Estrategias para alfabetización de adolescentes en Colombia dentro del ecosistema digital

Fernanda Cristancho Díaz
Especialización en Machine Learning
Jeizon Quintero Rojas
Especialización en Gerencia de Ciberseguridad

Universidad EAN
Facultad de ingenierías
Programa de especialización
Bogotá DC, Colombia
Junio de 2024

Estrategias para alfabetización de adolescentes en Colombia dentro del ecosistema digital

Fernanda Cristancho Díaz
Especialización en Machine Learning
Jeizon Quintero Rojas
Especialización en Gerencia de Ciberseguridad

Director (a):
Elizabeth León Velásquez

Universidad EAN
Facultad de ingenierías
Programa de especialización
Bogotá DC, Colombia
Junio de 2024

Tabla de contenido

Lista de figuras

Lista de tablas

Introducción

La era digital ha transformado la forma en la que interactuamos, nos comunicamos y accedemos a la información. La creciente presencia en el entorno digital de la humanidad postpandemia, especialmente la población adolescente sugiere el planteamiento de estrategias de alfabetización que no solo promuevan el acceso seguro a la información, sino que también que cuenten con la capacidad de utilizar de manera efectiva las tecnologías de la información, ser conscientes de los riesgos y desafíos que conlleva el uso del internet, dispositivos electrónicos y la protección de los datos que son compartidos.

En este sentido, a través del análisis de la información contenida en informes y estudios realizados por entidades públicas, empresas privadas y organizaciones independientes frente a los desafíos y riesgos que enfrentan en la actualidad los adolescentes en los entornos digitales. Posteriormente, desarrollar recomendaciones concretas que contribuyan en el fortalecimiento de la seguridad y privacidad de los datos de los adolescentes de Colombia en el entorno digital.

Resumen

La web 3.0 ha cambiado las dinámicas de comunicación e interacción entre las personas. Para aquellos nativos digitales, quienes nacieron en un mundo completamente digitalizado, los entornos digitales son un factor común, protagónico y hasta imprescindible en la manera en que se comunican y relacionan con el mundo, por ello, dada su alta exposición tienden a ser más susceptibles a enfrentar situaciones que supongan un riesgo para su integridad física y/o mental. En este sentido, esta investigación busca entender el nivel de conciencia que tiene la juventud colombiana sobre su presencia en plataformas digitales, los riegos a los que están expuestos, así como en brindar herramientas y conocimientos base para una interacción en la red más segura.

Palabras clave

Adolescencia, ciberseguridad, ecosistemas digitales, redes sociales, habeas data, ciberdelitos, ciberacoso, entorno digital, riesgos de seguridad, profesiones digitales, alfabetización digital, datos, perfiles de datos, Internet, consumo digital, inteligencia artificial.

Summary

The web 3.0 has changed the dynamics of communication and interaction among people. For those digital natives, those born into a fully digitalized world, digital environments are a common, leading, and even essential factor in how they communicate and relate to the world; therefore, due to their high exposure, they tend to be more susceptible to facing situations that pose a risk to their physical and/or mental integrity. In this regard, this research aims to understand the level of awareness that Colombian youth have about their presence on digital platforms, the risks they are exposed to, and to provide tools and basic knowledge for a safer interaction on the web.

Keywords

Adolescence, cybersecurity, digital ecosystems, social networks, data protection, cybercrimes, cyberbullying, digital environment, security risks, digital professions, digital literacy, data, data profiles, Internet, digital consumption, artificial intelligence, AI.

Objetivos de la investigación

Objetivo general

Proponer estrategias para la alfabetización digital en ciberseguridad que permitan asegurar el tratamiento y protección de los datos e información que comparte la población adolescente en Colombia en el ecosistema digital.

Objetivos específicos.

- Identificar los hábitos de consumo de plataformas digitales de la población juvenil en Colombia
- Analizar los riesgos y niveles de impacto a los que se ven expuestos los jóvenes colombianos en los diferentes escenarios de peligro dentro del entorno digital.
- Identificar, desde una visión regulatoria, el nivel de protección y legislación que cobija y rige a los jóvenes colombianos en sus actividades dentro de entornos digitales.
- Proponer estrategias para alfabetizar a la población de jóvenes colombianos, que les permita una interacción segura en entornos digitales.

Problema de investigación

Para inicios de 2023, 60,4% de la población colombiana tenía acceso a Internet según la OCDE (RNC, 2023), una cifra en crecimiento que nos permite darnos una idea del volumen poblacional que tienen a su disposición esta herramienta y que al día de hoy se ha vuelta tan necesaria, al punto de ser casi un recurso básico para estudiar, trabajar, relacionarse, entre muchas otras actividades que comprenden las rutinas diarias de una persona, de esta forma, este recurso, se ha hecho tan cotidiano en la vida de las personas, que para 2024, un ciudadano colombiano puede llegar a invertir hasta 8 horas 43 minutos por día, en promedio, navegando por la red (We Are Social, 2024), lo equivalente al 36% del día y solo comparable con la cantidad de tiempo que se dedica a descansar, dormir o trabajar.

De esta forma, y con la evolución que ha sufrido el Internet trayendo hasta lo que hoy se conoce como Web 3.0, se puede decir que, a mayor inmersión, mayor control o conocimiento, sin embargo, hay otros factores a considerar. Si bien los beneficios de tener acceso a Internet son altamente conocidos, los riesgos, como contraparte son, en ocasiones, voluntariamente ignorados amplificando su impacto y prejudicialidad en en la vida de las personas.

La potencialidad de dichos riesgos que abordan espectros psicosociales, económicos, reputacionales, entre otros, se ve amplificado por el surgimiento diario de nuevas tecnologías como la inteligencia artificial que, aún, en su etapa más prematura suponen una alerta temprana pues *“surge la preocupación que el uso de información de carácter personal para el desarrollo de la IA sea respetuoso de los derechos humanos”* (RIPD, 2019) así como seguro para la privacidad de los usuarios que diariamente generan y/o consumen contenido en plataformas del ecosistema digital.

Los riesgos dentro del ecosistema digital por la baja consciencia de los riesgos asociados con la divulgación de información personal en línea, hace a los usuarios vulnerables al acoso cibernético, el robo de identidad y otras amenazas cibernéticas de la actualidad, especialmente, a los jóvenes, personas entre 10 y 24 años quienes representan el 22,6 de los usuarios activos en Internet (We Are Social, 2024). Por otra parte, la falta de educación en ciberseguridad y alfabetización digital en las escuelas y en los hogares contribuye a esta problemática, ya que los jóvenes no cuentan con los conocimientos necesarios para proteger su información en línea.

Dicho esto, es necesario analizar el nivel de exposición de esta población, su comportamiento en plataformas y su grado de conciencia para evaluar en contraste con legislación, mecanismos de protección y herramientas de capacitación que permitan determinar si las medidas implementadas, por gobiernos y plataformas, son efectivas para garantizar la seguridad y privacidad de los datos de la población adolescente en el entorno digital en Colombia asegurando el tratamiento adecuado de la información que comparten en el mundo digital, de forma que el entendimiento de la propia existencia en un entorno digital y su vinculación con la realidad física sea desde un enfoque integral que genere una conciencia que disminuya la distorsión entre el mundo real y el mundo virtual para todos, que, como individuos sociales, adaptamos nuestras maneras de comunicarnos e interactuar al contexto que nos rodea (Valencia-Ortiz, R., Cabero-Almenara, J., Garay Ruiz, U. y Fernández Robles, B. (2021).

Con lo anterior, este trabajo busca responder la pregunta ¿Qué elementos se deben tener en cuenta para asegurar el tratamiento y protección de los datos e información que comparte la población adolescente en Colombia en el ecosistema digital?

Justificación

La sociedad en general ha sido educada desde la infancia para identificar la diferencia entre el bien y el mal. Se nos enseña desde pequeños sobre la existencia de potenciales riesgos a los que podríamos enfrentarnos en nuestra cotidianidad y en cómo enfrentarnos a dichas situaciones, a como no cruzar calles de manera imprudente o a no confiar en desconocidos, sin embargo, cuando de entornos digitales se trata, esa línea que divide lo bueno y lo malo se vuelve difusa, así como nuestro entendimiento sobre lo que puede significar un peligro para nuestra integridad.

En un país como Colombia, en donde hay más de 39 millones de personas haciendo uso del Internet (We are social, 2024) y donde el segundo delito más denunciado por la ciudadanía es la “Violación de datos personales” (Obando. J, 2024), es vital impulsar mecanismos de alfabetización y de apropiación digital que permitan un amplio aprovechamiento de las oportunidades que ofrece la red, pero desde una perspectiva con criterio propio, en la que el usuario esté en capacidad de comprender el impacto de su huella digital.

