UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSTGRADO

MAESTRÍA EN TECNOLOGÍA E INNOVACIÓN EDUCATIVA

DISEÑO DE ESTRATEGIAS DIDÁCTICAS PARA LA PREVENCIÓN DE RIESGOS TECNOLÓGICOS RELACIONADOS A LA SEGURIDAD INFORMÁTICA DIRIGIDO A ESTUDIANTES DE TERCERO DE BACHILLERATO

Trabajo de grado previo a la obtención del título de Msc. En Tecnología e Innovación Educativa

AUTOR: René Bolívar Cabascango Naranjo

DIRECTOR: Ing. Daisy Elizabeth Imbaquingo Esparza PhD.

IBARRA 2023

Dra. Lucia Yépez
Decana

Facultad de Postgrado

ASUNTO: Conformidad con documento final

Señora Decana: Lucia Yépez

Me permito informar a usted que una vez revisado el Trabajo final de DISEÑO DE ESTRATEGIAS DIDÁCTICAS PARA LA PREVENCIÓN DE RIESGOS TECNOLÓGICOS RELACIONADOS A LA SEGURIDAD INFORMÁTICA DIRIGIDO A ESTUDIANTES DE TERCERO DE BACHILLERATO, del maestrante, René Bolívar Cabascango Naranjo, de la Maestría de Tecnología e Innovación Educativa, certifico que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

1002873048 DAISY ELIZABETH IMBAQUINGO ESPARZA

Firmado digitalmente por 1002873048 DAISY ELIZABETH IMBAQUINGO ESPARZA
Fecha: 2023.11.28 16:17:29 -05'00'
Versión de Adobe Acrobat: 2021.011.20039

Msc. Daisy Imbaquingo Espaza
Directora de tesis

DEDICATORIA

A Dios por sus infinitas bendiciones.

AGRADECIMIENTO

A mi esposa Chio, por ser ese apoyo y soporte imprescindible en los momentos difíciles y aquella compañía inmejorable en los buenos momentos. Sin duda la mejor compañera de viaje.

A mis hijos Alejandro y Doménica son el regalo más precioso que me ha dado Dios, me han enseñado el significado del amor y la dedicación.

A mis padres, tengo la bendición, que incluso hasta ahora me brinden su cariño, sus consejos y su amor incondicional.

A mis hermanas y a toda mi gran familia por ser ese apoyo que dice presente cuando la vida se torna difícil, siempre les llevó en mis oraciones y en mi corazón.

A la Msc. Daisy Imbaquingo, Directora de la tesis, por todo su aporte profesional a lo largo del desarrollo de este trabajo.

A mis compañeros de maestría, en especial a los que conformamos el Grupo No. 2, Andrés, Mariuxi, Luis y Anita Lucía, grandes personas sin lugar a dudas.

A la Universidad Técnica del Norte y a través de está a sus autoridades, docentes y demás personal que conforma la misma, por trabajar arduamente en la formación y perfeccionamiento de profesionales de calidad.

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN
A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. Identificación de la obra

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DEL CONTACTO			
CEDULA DE IDENTIDAD	1710246511		
APELLIDOS Y NOMBRES	Cabascango Naranjo René Bolívar		
DIRECCIÓN	Av. Mariana de Jesús y Panzaleos, Urb. Portal de la Hacienda Calle F, Lote 200. Provincia de Pichincha, Cantón Rumiñahui.		
EMAIL	rene.cabascango@gmail.com		
TELÉFONO FIJO	023188353	**TELÉFONO MÓVIL**	0967027558

DATOS DE LA OBRA	
TÍTULO:	Diseño de estrategias didácticas para la prevención de riesgos tecnológicos relacionados a la seguridad informática dirigido a estudiantes de tercero de bachillerato.
AUTOR:	Cabascango Naranjo René Bolívar
FECHA: (DD/MM/AAAA)	**28/11/2023**
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA	**POSGRADO**
TÍTULO POR EL QUE OPTA	Magister en Tecnología e Innovación Educativa.
TUTOR	Msc. Daisy Elizabeth Imbaquingo Esparza

2. Constancia

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 28 días del mes de Noviembre del año 2023.

