesta correcta). E9ME11			X
	Cuando no comparto lo que ha subido a las redes sociales (ENT10ME11).	Lo elimino e informo dicho amigo(a) sobre su información personal que está siendo compartida en las redes sociales y otros medios (respuesta correcta). E10ME11			X
Acciones frente a la suplantación de identidad	Primero recurro a mis padres para informarles de lo que me está sucediendo. Luego de ello, denunció el perfil falso (ENT1HE12).	Envió un mensaje a la red social denunciando la existencia de un perfil falso para que lo eliminen (respuesta correcta). E1HE12		X	
	Me contactaría con mis amigos, informarles a mis amigos que se ha creado un perfil falso con mi nombre y contactar con la página para que lo puedan eliminar o bloquear ese perfil falso (ENT2ME12).	Envío un mensaje a mis contactos por medio de una publicación informando que han creado un perfil falso con mis datos personales para que eviten responder a ese perfil (respuesta correcta) E2ME12		X	
	En caso de que alguien haya creado un perfil falso con mis datos personales denunció la cuenta (ENT3HE12).	Envió un mensaje a la red social denunciando la existencia de un perfil falso para que lo eliminen (Respuesta correcta). E3HE12		X	
	Denunciar la cuenta por medio de las redes sociales, informando a mis amigos que se ha creado un perfil falso con mis datos personales (ENT4HE11).	Envió un mensaje a la red social denunciando la existencia de un perfil falso para que lo eliminen (respuesta correcta). E4HE11		X	
	Publicaría un mensaje o video informando que se ha creado una cuenta falsa, que está robando mis datos personales y diría a mis amigos que tengan cuidado (ENT5ME11).	Envío un mensaje a mis contactos por medio de una publicación informando que han creado un perfil falso con mis datos personales para que eviten responder a ese perfil (respuesta incorrecta). E5ME11	X		
	Le escribiría a esa persona que elimine esa cuenta, le insistiría que lo haga (ENT6ME12).	Envió un mensaje a la red social denunciando la existencia de un perfil falso para que lo eliminen (respuesta correcta) E6ME12		X	
	Lo primero que haría sería denunciar el perfil por daños a mi privacidad (ENT7HE11).	Envió un mensaje a la red social denunciando la existencia de un perfil falso para que lo eliminen (respuesta correcta). E7HE11		X	
	Le informaría a mis padres para que me ayuden (ENT8HE11).	Envió un mensaje a la red social denunciando la existencia de un perfil falso para que lo eliminen (respuesta correcta). E8HE11		X	
	Sería informarles a mis padres que me están acosando o se han creado un perfil falso con mis nombres. También puedes denunciar esa cuenta por las redes sociales: “esa no soy yo, y automáticamente lo borran (ENT9ME11).	Envió un mensaje a la red social denunciando la existencia de un perfil falso para que lo eliminen (respuesta correcta). (E9ME11)		X	
	Le comunicaría a mis padres que han creado un perfil falso con mis datos personales (ENT10ME11).	Envío un mensaje a mis contactos por medio de una publicación informando que han creado un perfil falso con mis datos personales para que eviten responder a ese perfil (respuesta correcta). E10ME11	X		

Categoría	Competencia digital en seguridad				
Subcategoría	Protección de la salud y bienestar				
Codificación emergente	**Hallazgos de instrumento 1: Entrevista**	**Hallazgos de instrumento 2: Encuesta**	**Competencia: Protección de datos personales y privacidad**		
			Básico	**Intermedio**	**Avanzado**