Por eso, profesionales del área tecnológica y colombianos, somos conscientes de la acelerada evolución del sector, sus beneficios a la industria y a la sociedad en general, pero también de los peligros a los que como personas nos enfrentamos día a día al interactuar dentro de estos espacios cibernéticos y la poca conciencia que hay, por esto, en aras de brindar herramientas que disminuyan esa brecha de desconocimiento, desarrollamos este trabajo con la esperanza de que sea un primer paso para enfrentar esta problemática.

Marco institucional

El marco institucional colombiano abarca el conjunto de organismos e instituciones que conforman su estructura gubernamental. Se incluyen los poderes ejecutivo, legislativo y judicial, los órganos de vigilancia y control, así como entidades públicas encargadas de la prestación de servicios y regulación de los diferentes sectores que dinamizan y orientan a la población del país. La población de Colombia según el DANE es de 52,2 millones a diciembre de 2023, de los cuales el 50,7% de la población es femenina y el 49,3% es masculina.

Por su parte, el 29,6% corresponde a la población adolescente de la nación. De acuerdo con las cifras informadas en el portal de Datareportal, 39,51 millones de colombianos cuentan con acceso a internet, otra de las cifras relevantes reportadas indica que había 36,7 millones de cuentas activas en redes sociales, de las cuales el 50,9% de los usuarios son de género femenino y el 49,1% del género masculino. Esto sugiere que la cantidad de cuentas activas corresponde al 70,3% de la población total.

Sin embargo, la cantidad de cuentas activas no representan a cada miembro de la población, toda vez que como veremos en el estudio realizado, los adolescentes por su parte cuentan con una o más cuentas activas en redes sociales. Las redes más utilizadas por los colombianos son TikTok, Snapchat, LinkedIn, Facebook, Instagram, YouTube, X, Pinterest, entre otras.

Marco teórico

Desde el surgimiento del Internet, la información y los datos han cobrado un nuevo significado. Los datos personales que en Colombia antes circulaban en el extinto directorio ahora reposan en el inmenso Internet y pueden ser consultados por cualquiera, desde cualquier parte del mundo en una milésima de segundo, por ello, en su surgimiento, las redes sociales eran canales de reconexión, espacios en donde era posible contactar con viejos conocidos, con familia lejana o con personas con las que se perdió el contacto en algún momento de la vida pero que con esta nueva tecnología se tenían a un par de clics de distancia, sin embargo, al igual que en el mundo físico, el mundo digital alberga personas con intenciones que carecen de moral y con ellas, los peligros que nos aquejan en la cotidianidad fueron replicados en el mundo virtual y sus implicaciones a nivel físico, psicológico y hasta financiero pueden llegar al mismo nivel que los concebidos fuera de entornos digitales, aunque de hecho, no son percibidos como tal.

Según la Encuesta Global de Seguridad en Línea de Microsoft, los padres de adolescentes subestiman los riesgos a los que éstos están expuestos en Internet, en este informe, el gigante tecnológico muestra como resultado de su investigación anual en Colombia, que la preocupación más grande de los padres está relacionada a temas desinformación, explotación sexual y ciberbullying, en donde, independientemente de la categoría, las niñas y adolescentes son las más vulnerables y han sido la población que más ha experimentado o enfrentado situaciones de riesgo en entornos digitales (Microsoft, 2024).

La baja percepción de riesgos en el ciberespacio es una problemática creciente y tan relevante para un mundo digitalizado como en el que vivimos actualmente que, entidades sociales, empresas de todas las ramas, entidades gubernamentales y hasta de alcance internacional, se han visto en la obligación de tomar cartas en el asunto. Caso particular, para 2020, la INTERPOL lanzó una campaña enfocada en recordar a la sociedad que los delitos digitales son delitos reales, mencionando al respecto que el peligro en entornos digitales "*es prácticamente imperceptible, lo que nos lleva a subestimar la magnitud de sus estragos o el riesgo de convertirnos en víctimas, aun cuando sus consecuencias pueden ser tan demoledoras como las de los delitos tangibles"* (INTERPOL, 2020), lo que nos lleva a analizar la clase de riesgos a los que se exponen los individuos en entornos digitales.

La ligereza con la que se tratan las interacciones en plataformas digitales es uno de los factores más relevantes en esta problemática. Desde retos virales que ponen en riesgo la integridad física de quienes los practican, pasando por suplantaciones resultado de una exposición inadecuada de información, hasta daños psicológicos por ciberacoso, ciberbullying, entre otros, hacen del espectro de amenazas un amplio campo de batalla, especialmente para los jóvenes quienes al parecer no sienten miedo y asocian estos peligros a algo natural que no repercute fuera de las pantallas (CEU, 2021), lo que también sería el reflejo de que aun siendo nativos digitales, los jóvenes *"no poseen inherentemente habilidades digitales",* por el contrario, sobreestiman su conocimiento aunque tienen mayor habilidad y facilidad de adaptación por lo que pueden aprender más rápido (ICDL, sf).

Bajo dicho debate, todos nos hemos convertido en potenciales víctimas, pero en una generación de nativos digitales, quienes nacieron en un mundo donde el Internet es la regla y no la excepción, su exposición constante los hace un blanco más visible de los ciberdelincuentes, incluso, el no concebir la trascendencia de sus actos en la red como actos con impacto en el mundo físico también los convierte en potenciales ciberdelincuentes, en donde el *Lifespan Brain Institute* del Hospital Infantil de Pensilvania, identificó una relación directamente proporcional entre el aumento de pensamientos autodestructivos, de flagelación o suicidio en las víctimas de ciberacoso o ciberbulliying (CHOP, 2022).

Las diversas perspectivas que se han abordado a lo largo de esta investigación dan una visión general de la problemática a la que se enfrentan los adolescentes. Sin embargo, la amplitud de su abordaje se suma a la dificultad para una óptima búsqueda de soluciones, como es el caso de las plataformas de redes sociales, quienes desde su responsabilidad como propulsores y principales actores se han visto obligados a implementar estrategias que mantengan bajo control potenciales situaciones de riesgo, tal es el caso de Meta, empresa dueña de plataformas como Facebook, Instagram y WhatsApp, quienes en los últimos años han implementado medidas como la cancelación de la monetización de perfiles, anuncios de advertencia sobre la veracidad de los contenidos y eliminación de contenidos fraudulentos en el caso de la desinformación, bloqueos de cuentas, baneo de usuarios con múltiples perfiles, opciones de denuncia y material informativo para abordaje de temas de acoso (Facebook, sf) sin embargo, para muchos, dichas medidas son insuficientes y no representan una verdadera solución para los usuarios de estas plataformas, por el contrarios, se ha considerado que las decisiones tomadas por la dirección de la plataforma responden a intereses propios o en

beneficio de terceros pero no contemplando a los millones de personas que hacen uso de estas (Roose. K, Isaac. K, Frenkel. S, 2020).

De igual forma, otras plataformas como X, antes Twitter, están en el ojo del público pues sus medidas han sido igualmente débiles en la protección al usuario. Es red social recientemente adquirida por Elon Musk, es de las pocas en su rubro que actualmente permite publicar y compartir contenido sexualmente explicito o visualmente violento, respecto a esto, la plataforma ha informado a sus usuarios que cuenta con diversos protocolos que curan el contenido, por ejemplo, en el caso de material sexual este está permitido dentro de la plataforma siempre y cuando sea material captado y distribuido con consentimiento de los involucrados y no muestre ninguna actividad ilegal (X, 2021). A su vez, han manifestado que aquel contenido delicado que cumpla con las normas se mantendrá en circulación en la plataforma, pero no será mostrado en la misma medida que los demás contenidos gracias a su algoritmo (El Tiempo, 2023).

De manera paralela, otra clase plataformas como apps de citas, comercios electrónicos, blogs, canales de difusión, entre otros que también están al alcance de las juventudes, cuentan algunos mecanismos de protección que buscan salvaguardar a sus usuarios y segmentar la audiencia que accede a estas. Verificación de edad, controles parentales, verificaciones de identidad y autenticaciones de información son algunas de las herramientas que proporcionan dichas plataformas pero que los niños y jóvenes pueden vulnerar fácilmente como lo identificó la Dr Liliana Pasquale, Profesora asistente de la *University College Dublin's School of Computer Science* (L. Pasquale, P. Zippo, C. Curley, B. O'Neill and M. Mongiello, 2021)

Por otro lado, los alcances del gobierno se han visto cortos. A la fecha en Colombia, aunque varias instituciones gubernamentales cuentan con grupos especializados para tratar casos relacionados a los ciberdelitos como es el caso de la Policía Nacional, la Fiscalía General de la Nación o el Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio de Tecnologías de la Información y las Comunicaciones, sin embargo, en cuanto a leyes no hay anda que cobije a la comunidad y menos a los jóvenes, si bien desde 2012 existe la Ley 1581 para la protección de datos “Habeas Data” esta aborda un espectro muy general y solo impacta en materia de recolección, tratamiento y circulación de datos, por lo que la creación de una institución más enfocada en el campo se encuentra en desarrollo bajo el nombre de Agencia de Seguridad Digital, la cual busca ser *“un organismo de carácter técnico,*

especializado, que tendrá como objeto planificar, articular y gestionar los riesgos de seguridad digital en Colombia" (MinTIC, 2023).