EL AUTOR

RENE BOLIVAR CABASCANGO NARANJO

Firmado digitalmente por RENE BOLIVAR CABASCANGO NARANJO
Fecha: 2023.11.28 16:49:40 -05'00'

Firma
René Bolívar Cabascango Naranjo.

INDICE DE CONTENIDOS

Tabla de contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DEL NORTE
INSTITUTO DE POSGRADO
PROGRAMA DE MAESTRÍA EN TECNOLOGÍA E INNOVACIÓN EDUCATIVA

DISEÑO DE ESTRATEGIAS DIDÁCTICAS PARA LA PREVENCIÓN DE RIESGOS TECNOLÓGICOS RELACIONADOS A LA SEGURIDAD INFORMÁTICA DIRIGIDO A ESTUDIANTES DE TERCERO DE BACHILLERATO

Autor: René Bolívar Cabascango Naranjo
Tutor: Msc. Daisy Elizabeth Imbaquingo Esparza
Año: 2023

RESUMEN

La tecnología ha llegado a un nivel de desarrollo que se encuentra presente en casi todas las actividades de la vida diaria, realizar un pago en una tienda, con una transacción financiera a través de un teléfono y en áreas como la medicina, educación, periodismo, música, comunicación y un sinfín de otras ramas del conocimiento humano. En los adolescentes la parte que más se ha visto afectada es la manera en la que se comunican por el aparecimiento de una serie de redes sociales y otro tipo de aplicaciones que han transformado la vida actual de los adolescentes. Todo es instantáneo, una foto, un video, una conversación, un juego, una noticia, todo es en vivo, al momento, esto ha cambiado la forma que tienen ellos de concebir el mundo, porque pueden incluso para un juego compartirlo con personas que no conocen y ni siquiera podían hablar el mismo idioma, lo único que requieren es tener la afición por el juego y una conexión a internet. Con todas las facilidades de comunicación actual, también existen riesgos digitales a los que se encuentran expuestos los adolescentes, el objetivo del presente trabajo es hacer un aporte sobre este tema y conscientes de que en la actualidad prefieren estar en línea que leer un libro se ha desarrollado una plataforma interactiva que está disponible en la dirección https://seguridadinformaticarcn.com/rcn/web20/web/web.htm, con el fin de que puedan aprender jugando sobre la seguridad informática y sus riesgos digitales.

Palabras claves: Seguridad informática, riesgos digitales, internet, adolescentes.

ABSTRACT

Technology has reached a level of development that is present in almost all activities of daily life, making a payment in a store, with a financial transaction through a telephone and in areas such as medicine, education, journalism, music, communication, and countless other branches of human knowledge. In adolescents, the part that has been most affected is the way in which they communicate due to the appearance of a series of social networks and other types of applications that have transformed the current lives of adolescents. Everything is instantaneous, a photo, a video, a conversation, a game, a news item, everything is live, in the moment, this has changed the way they conceive the world, because they can even share it with a game with people who They do not know and could not even speak the same language, the only thing they require is to have a love for the game and an internet connection. With all the current communication facilities, there are also digital risks to which adolescents are exposed, the objective of this work is to make a contribution on this topic and aware that currently they prefer to be online than reading a book developed an interactive platform that is available at the address https://seguridadinformaticarcn.com/rcn/web20/web/web.htm, so that they can learn by playing about informatic security and its digital risks.

Keywords: Informatic security, digital risks, internet, teenagers

CAPITULO I
El problema

1.1 Planteamiento del problema

En las últimas décadas la tecnología abarca prácticamente todos los ámbitos del desarrollo humano tanto en la parte personal como en la sociedad en general. La educación es una de las múltiples áreas en donde la tecnología a través de diferentes aplicaciones ha empezado a transformar el proceso de enseñanza aprendizaje.

El periodo actual en el que nos encontramos producto de la pandemia del COVID 19 prácticamente ha obligado que tanto profesores, alumnos y padres de familia se involucren con diferentes herramientas informáticas para poder continuar con la educación en los diferentes niveles.