			Prevenir riesgos que afecte a la salud, en específico, a la integridad física y el bienestar psicológico, ocasionados por el ciberacoso y el uso de la tecnología. ● Capacidades básicas para emplear medidas básicas preventivas para protegerse a sí mismo del ciberacoso. ● Conocimiento de las consecuencias por el uso constante de las tecnológicas (tiempo invertido en uso de internet, problemas auditivos y visuales, posturas). ● Conocimiento de las consecuencias y causas del ciberacoso. ● Capacidad de establecer relaciones interpersonales por medio de las redes sociales. ● Actitud de respeto, tolerancia y aceptación de las diferencias entre los usuarios.	Sé cómo protegerme a mí mismo y a otras personas del ciberacoso y comprendo los riesgos que afecta a la salud originados por el uso de tecnologías (desde los aspectos ergonómicos hasta la adicción a las tecnologías). ● Conocimiento sobre medidas preventivas para protegerse a sí mismo y a otros del ciberacoso. ● Conocimiento de los riesgos que genera el uso de tecnologías digitales para la salud. ● Conocimientos de pautas saludables (ejemplo: ergonómicas, visuales, tiempos, auditivos. etc.) para el uso correcto de las tecnologías. ● Capacidad para actuar preventivamente en relación al ciberacoso. Actitud de prevención para evitar el ciberacoso.	Estoy al tanto del uso correcto de las tecnologías para evitar problemas de salud. Sé cómo encontrar un buen equilibrio entre el mundo en línea y el mundo tradicional. ● Capacidad para evitar los elementos distractores que generan pérdida de tiempo cuando navegan por el internet. ● Capacidad para emplear estrategias que permitan evitar consecuencias dañinas del uso de las tecnologías. ● Actitud crítica frente al uso inadecuado de las tecnologías (tipo de información que se consulta, contenidos inapropiados, dispositivos, etc.) ● Capacidad para emplear conductas saludables en el uso de dispositivos tecnológicos (volumen adecuado de altavoces, tamaño adecuado del texto, iluminación del dispositivo, etc.). Actitud de comprensión frente a las estrategias que emplean los padres y maestros en el uso de las tecnologías.

			B	I	A
Consecuencias del uso inadecuado de las redes sociales y páginas web	Nos puede acosarnos por las redes sociales, hasta raptarnos porque sabe donde vivo. Y eso puede traer consecuencias psicológicas o podemos ser víctimas de acosos cibernéticos (ENT1HE12).	Confío en personas que conozco y quieren contactarse conmigo (respuesta correcta). E1HE12		X	
	Una consecuencia sería la adicción a las redes sociales o las páginas web, ya que sobrepasamos su uso. También puede cambiar mi comportamiento o daños psicológicos si observamos algún video que tiene contenidos de violencia, asesinatos u otros (ENT2ME12).	Confío en personas que conozco y quieren contactarse conmigo (respuesta correcta). E2ME12		X	
	Puede que sea víctima de algún acoso cibernético, volvernos adictos a las redes sociales, Youtube (ENT3HE12).	Confío en personas que conozco y quieren contactarse conmigo (respuesta correcta). E3HE12		X	
	Si públicas alguna foto personal puede que lo compartan otras personas y lleguen a acosarte (ENT4HE11).	Confío en personas que conozco y quieren contactarse conmigo (respuesta correcta). E4HE11		X	
	Si hacen algún meme de alguna de mis fotos puedo ser víctima de burlas, lo que me originaría tener depresión o estrés (ENT5ME11)	Utilizo una falsa personalidad en la Red (respuesta incorrecta). E5ME11	X		
	Si uso inadecuadamente las redes sociales o páginas web puede que alguien comparte mi información personal y me pueden acosar (ENT6ME12).	Solo me comunico con otros si presencialmente (respuesta incorrecta). E6ME12	X		
	Otras personas pueden entrar a tu perfil y ven ahí tu número, y te estarían escribiendo, tipo acosándome. Cuando observas videos que fomentan la violencia contra los animales o las personas puede que sufras algún daño psicológico, ya que puedes replicar los que hicieron en el video (ENT7HE11).	Confío en personas que conozco y quieren contactarse conmigo (respuesta correcta). E7HE11		X	
	Podemos publicar información personal que puede afectarnos, ya que podemos sufrir algún tipo de acoso cibernético (ENT8HE11).	Confío en personas que conozco y quieren contactarse conmigo (respuesta correcta). E8HE11		X	