Como se ha detallado a lo largo de este documento, las potenciales amenazas relacionadas a la interacción en entornos digitales abordan una variada serie de escenarios a los que se está sobreexpuesto en los diferentes frentes como redes sociales, comercios electrónicos, aplicaciones móviles, correos electrónicos, entre muchos otras que además mutan diariamente y se adaptan a las barreras de seguridad de nuestros dispositivos, a los algoritmos de las compañías desarrolladoras, a las legislaciones vigentes y a cada intento, hasta ahora insuficiente, para seguirle el paso y darle el debido manejo a estas situaciones que son el día a día de la sociedad actual.

Con todo lo anterior, varios expertos proponen que, si bien es necesaria una intervención integral entre privados y públicos, incluso academia, hay una responsabilidad directa que esta arraigada a las personas y el desarrollo individual de habilidades de alfabetización digital que nos permitan ejercer como individuos, una ciudadanía digital segura y responsable como lo demanda la actualidad (Román. R, 2023).

Seguridad de la información

En general, el término se sustenta en la preservación de la confidencialidad, integridad y disponibilidad de la información y en su mínima expresión la de los datos. Otras propiedades que acuña este término son la autenticidad, confiabilidad, responsabilidad, no repudio. De acuerdo con estos criterios sobre la seguridad de la información se han establecido de manera estandarizada controles para salvaguardar y proteger la información de accesos no autorizados, acceso abusivo o el tratamiento indebido de la misma bajo el precepto y dependencia de la autorización de su propietario.

Metodología

Esta investigación será enriquecedora ya que aborda una problemática creciente y actual en la que, gracias al uso de testimonios verídicos, información actualizada y un análisis integral desde la visión social, legislativa y técnica podremos ampliar el panorama de ciberseguridad y generar referentes en la búsqueda de mecanismos para enfrentar las

falencias conductuales, formativas o de acceso para enfrentar los riesgos a los que podemos exponernos como usuarios de la Internet.

Entre tanto, el este estudio pretende abrir el debate que permita resaltar la importancia de hacer un acompañamiento adecuado, permanente y consiente de los tutores legales a la población adolescente para un consumo responsable y seguro, ofreciendo herramientas que permitan prevenir y entender el alcance de la huella digital que como usuarios de la red generamos, así como su trascendencia a la percepción física para un mejor entendimiento y prevención en el manejo, gestión y divulgación de datos.

Tipo de investigación

Mediante una investigación cualitativa con enfoque descriptivo, se busca recolectar información de manera independiente o conjunta con base en la información obtenida del sector (Hernández et al, 2016). Principalmente, se orientan a la revisión documentada en un contexto normativo y técnico que proporcionan la información que se quiere procesar, así como la recolección de datos no estructurados, tales como observaciones, entrevistas, grupos focales o documentos de otros estudios, que permitan proponer estrategias de alfabetización en relación con el caso de estudio.

Para obtener información de estudios o informes realizadas por fuentes secundarias se realizó consulta mediante buscadores web utilizando la siguiente sintaxis: ("informe") OR ("estudio") AND ("redes sociales") AND ("jovenes") OR ("adolescentes") OR ("niños") AND ("riesgo") AND ("seguridad") AND ("datos") AND ("personales"), lo anterior con el fin de filtrar los resultados de la búsqueda a través de operadores condicionales.

Tipo de estudio

El tipo de estudio para la presente investigación es descriptivo, de acuerdo con el concepto de (Bernal, 2016), en el tipo de estudio descriptiva se identifican situaciones, características de un objeto de estudio, se diseña productos, modelos, guías y otros, sin dar explicaciones o razones de las situaciones, hechos o fenómenos. Por lo tanto, la investigación descriptiva se soporta principalmente en técnicas como el diagnostico, la observación y la revisión documental, que le permita establecer escenarios de riesgos, su análisis y seguidamente la definición de estrategias de alfabetización orientadas a entornos seguros de interacción digital.

Población y muestra

De acuerdo con (Hernández et al., 2014), para el caso de estudio, el tipo de muestra es no probabilístico, toda vez que la investigación se relaciona con el propósito del investigador puesto que depende del proceso adoptado para la toma de decisiones.

Recolección y análisis de datos

Los instrumentos para recabar información son las observaciones, recolección de documentos, pruebas de diagnóstico estandarizadas y no estandarizadas y revisión del componente normativo, aplicable dentro alcance del estudio de caso. (Hernández, Fernández, & Baptista, 2010).

Tratamiento de los datos

Teniendo en cuenta las definiciones propuestas por (Hernández et al., 2014) el análisis de los datos cuantitativos se realiza posterior a su recolección, mientras que el análisis de datos cualitativos ocurre prácticamente en paralelo, en este último los datos obtenidos son variados, pero en esencia son narraciones de los participantes: textos escritos (documentos, informes y otros), expresiones verbales y no verbales (respuestas orales y gestos en una entrevista o un grupo de enfoque), además de las narraciones del investigador.

Análisis de los resultados

En el desarrollo de la investigación se realizó muestreo por conveniencia dada la amplitud del grupo poblacional objeto de estudio. Un muestreo por conveniencia *“consiste en la elección por métodos no aleatorios de una muestra cuyas características sean similares a las de la población objetivo"* (Casal. J, Mateu. E, 2003), determinando la intención de recopilar datos de un grupo entre los 50 y 100 individuos de nacionalidad colombiana que se encontraran entre los 12 y 26 años, a quienes se les realizaron 24 preguntas de tipo abierto y cerrado, que abordaron desde el espectro del uso y la experiencia hasta la percepción de seguridad y aprendizaje a través de componentes regulatorios y académicos. Posterior a la aplicación del instrumento, estos son los hallazgos más relevantes, encontrados en el estudio:

Para iniciar, se identificó que la población femenina representa una leve mayoría en la muestra analizada, lo que va en concordancia con el Reporte Digital 2024 de We Are Social, en donde identificaron que 50.9% de los usuarios de plataformas de redes sociales en Colombia son mujeres (We are social, 2024), misma población que según estudios, ha enfrentado en al menos un 60% algún delito en entornos digitales, especialmente en temas relacionados al acoso (Amu. L, Serna. K, Toro. G, 2023)

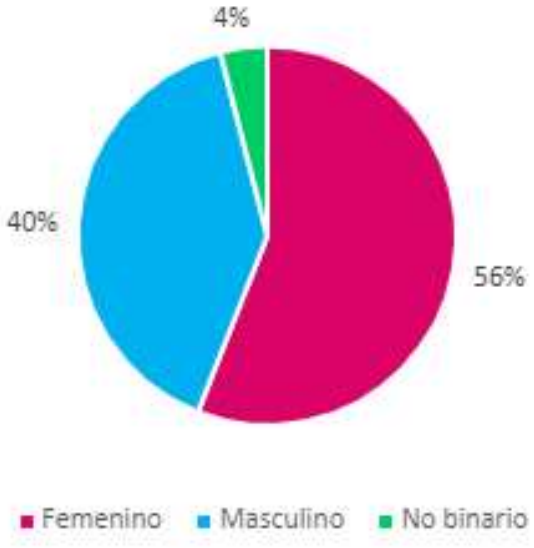

Figura 1 - ¿Qué edad tienes?

Ahora bien, la exposición a potenciales peligros también tiene una relación importante con la cantidad de tiempo que pasan interactuando o navegando en entornos digitales, dicho esto, el 90% del grupo encuestado manifestó hacer uso de plataformas digitales todos los días, entre las más usadas están Instagram, TikTok y Facebook.

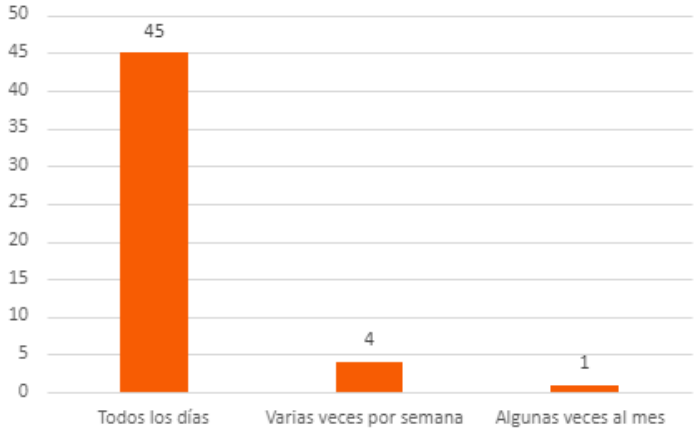

Figura 2 - ¿Con qué frecuencia utilizas plataformas digitales (redes sociales, aplicaciones de mensajería, etc.)?