En internet encontramos a parte de las aulas virtuales otro tipo de herramientas como son redes de conocimientos, redes sociales, pizarras electrónicas, libros digitales,herramientas MOCC, banco de preguntas y un sinnúmero de aplicaciones que permiten mejorar el proceso de enseñanza aprendizaje.

Los docentes, alumnos y padres de familia no se han enfocado en un aspecto relevante de la tecnología que es la seguridad informática en la educación, en el país en general casi no existe ningún tipo de legislación en cuanto a esta temática se refiere, apenas el 21 de Mayo del 2021 en el Registro Oficial No. 469 se publicó la "Ley orgánica de datos personales", cuya finalidad es garantizar el ejercicio del derecho a la protección de datos personales, consideremos que el 30 de Noviembre de 1988 se celebró por primera vez el día mundial de la seguridad de la información por iniciativa de la Association for Computing Machinery (ACM).

Ante la ausencia de procesos en el tratamiento de la información por parte de los docentes y de padres de familia, el alumno debería poseer competencias para actuar en casos de problemas tecnológicos al igual que saber cómo hacerlo en situaciones que se pueden presentar en su vida normal.

La falta de conocimientos de seguridad informática en la educación en la actualidad ya conlleva diferentes tipos de riesgos que se producen en los centros de

formación como son ciber acoso, sustracción de la información, pérdida de la privacidad, pornografía, fraudes informáticos, usurpación de la identidad, amenazas, usurpación a contenidos nocivos, publicación de información privada, ciberacoso, sexting, grooming entre otros.

Los alumnos no saben cómo actuar cuando se presentan estos riesgos puesto que adicionalmente existen las redes sociales que permiten propagar cualquier tema en tiempo real lo que dificulta más la solución del problema.

En el Ecuador la seguridad de la información es un tema poco conocido por la sociedady poco tratado y la seguridad informática en la educación es prácticamente nula, en los colegios no existe lineamientos ni políticas escritas sobre los diferentes tipos de riesgos que existen por el uso de la tecnología en el ámbito educativo ni una planificación para minimizar los riesgos.

La informática sigue creciendo a pasos agigantados en todos los ámbitos incluyendo el de la educación, sin embargo solo para brindar un ejemplo para navegar en internet en casa no existe el conocimiento, ni maneras gratuitas de controlar la información a la que se accede en especial los menores de edad, si sumamos a esto que el acceso a dispositivos tecnológicos cada vez es mayor dentro de la sociedad ecuatoriana, según ARCOTEL (Agencia de Control y Regulación de las Telecomunicaciones) en su documento (Servicio Móvil Avanzado, 2023) para el mes de Enero del presente año existe un total de 17’513.535 líneas activas y en el documento (Cuentas de Servicio de Acceso a Internet Fijo y Móvil,2023) para el mes de Enero el 74,44% de la población tiene acceso a internet sea por medios móviles (celulares, tablets, otros) o fijos (Computadores de escritorio, portátiles), los problemas que se suscitan por la falta de conocimiento de seguridad informática son cada vez mayores.

Tabla 1: Cobertura de servicio móvil

Año / Mes	Total nacional de líneas activas	Población Nacional	Densidad nacional de líneas activas
Enero 2019	15’841.541	17’043.789	92,95 %
Enero 2020	15’906.957	17’288.207	92,01 %
Enero 2021	15’521.059	17’510.643	88,64 %

Enero 2022	16’848.189	17’989.912	93,65 %
Enero 2023	17’513.535	18’205.188	96,20 %

Fuente: Registros Administrativos ARCOTEL (Febrero 2023)

Tabla 2: Cuentas de servicio de acceso a internet fijo y móvil

Año / Mes	**Cuentas**	**Población Nacional**	**Cuentas Internet por cada 100 habitantes**
Enero 2019	11’428.471	17’043.789	67.05%
Enero 2020	11’921.796	17’288.207	68,96%
Enero 2021	12’563.020	17’510.643	71,75 %
Diciembre 2022	13’390.898	17’989’912	74,44%

Fuente: SIETEL - ARCOTEL (Enero 2023)

Con estos antecedentes se torna necesario coadyuvar al conocimiento de la seguridad dela información en el medio educativo mediante la implementación de técnicas didácticas que estén disponibles en línea a través de una página web tanto para docentes, alumnos y padres de familia interesados en el tema.