	Nos puede acosar por las redes sociales. También podemos encontrar contenidos que no son propios de nuestra edad, como vídeos pornográficos, de violencia e información que nos pueda afectar psicológicamente (ENT9ME11)	Confío en personas que conozco y quieren contactarse conmigo (respuesta correcta). E9ME11		X	
	Quizá puedo ser víctima del ciberbullying, sexting o grooming (ENT10ME11)	Utilizo una falsa personalidad en la Red (respuesta incorrecta). E10ME11	X		
Cuidado de la salud por el uso de las TIC	Sí, tengo cuidado con la postura. Bajo el brillo del celular, escucho música o video sin audífonos en bajo volumen. Pero cuando utilizo el audífono escucho en alto volumen (ENT1HE12).	Muchas veces me terminan doliendo la espalda, piernas o cuello. (respuesta incorrecta). E1HE12	X		
	Si, tengo cuidado con el brillo del celular lo tengo reducido, pero con la postura no, ya que cuando utilizo mantengo una postura. Si utilizo audífonos lo pongo en bajo volumen. ENT2ME12	Muchas veces me terminan doliendo la espalda, piernas o cuello. (respuesta incorrecta). E2ME12	X		
	Sí. Bueno, el brillo del celular lo tengo bajo, el audio del volumen lo pongo alto, pero cuando no los utilizo con audífono. Ahora, cuando utilizo mi celular o tablet trato de sentarme bien para no cansarme o para que luego no me esté doliendo mi espalda o brazos (ENT3HE12).	Me siento correctamente en una silla, sofá, sillón, etc. y empleo trípode para sostener el equipo tecnológico. (respuesta correcta). E3HE12		X	
	Sí, a veces sí. Lo que hago es bajar el brillo del celular y de la laptop, ya que me fastidia la vista. Por otro lado, cuando escucho música el volumen lo tengo bajo. Pero con respecto a la postura no tengo cuidado ya que no me siento correctamente en la	Muchas veces me terminan doliendo la espalda, piernas o cuello. (respuesta incorrecta). E4HE11	X		

	silla, por lo que muchas veces me duele la espalda (ENT4HE11).				
	Cuando utilizo mi celular bajo el brillo de mi celular, y cuando estoy escuchando música o viendo videos trato de poner en un volumen adecuado (ENT5ME11)	Muchas veces me terminan doliendo la espalda, piernas o cuello (respuesta incorrecta). E5ME11	X		
	Sí, tengo mucho cuidado cuando utilizo mi celular. Bueno, me siento bien y no de manera como echada en la silla para que no me duela la espalda, escucho música con el volumen bajo y el brillo también lo tengo bajo porque si no me duelen los ojos (ENT6ME12)	Muchas veces me terminan doliendo la espalda, piernas o cuello. (respuesta incorrecta). E6ME12	X		
	Sí, cuando utilizo tengo cuidado con los aspectos del brillo, lo pongo en brillo automático, no utilizo muy cerca de la vista y del volumen, no lo uso en alto volumen, solo la cuarta parte. Con la postura no tengo mucho cuidado, ya que después me duele la espalda porque no me siento bien en la silla (ENT7HE11).	Me siento correctamente en una silla, sofá, sillón, etc. y empleo trípode para sostener el equipo tecnológico (respuesta correcta). E7HE11.		X	
	Sí. Bueno, cuando uso audífonos lo uso en bajo volumen, el brillo de la pantalla lo tengo bajo para cuidar mi vista. Cuando utilizo el celular me siento bien tanto en el sofá o en la silla (ENT8HE11).	Me siento correctamente en una silla, sofá, sillón, etc. y empleo trípode para sostener el equipo tecnológico (respuesta correcta). E8HE11		X	
	Sí, por ejemplo, no escucho música en alto volumen, me siento bien en la silla y, también bajo el brillo del celular para que mi ojo no me duela (ENT9ME11).	Me siento correctamente en una silla, sofá, sillón, etc. y empleo trípode para sostener el equipo tecnológico (respuesta correcta). E9ME11		X	
	Bueno, muchas veces no tengo cuidado cuando utilizo mi celular y la computadora. Por ejemplo, cuando utilizo audífono, como está malogrado, escucho solo con uno y en alto volumen. Yo lo utilizo echada en el sofá y suelo bajar el brillo del celular (ENT10ME11).	Muchas veces me terminan doliendo la espalda, piernas o cuello. (respuesta incorrecta). E10ME11	X		