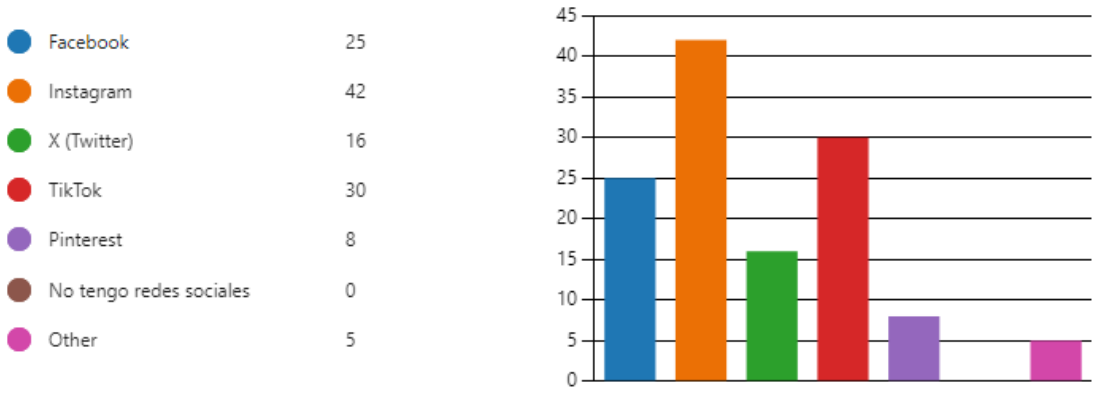

Figura 3 ¿Cuáles de las siguientes plataformas digitales utilizas con más frecuencia? (Selecciona todas las que apliquen)

En contraste, el Reporte Digital de We Are Social registro para 2024 en Colombia a WhatsApp como la red social más usada, seguida por Facebook e Instagram, mientras que en la categoría de páginas web, el ranking es liderado por Google, YouTube y Facebook, seguido por PornHub y XVideos (We Are Social, 2024), plataformas con innumerables denuncias por captación ilegal de datos (El Espectador, 2022) y distribución de material sexual sin consentimiento (El Español, 2023).

De igual forma, se consultó con los encuestados respecto al manejo que les dan a sus plataformas digitales, allí se abordaron temáticas sobre medidas de seguridad, relacionamiento con usuarios desconocidos, roles de usuario y uso de perfiles múltiples, con el fin de comprender características conductuales de los encuestados en entornos digitales, de allí se logra identificar lo siguiente:

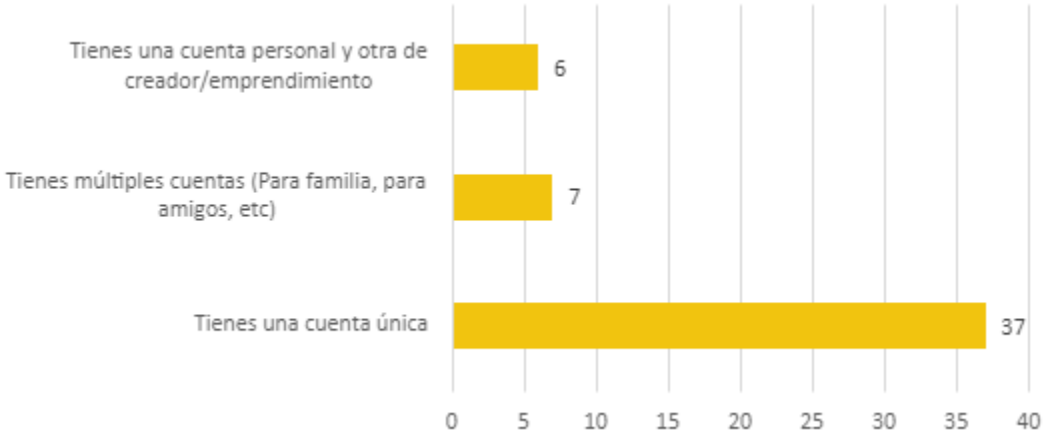

Figura 4 En estas plataformas tu

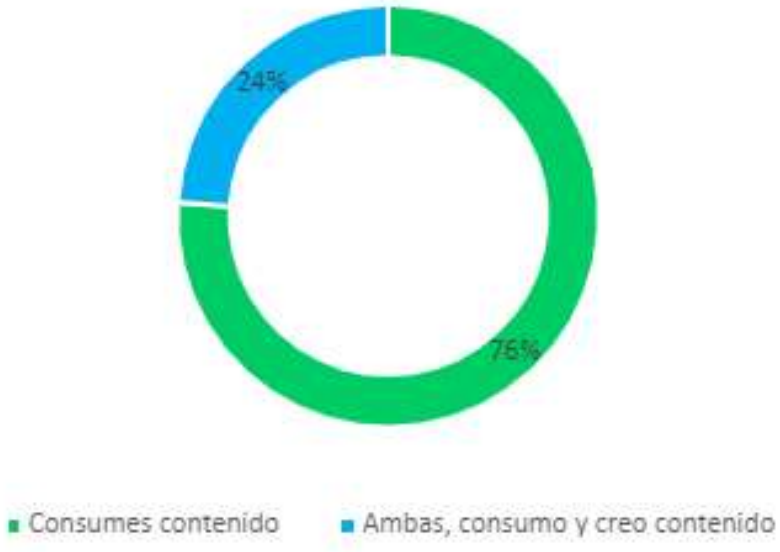

Figura 5 Respecto a los posibles roles que podemos tener en redes sociales tu

Por un lado, se evidencia que un 26% de los participantes cuentan con perfiles múltiples bien sea por razones propias respecto al interés de mantener círculos sociales separados o por razones laborales relacionadas con actividades laborales o de ocio como es el caso de las cuentas de emprendimiento o de creación de contenido que tienen el objetivo de monetizar el uso de dichas plataformas. Consecuentemente, el segmento que manifestó tener un rol bidireccional en entornos digitales es muy similar, dando sentido a que al menos una cuarta parte de los encuestados realizan actividades de consumo y creación de contenido de manera paralela.

A su vez, se determinó que el 46% de los encuestados consideran que “raramente” se relacionan con desconocidos y solo un 4% lo hace “con frecuencia” lo que podría ser un buen indicador. Sin embargo, ¿Son estas apreciaciones correctas? La respuesta es no, y se debe a que el planteamiento de la pregunta “¿Con qué frecuencia interactúas con personas desconocidas en línea?” es un planteamiento “trampa” que buscaba analizar más allá del relacionamiento de la muestra con otros usuarios, su percepción del entorno, en razón de esto es posible identificar que ese 46% puede estar teniendo una baja conciencia de cómo funcionan los entornos digitales pues hasta la más mínima interacción con cuentas conocidas, nos conecta a su vez con un incontable número de desconocidos que forman parte de la red de terceros, es decir, como usuarios podemos limitarnos a interactuar solo con contenido de familiares, amigos o conocidos pero está fuera de nuestro control el determinar hasta quién

vaya a llegar dicha interacción, el simple hecho de dejar un comentario en la publicación de un familiar abre la puerta a que un usuario fuera de circulo primario de contacto, pero que si haga parte de la red de dicho familiar o amigo pueda interactuar conmigo sin conocerlo y que de esta manera escale o que la reacción que se deposita en una publicación recomendada por el algoritmo no amplifique el alcance del material con el cual se está interactuando, especialmente en plataformas cuyo algoritmo está programado para ello, viralizar interacciones.

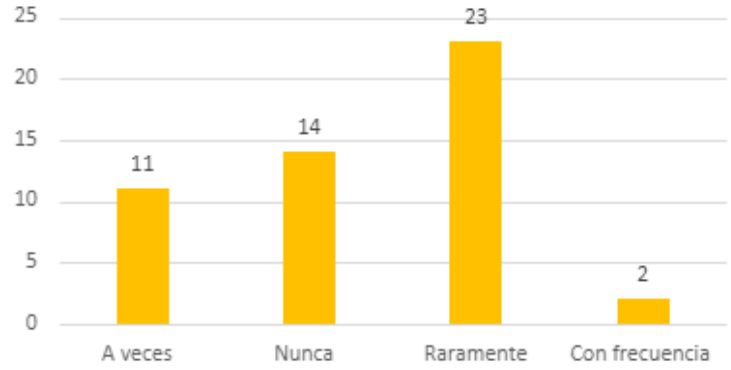

Figura 6 ¿Con qué frecuencia interactúas con personas desconocidas en línea?

Debido a lo anterior, frente a la pregunta relacionada con los mecanismos utilizados para proteger sus cuentas, tomó relevancia las herramientas de autenticación, enlace con dispositivos frecuentes o contraseñas seguras.

Figura 7¿Qué medidas de seguridad aplicas?

Esta clase de mecanismos es popular dado que son herramientas generalmente proporcionadas por las plataformas. Sin embargo, previenen el acceso abusivo, fuerza bruta o de ingeniería social, pero no eficientes con otra clase de riesgos, para ello, McAfee, empresa experta en seguridad cibernética recomienda el uso de otras estrategias complementarias como la configuración de permisos de las cuentas o la conciencia y rigurosidad de nuestras actividades en línea (McAfee, 2024).

El siguiente componente del cuestionario busca comprender, desde la percepción y experiencia de los encuestados, la conciencia frente a los potenciales riesgos en plataformas digitales, de ahí se identificó que hay un porcentaje importante del 70% que, aunque confía en la información de entornos digitales, está abierto a la duda de su veracidad, el 30% restante se remiten a la desconfianza y un 0% en la confianza absoluta, estos resultados resultan alentadores pues se podrían interpretar como una alta percepción de lo poco rastreable, sustentable o entendible que pueda ser la información que se encuentra en la red.

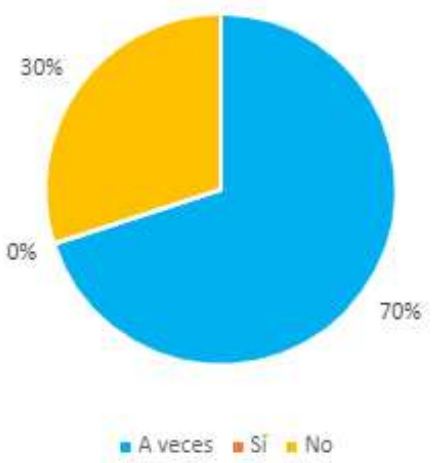

Figura 8 ¿Confías en la veracidad de la información que encuentras en línea?

De igual manera, cuando se consultó a los encuestados respecto a "¿Has tenido que enfrentar alguna situación de acoso, suplantación, extorsión, estafa, hackeo u otra situación que te haya hecho sentir vulnerable al usar redes sociales o plataformas digitales?", 36% de la muestra manifestó si haber enfrentado una situación de cibercrimen, mientras que el 4% no sabe o no concluye del todo si ha enfrentado o no una situación de este tipo. Entre los casos mencionados por los participantes se hace referencia a hackeos, estafas en compras, suplantaciones con creación de cuentas a su nombre o suplantación con robo de identidad, extorsión con contenido íntimo, robo de cuentas, entre otros.

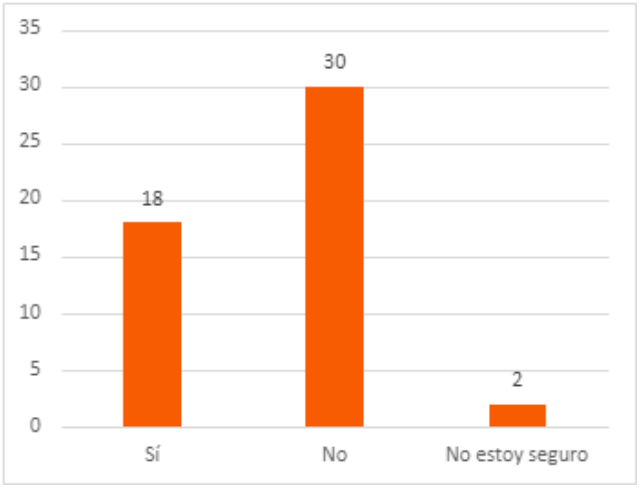

Figura 9 ¿Has tenido que enfrentar alguna situación de acoso, suplantación, extorsión, estafa, hackeo u otra situación que te haya hecho sentir vulnerable al usar redes sociales o plataformas digitales?

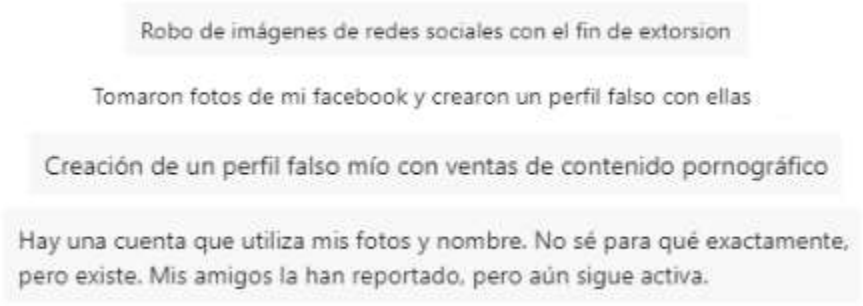

Figura 10 ¿Podrías contarnos sobre esa situación?

Respecto a la percepción en instituciones compuestas por los individuos, como las familias, o externas con injerencias sobre la población como el estado y la academia, se consultó a los encuestados bajo dos ejes, el eje de regulación que aborda los mecanismos de acción de los actores correspondientes en fomentar la seguridad de los entornos digitales y el eje de capacitación, que se enfoca en el otorgamiento de herramientas para abordar dichas situaciones de riesgo.

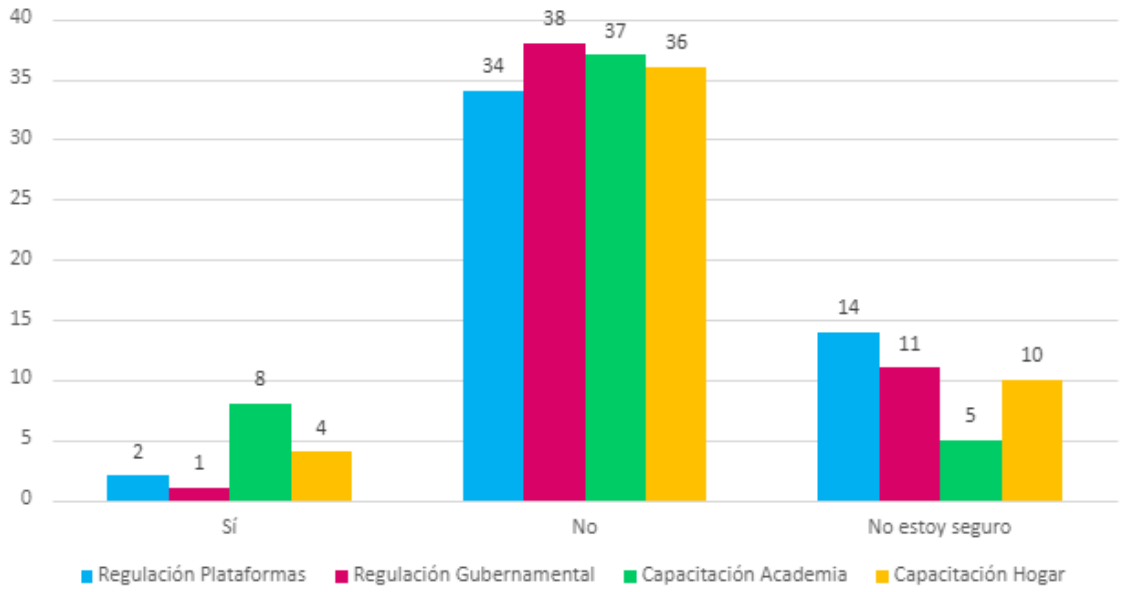

Figura 11 Regulación y capacitación

Bajo dicha lógica, la encuesta arrojó que entre un 72% y un 84% de los encuestados perciben como ineficientes y/o inexistentes los componentes actuales en materia de regulación y capacitación, mientras que un segmento entre el 20% y 28% no tiene clara su posición al respecto, dejando como minaría quienes, si perciben como suficiente las estrategias actuales, especialmente desde la Academia.

Sobre los riesgos y peligros en entornos digitales

De acuerdo con los resultados de la encuesta, el 6% de los encuestados manifestó estar entre los 12 y 17 años, corta y mediana edad, de los cuales 100% indicó que en ocasiones tiene interacción con desconocidos a través del entorno digital. Es preciso indicar que para crear una cuenta de usuario en redes sociales la edad mínima es de 14 años de acuerdo con los términos de condiciones de uso de las plataformas. Sin embargo, en contraste con los resultados obtenidos en la encuesta realizada y en concordancia con otros estudios realizados, suponen que a pesar de contar con restricciones y salvedades en los términos de uso y condiciones del servicio, los usuarios clasificados en corta y mediana edad ya cuentan con un perfil de usuario en redes sociales.

Por otra parte, en la investigación realizada por Mario Iles en el año 2019 como parte del proyecto “Análisis de riesgo por el uso de la red social facebook en la población juvenil colombiana”, indica que en Colombia no existe una Ley que regule específicamente la edad mínima o requerida para tener acceso a las redes sociales, esto de acuerdo con estudios realizados por Universidad Eafit y Tigo-Une en la que indican que el 84% de la población de infantil entre los 9 y 16 años cuenta con un dispositivo móvil personal y acceso a redes sociales. Su primera interacción en muchos casos está relacionada con dispositivos móviles celulares "smartphone", generalmente para el entretenimiento del menor con acceso Youtube. No obstante, el acceso a internet si el padre no configura el control parental, no está restringido o vigilado.

En concordancia con los resultados de la encuesta realizada y resultados consultados en fuentes secundarias, los menores mienten sobre su edad y año de nacimiento, datos requeridos para poder crear una cuenta de usuario en cualquier red social. Es preciso indicar que no hay ningún sistema capaz de verificar si el usuario está mintiendo o no, por lo que los menos y adolescentes pueden crearse un perfil en redes sociales, incluso cuando no alcanzan la edad mínima para ello. Aunque los padres implementen diferentes mecanismos para controlar a qué acceden y qué aplicaciones utilizan sus hijos, muchos adolescentes saben cómo saltarse el control parental. Por ello siempre es recomendable conocer y dar herramientas a los adolescentes que permitan desarrollar la capacidad de reconocer los peligros a los que se exponen en las redes sociales, para que no dejen de ser precavidos al momento de acceder a estas.

La privacidad en la red de internet es algo con lo que lidian incluso hasta lo adultos, sin llegar a ser conscientes de la cantidad y el tipo de información que se puede llegar a compartir y exponer, en especial en las redes sociales. Los menores y adolescentes no son la excepción y son más vulnerables a los riesgos y peligros de las redes sociales en relación con la privacidad, esto dada la cantidad de datos personales tanto textuales, multimedia y biométricos que comparten sin ser conscientes de ello, lo menos relevante para ellos al momento de crear un perfil en una red social es la interacción, pasando por alto la configuración de seguridad del perfil de usuario para controlar quién o quiénes puede visualizar el contenido que comparten. Esta configuración básica y necesaria para minimizar los riesgos consiste en asignar permisos de acceso por grupos de tipo familiar, amigos, amigos de los amigos y todo público.

Los riesgos y peligros habituales relacionados con el acceso a las redes sociales a los que se exponen los menores y adolescentes se relacionan con:

Sharenting: práctica que realizan los usuarios de las redes cuándo exponen a sus hijos a diferentes peligros por la exposición de contenido multimedia, lo cual se relaciona principalmente con la violación de su privacidad dado que los menores no son quienes deciden publicar fotos y videos suyos en la red social.

Ingeniería social: se refiere a una técnica utilizada por sujetos malintencionados para manipular a otros individuos con el fin de obtener información confidencial y privada para acceder a sistemas o efectuar acciones sin su consentimiento.

Acoso o Ciberbullying: es una forma de violencia y maltrato al que está expuesto el individuo a través de los diferentes medios digitales con la finalidad de enviar o compartir información de manera malintencionada con la intención de dañar o avergonzar a individuo afectado.

Suplantación de identidad o phishing: consiste en engañar a otros individuos haciéndose pasar por otra persona conocida para la victima para generar un ambiente de confianza o familiar con el fin de obtener información confidencial, datos de acceso, datos privados de cuentas personales o financieras.

Acoso sexual o Grooming: práctica generalmente empleada por agresores sexuales que buscan ganar la confianza de los menores de edad o adolescentes con el objetivo de sostener relaciones sexuales no consensuadas.

Sexo conversacional o Sexting: práctica realizada por los individuos a través de los diferentes medios digitales, en el que envían, reciben, y comparten mensajes, fotografías y videos con contenido sexual. Masificado su uso generalmente en adultos, que luego fue adoptado en gran medida por los adolescentes, en algunos casos se ha evidenciado el involucramiento de menores de edad de manera consensuada.

Noticias falsas o Fake News: práctica que consiste en la generación y distribución de información falsa que se difunde con la intención de engañar, desinformar o manipular a los individuos.

Retos virales o Challenge: práctica que consiste en el planteamiento de pruebas o actividades realizadas por los individuos con fines recreativos, entretenimiento. Sin embargo, personas malintencionadas promueven retos con actividades o prácticas peligrosas que son potencialmente dañinas para quienes las efectúan.

Conducta: se refiere a la interacción que tienen los individuos relacionada con el contacto con otros individuos que no hacen parte de su circulo social o familiar. También sugiere la posibilidad de exposición a contenido orientado al adoctrinamiento o generación de odio dentro del contexto racial, religioso, político o socioeconómico.

Sextorsión: es una práctica malintencionada con el fin de dañar a los individuos a través del chantaje. El contenido utilizado para realizar la extorción presenta alto contenido sexual explicito en fotografías, videos o mensajes mediante el cual el atacante busca obtener beneficio económico, emocional o incluso físico si la víctima no accede a sus demandas.

Estafa: es un acto de engaño o fraude en el que un individuo intenta obtener dinero, bienes u otros beneficios de manera deshonesta, aprovechándose de la confianza, la ingenuidad o la falta de conocimiento de la víctima. En el mundo digital se emplea esta técnica a correos de tipo phishing, llamadas telefónicas, aplicaciones y mensajes de texto.

Dentro del contexto de la seguridad de la información, el riesgo se define como la posibilidad de que ocurra un evento no deseado y que cause un impacto negativo en la confidencialidad, integridad o disponibilidad de la información. Así mismo la debilidad se refiere a una falla o deficiencia en un sistema, un proceso o un control que puede ser explotada por una amenaza para causar un impacto negativo en la seguridad de la información. Respecto al ser, el riesgo se podría interpretar como la posibilidad de experimentar consecuencias negativas o dañinas como resultado de ciertas acciones, decisiones o situaciones y la debilidad por su parte se puede definir como un aspecto o característica del sujeto que limita su desempeño, bienestar emocional o sus relaciones interpersonales. Estas debilidades pueden manifestarse en forma de rasgos de personalidad, patrones de pensamiento, comportamientos problemáticos o dificultades emocionales que afectan su vida cotidiana.

Cuando un individuo está expuesto de manera continua o prolongada a situaciones de riesgo, estrés o peligro, se puede ocasionar un desequilibrio en la activación del sistema

nervioso autónomo simpático y parasimpático, lo que puede resultar en efectos negativos para la salud, tales como: estrés crónico debido a la exposición constante a situaciones de riesgo o peligro, lo que puede contribuir al desarrollo de trastornos de ansiedad, hipertensión, problemas cardíacos y trastornos del sueño; la fatiga y agotamiento del individuo por agotamiento de los recursos del cuerpo, lo que puede resultar en fatiga crónica, falta de energía y dificultades para recuperarse adecuadamente dado al desequilibrio que presenta el sistema nervioso y por último el alto impacto en la salud mental, esto debido al estrés crónico y la activación persistente del sistema nervioso simpático que repercute en riesgo de trastornos mentales, tales como depresión, ansiedad y el estrés postraumático.

De acuerdo con lo expuesto, los resultados de la encuesta realizada y en concordancia con la revisión documentada en otros estudios, es pertinente abordar los riesgos y peligros no solo a nivel tecnológico, si no también en las condiciones físicas y mentales del individuo.

A continuación, se presenta la matriz de riesgos identificados:

Tabla 1: Matriz de riesgos identificados

Riesgo	Causa	Consecuencia	Probabilidad	Impacto
Posibilidad de afectación a la privacidad y exposición de información sensible de menores y adolescentes - Sharenting	Publicación de contenido, fotografías, videos de los menores y adolescentes sin autorización	Violación de la privacidad de los menores y adolescentes, implicaciones legales, suplantación, robo de identidad	Alto	Medio
Posibilidad de robo de información por publicación de datos e información personal y de contacto, pérdida o robo de identidad digital por secuestro de perfiles en redes sociales, información personal y financiera – Phishing/Ingeniería social	Publicación de información de contacto, perfiles de usuario sin configuraciones de seguridad y restricción de acceso	Acceso no consentido a datos privados, robo de información personal, suplantación de identidad. Distorsión de la realidad por posible adoctrinamiento o fanatismos orientados a la afectación personal o de terceros	Media	Alto
	Publicación de información confidencial y privada, ubicación y posesiones que puede	Robo y estafa físico y virtual. Suplantación de identidad física y virtual.	Medio	Alto

Riesgo	Causa	Consecuencia	Probabilidad	Impacto
	ser utilizada por atacantes que, mediante técnicas engañosas generan un ambiente de confianza y familiaridad con la víctima, lo que les permite acceder a información sensible y realizar acciones fraudulentas.	Fraudes financieros. Afectación a terceros debido a la suplantación		
Posibilidad de daño físico y emocional por acoso - Ciberbulling	Publicación de contenido mal intencionado con el fin de dañar o denigrar a uno o varios individuos relacionado con su etnia, credo, clase social, afinidad política.	Daño emocional, aislamiento social, impacto en la autoestima y salud mental de la víctima.	Alto	Alto
Posibilidad de afectación a la integridad física y mental por acoso sexual – Grooming/Sextorsión	Perfiles de redes sociales abiertos, sin ningún tipo de restricción de contacto o por contacto directo de las victimas con sus atacantes en el entorno digital, lo cual les permite generar un ambiente de confianza que puede repercutir en violaciones y ataques físicos	Violación a la intimidad de los menores y adolescentes debido al contacto con extraños o personas del grupo social que les permite realizar acoso sexual físico y digital	Bajo	Alto
Posibilidad de afectación a la imagen y reputación física y digital debido al intercambio de contenido digital explicito – Sexting/Sextorsión	Falta de conciencia en los menores y adolescentes debido a la realización de prácticas de intercambio de mensajes, fotografías y videos con contenido sexual explicito.	Situaciones de chantaje, ciberacoso, vulneración de la privacidad y reputación en entornos físicos y digitales	Media	Alto
Posibilidad de difamación y manipulación debido a la generación o divulgación de información no verificada - Fake News	Distribución o generación de contenido difuso o de difamación de las personas, la información compartida no es verificada o cuenta con un alto grado de sensacionalismo para conseguir seguidores o interacciones “clickbait”.	Afectación a la integridad de las personas, impacto en la toma de decisiones debido a sesgos en la información, desinformación deliberada, polarización y división social, aislamiento del individuo afectado	Alto	Medio

Riesgo	Causa	Consecuencia	Probabilidad	Impacto
Posibilidad de afectación física y mental ocasionada por la práctica de actividades propuestas por otros individuos en la red	Promoción y divulgación deliberada que promueven la realización de actividades riesgosos que pueden afectar la integridad física y emocional de quienes participan.	Afectación física y emocional que puede generar un alto impacto negativo en la condición física de los individuos, además de los daños sicológicos del ser	Medio	Alto

Nota: Esta tabla muestra la relación de riesgos a los que se ven expuestos los usuarios en entornos digitales.

Formulación de propuestas pedagógicas

Una de las principales intenciones de esta investigación era el brindar potenciales estrategias de alfabetización digital que permitieran a las juventudes colombianas contar con herramientas para afrontar peligros en el entorno digital, por ello, para abordar opciones a parte de las ya disponibles como seminarios, proponemos lo siguiente:

1. **Pedagogía de inmersión:** Entendemos en este caso que la falta de percepción de muchos usuarios es la red no es por desconocimiento en cuanto al funcionamiento de las plataformas si no por la poca asimilación que se tiene del impacto de las acciones en línea con la vida real, por lo que esta propuesta va orientada en ofrecer, desde la pedagogía en universidades y colegios, herramientas de exposición con los casos más simples donde bajo la supervisión docente, los estudiantes asuman un rol decisorio y a través de planteamientos hipotéticos tengan la libertad de tomar decisiones que generen consecuencias, igualmente hipotéticas, y potenciales soluciones a estas, para que se puedan ir relacionando posibles escenarios desde la asimilación de conceptos en primera persona.

2. **Contenido multimedia:** Dada la claridad de que el desconocimiento no ha sido una barrera para que los jóvenes se alejen de los entornos virtuales, una de las mejores herramientas es crear contenido que informe tanto de riesgos como de los mecanismos para enfrentar dichos riesgos, sacando provecho de recursos ya existentes como lo son las redes sociales para difundir contenido de valor de manera masiva a través de formatos cortos pero atractivos para la audiencia.

3. **Hackáthones:** Integrando a las entidades gubernamentales, académicas y/o corporaciones, a modo de concurso brindar recursos y un reto a estudiantes de diversos niveles académicos para que propongan propuestas a delitos cibernéticos específicos, asegurando así para los participantes el conocimiento sobre el tema y dándoles la oportunidad de como individuos y usuarios ofrecer soluciones desde sus perspectivas que pueden escalar a convertirse en políticas públicas o estrategias interinstitucionales.

4. **Campañas de sensibilización en los entornos digitales**: Emplear las propias plataformas digitales de mayor uso por los adolescentes, como Instagram, X, TikTok o YouTube, para lanzar campañas de sensibilización y concienciación sobre el uso y comportamiento en el entorno digital. Las campañas pueden incluir videos cortos, infografías, piezas gráficas, consejos rápidos y desafíos interactivos que aborden temas relevantes de seguridad en línea, protección de datos y prácticas seguras en el uso de internet y redes sociales. Adicionalmente involucrar personalidades juveniles “influencers” para llegar a un público más amplio y generar mayor impacto.

Conclusiones

En este estudio se logra comprender mejor el amplio espectro de las plataformas digitales, desde páginas web y redes sociales hasta aplicaciones o videojuegos, y con ello los riesgos que se esconden en sus múltiples atributos. Si bien, la tecnología es sin duda una gran aliada, su rápida evolución ha abierto campo para que los individuos la usen en beneficio propio o para la sociedad, el propósito de uso sea bueno o malo siempre dependerá del libre albedrio. Por lo tanto, todos los actores están obligados en adaptarse y evolucionar con ella entendiendo sus matices lo mejor posible y comprendiendo a profundidad que el hecho de que no ser tangible, no lo hace menos riesgoso. Que, como individuos nuestros actos o la omisión de ellos en nuestro paso por la red tienen las mismas implicaciones, consecuencias y/o alcances que en el plano físico y que indudablemente la prevención va de la mano con el conocimiento, por lo que parte de ese deber, es acompañar a las infancias y juventudes durante su proceso de entendimiento de esta clase de entornos tal y cómo lo hacemos frente a otra clase de amenazas, brindándoles las herramientas correctas para desenvolverse con tranquilidad y seguridad en esta clase de entornos.

De igual forma, en el desarrollo de esta investigación se evidenció que la temática y la población objeto de estudio, son mucho más amplios y abarcan una cantidad de matices que complejizan abordar a profundidad la problemática, por lo que se encuentran grandes limitaciones en el proceso. Sin embargo, sirven como recordatorio de la importancia de seguir abriendo espacios de socialización, capacitación e investigación en estos temas en los que, particularmente en Colombia, somos aún muy novatos.

Para el caso de estudio se debe abordar diferentes variables con el fin de lograr un resultado más acertado frente a la problemática planteada. En este sentido, reconocer en un amplio espectro los hábitos de consumo de plataformas digitales por parte de la población juvenil en Colombia y definir estrategias acordes a los diferentes grupos poblacionales.

Luego de analizar la exposición de los adolescentes y la niñez del país en los entornos digitales, se evidencia la carencia en el desarrollo de prácticas de socialización y concienciación frente al manejo de los datos y de la información que comparten en la red. Asimismo, se sugiere identificar los riesgos en contraste con sus causas, dadas las características de la población objeto de estudio y considerar las estrategias propuestas para alfabetizar a la población de jóvenes colombianos, permitiendo desarrollar la capacidad y

obtener herramientas para interactuar de manera segura en entornos digitales; auto regulándose de forma que puedan adoptar normas de comportamiento en el ciberespacio basadas en el respeto mutuo (Netiqueta), sin que estas sean impuestas por un organismo rector.

Por otra parte, dentro del contexto normativo, en Colombia no se cuenta con regulaciones específicas frente al manejo, uso y comportamiento en el entorno digital. Si bien se cuenta con articulado relaciona con delitos informáticos (Ley 1273 de 2009), el actuar de los adolescentes en entornos digitales requiere mayor control por parte de las instituciones.

Finalmente, se reconoce que los entornos digitales son hoy, una parte integral para todos como sociedad por lo que es indispensable aterrizar la conciencia, tanto de jóvenes como adultos, para que en el mundo virtual como el terrenal sean comprendidos como complemento y no como opuestos, y para ello, el trabajo es amplio y requiere la participación de los gobiernos, las empresas y la academia como actores fundamentales, siendo este tal vez, el componente más complejo pues la falta de componentes pedagógicos en la formación de infancia, la limitada regulación por parte de las entidades y ligereza en responsabilidad de las corporaciones juegan un papel antagónico en esta problemática que poco o nada puede ser solucionada desde la individualidad por lo que, entre tanto, como ciudadanos e individuos no podemos liberarnos de la responsabilidad que está también en nuestras manos de incentivar mejores usos de estas herramientas y adaptarnos a los mecanismos disponibles para protegernos a nosotros mismos y a quienes nos rodean.

Referencias

‘Alerta en línea’, la nueva estrategia para prevenir ‘ciberdelitos’ que afectan a jóvenes en Bogotá (2023) Secretaría Distrital de Educación, Recuperado de: https://www.educacionbogota.edu.co/portal_institucional/noticia/alerta-en-linea-la-nueva-estrategia-para-prevenir-ciberdelitos-que-afectan-jovenes-en#:~:text=%2DSeg%C3%BAn%20cifras%20del%20Centro%20Cibern%C3%A9tico,explotaci%C3%B3n%20sexual%20infantil%20en%20Internet.&text=Bogot%C3%A1%20D.%20C.%2C%206%20de%20septiembre%20de%202023

Análisis de riesgos por el uso de la red social Facebook en la población juvenil colombiana. (2019). Iles Mario. Recuperado de https://repository.unad.edu.co/bitstream/handle/10596/31453/miles.pdf?sequence=1&isAllowed=y

CEU (2021) Ciberdelicuencia: una amenaza real para los menores, recuperado de: https://www.colegioceumonteprincipe.es/blog/ciberdelicuencia-una-amenaza-real-para-los-menores/

CHOP (2022) Study Shows Link Between Cyberbullying and Suicidality in Early Adolescence, Recuperado de: https://www.chop.edu/news/study-shows-link-between-cyberbullying-and-suicidality-early-adolescence

Colombia es el país miembro con menor cobertura de internet: OCDE (2023) Radio Nacional de Colombia, Recuperado de: https://www.radionacional.co/actualidad/tecnologia/que-cobertura-de-internet-tiene-colombia-ocde

Cuida tu identidad digital y protege tus datos personales: riesgos sobre el tratamiento de datos personales de niños, niñas y adolescentes. (2021). Recuperado de

https://www.sic.gov.co/sites/default/files/files/2021/Guia%20CUIDA%20TU%20IDENTIDAD%20DIGITAL%20002.pdf.

Digital Age of Consent and Age Verification: Can They Protect Children? L. Pasquale, P. Zippo, C. Curley, B. O'Neill and M. Mongiello (sf), Recuperado de: https://www.eurekalert.org/news-releases/550700

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

El Proyecto de Investigación: Introducción a la metodología científica (2012). 6ta Edición. Caracas: Episteme. Arias, F.

El Tiempo (2023) Directora de Twitter dice que contenido tóxico no será eliminado pero sí difícil de ver, Recuperado de: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/twitter-directora-de-x-dice-que-el-contenido-toxico-sera-dificil-de-ver-795099

ICDL (sf) Percepción y realidad: midiendo las habilidades digitales, Recuperado de: https://icdl.org/percepcion-y-realidad-midiendo-las-habilidades-digitales/

Impacto de la tecnología en la adolescencia. Relaciones, riesgos y oportunidades. (2021). Madrid: UNICEF España. Andrade, B., Guadix, I., Rial, A. y Suárez, F.

Impacto de las redes sociales e internet en la adolescencia: aspectos positivos y negativos. (2015). Revista Médica Clínica Las Condes.

Informe anual de ciberseguridad. IA para la protección y prevención de amenazas. (2023). Equipo TicTac.

Inseguridad en las redes sociales e Internet: Prioridad en las escuelas de la provincia de Ocaña. (2016). (n.p.): Instituto Tecnológico Metropolitano.

Internet, smartphone y redes sociales: entre el uso y abuso, previo a la adicción. (2023). Eneko Tejada-Garitano; Ander Arce-Alonso; Naiara Bilbao-Quintana; et al. Recuperado de https://www.redalyc.org/journal/4677/467774008001/.

INTERPOL (2020) INTERPOL nos recuerda que la ciberdelincuencia es un delito real (#OnlineCrimeIsReal), Recuperado de: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/INTERPOL-nos-recuerda-que-la-ciberdelincuencia-es-un-delito-real-OnlineCrimeIsRealMetodología para el análisis de riesgos de TI. Pág. 1. (2013). OCTAVE, Carmona, E. J.

Metodologías Para el Análisis de Riesgos en los SCSI. Pág. 76. (2014). Revista Especializada en Ingeniería. Castellanos, F. U.

Meta (sf) Cómo evitar la publicación de contenido engañoso en Facebook, Recuperado de: https://es-la.facebook.com/business/help/366867510744964?id=208060977200861

Meta (sf) Recursos sobre el abuso, Recuperado de: https://es-la.facebook.com/help/726709730764837

Microsoft (2024) Resultados de la encuesta global de seguridad en línea, Recuperado de: https://go.microsoft.com/fwlink/?linkid=2257801&culture=es-mx

MinTIC (2023) Proyecto del MinTIC para la creación de la Agencia Nacional de Seguridad Digital y Asuntos Espaciales pasa el primer debate, Recuperado de: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/281222:Proyecto-del-MinTIC-para-la-creacion-de-la-Agencia-Nacional-de-Seguridad-Digital-y-Asuntos-Espaciales-pasa-el-primer-debate

Problemática de estudio e investigación de la adicción a las redes sociales online en jóvenes y adolescentes. Tecnología, Ciencia y Educación, 18, 99-125. Valencia-Ortiz, R., Cabero-Almenara, J., Garay Ruiz, U. y Fernández Robles, B. (2021).

Protección de niños, niñas y adolescentes en el uso de redes sociales: análisis de riesgos y medidas eficaces. (2022). Urbano, A. Recuperado de https://repository.javeriana.edu.co/bitstream/handle/10554/60838/Protecci%C3%B3n%20de%20ni%C3%B1os,%20ni%C3%B1as%20y%20adolescentes%20en%20el%20uso%20de%20redes%20sociales.pdf?sequence=1

Obando, J (2024) Ciberseguridad en Colombia: panorama completo de su estado en 2023, Recuperado de: https://linktic.com/blog/panorama-completo-de-la-ciberseguridad-en-colombia/

Recomendaciones generales para el tratamiento de datos en la inteligencia artificial (2019) Red Iberoamericana de Protección de Datos (RIPD) Recuperado de: https://www.sic.gov.co/sites/default/files/files/pdf/1%20RIPD%20(2019)%20RECOMENDACIONES%20GENERALES%20PARA%20EL%20TRATAMIENTO%20DE%20DATOS%20EN%20LA%20IA.pdf

Reglamento General de Protección de Datos (RGPD) de la UE. (2016). IT Governance Publishing. CARDER, A.

Román, R (2023) Seguridad digital de los jóvenes en Latinoamérica Recuperado de: https://observatorio.tec.mx/edu-news/seguridad-digital-de-los-jovenes-en-latinoamerica/

The New York Times (2020) Facebook se debate entre combatir la desinformación y no afectar su crecimiento, Recuperado de: https://www.nytimes.com/es/2020/11/27/espanol/ciencia-y-tecnologia/facebook-desinformacion.html

Seguridad y ciudadanía. (2021). España: Editorial Dykinson, S.L.

Uso y riesgos en el uso de internet de adolescentes escolarizados entre 12 y 17 años con enfoque de explotación sexual en línea. (2021). Fondo de las naciones unidas para la infancia UNICEF. República Dominicana. Recuperado de https://www.unicef.org/dominicanrepublic/media/5771/file/Adolescentes%20y%20el%20uso%20de%20Internet%20-%20PUBLICACI%C3%93N.pdf

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

X (sf) Política relativa a la desnudez no consensuada, Recuperado de: https://help.twitter.com/es/rules-and-policies/intimate-media

Casal. J, Mateu. E (2003) Tipos de muestreo Recuperado de https://d1wqtxts1xzle7.cloudfront.net/55524032/TiposMuestreo1-libre.pdf?1515813042=&response-content-disposition=inline%3B+filename%3DTIPOS_DE_MUESTREO.pdf&Expires=1717383327&Signature=fab78fg9YUwqHDgRzn0BWmmaGeVaZlDO2Yh~amD-wW2H~o4CVIhrIIVSsel0vOd7b0xuYs563UCHmJgVa~aCrsn6hGbm50F0-FF7dOP7cAOujpjlQWnONLjVhbU~V4FDX~7FpQgCkYrJiXJhxnXxKWCT6r2zNu-zGxYnDVp5VbKy1Y7cxBmNapNwrx2o5qOHZnK69ztRKvh1lmNfgaJaZbteX1vddCyZzESXfTBjzs4EqtPbMVn52rZQcCToMjno2JkTl5BzROs6kkHPncmqrvKO-qe8a77W-4Cz4kwYsOBdig6x7PVsAw-hiWtsG4Ph5OrZzLcd7J-EroT1tMA~OQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

El País (2023) Violencia digital, un delito que acecha al 60 % de las mujeres, Recuperado de: https://www.elpais.com.co/judicial/violencia-digital-un-delito-que-acecha-al-60-de-las-mujeres-1227.html

El Español (2023) Pornhub, acusada de recolectar datos de millones de usuarios de forma ilegal, Recuperado de: https://www.elespanol.com/omicrono/software/20230629/pornhub-acusada-recolectar-datos-millones-usuarios-forma-ilegal/775172789_0.html

El Espectador (2022) Pornhub: directivos habrían renunciado tras escándalo por delitos sexuales, Recuperado de: https://www.elespectador.com/mundo/mas-paises/pornhub-directivos-habrian-renunciado-tras-escandalo-por-delitos-sexuales-noticias-hoy/

McAffe (2024) Cómo proteger tus cuentas en las redes sociales, Recuperado de: https://www.mcafee.com/blogs/es-mx/privacy-identity-protection/como-proteger-tus-cuentas-en-las-redes-sociales//