El 17 de Mayo del 2007 por el día mundial de la sociedad de la información, Hamadoun Touré, Secretario General de la UIT (Unión Internacional de Telecomunicaciones) dijo“….En un mundo cada vez más conectado, los jóvenes no sólo son los beneficiarios, sino a menudo también el motor de las últimas innovaciones y prácticas. La clave para alcanzar las aspiraciones de desarrollo de todos los habitantes del mundo reside en invertir en las generaciones futuras, sobre todo facilitando el acceso de los niños de hoy en día a las comunicaciones y mejorando sus capacidades…”

1.2 Antecedentes

Johanna Morales Carrillo1, Nerina Avellán Zambrano, José Simón Mera Cantos, María Zambrano Bravo (2019) realizan un estudio sobre ciberseguridad en instituciones de educación superior en Manabí en base a la norma técnica ISO 27001. La metodología utilizada tuvo un enfoque de tipo cualitativo descriptivo. La población objetiva fue la Universidad Técnica de Manabí (UTM), Universidad Laica Eloy Alfaro de Manabí (ULEAM), Escuela Superior Politécnica Agropecuaria de

Manabí Manuel Félix López (ESPAM MFL) y Universidad Estatal del Sur de Manabí (UNESUM), como resultado se obtiene un plan que permite a las Universidad mitigar los riesgos de la seguridad de la información.

Bragado Pérez (2014) realiza un plan estratégico de seguridad y privacidad en la red para alumnos y docentes en los centros de enseñanza, este plan es general pero puede aplicarse de manera particular con ciertos cambios en las diferentes instituciones educativas, Trata sobre alguno de los problemas existentes en cuanto se refiere a seguridad informática en la Educación. La metodología utilizada tiene un enfoque cualitativo descriptivo y como resultado como ya se ha mencionado es un plan estratégico aplicable a nivel general para cualquier educación educativa.

España Villegas (2014) en la Universidad de Educación a Distancia de Madrid realiza un estudio sobre seguridad e internet en educación para el Colegio Felipe Palazón ubicado en la ciudad de Tarija en Bolivia el enfoque de la metodología de la investigación es descriptiva como resultado del trabajo se obtienen algunas recomendaciones y guías para una navegación segura en internet y el tratamiento de diferentes tipos de ataques informáticos

Rodríguez (2009) desarrolla el siguiente tema Seguridad Informática para alumnos de la Escuela Secundaria. Software educativo, un aporte a la educación. Desarrolla una herramienta para facilitar el aprendizaje a los estudiantes de secundaria sobre la seguridad informática. El enfoque de la metodología es aplicativo. Como resultado se obtiene el análisis, diseño y construcción del prototipo de la herramienta informática y se acoge las sugerencias de diferentes maestros para llevar adelante la implementación de la herramienta. El trabajo termina con la construcción del prototipo.

Como un punto adicional dentro de antecedentes se debe mencionar que en países como Argentina para hablar de Sudamérica ya se debate sobre la necesidad de incluir como materia de bachillerato la seguridad informática debido a la importancia de esta temática para la sociedad en el presente y más aún en el futuro, en Ecuador sin embargo todavía no existen lineamientos ni políticas de estado al respecto, el conocimiento de la seguridad informática en general dentro la sociedad ecuatoriana es prácticamente nulo.

1.3 Objetivos de la Investigación

1.3.1 Objetivo General

Diseñar estrategias didácticas para la prevención de riesgos tecnológicos relacionados a la seguridad informática dirigido a estudiantes de tercero de bachillerato.

1.3.2 Objetivos Específicos

1. Recopilar bases teóricas y conceptuales de la problemática de la seguridadinformática con especial énfasis en la educación.
2. Desarrollar estrategias didácticas en una plataforma tecnológica interactivasobre seguridad informática dirigido a estudiantes de tercero de bachillerato
3. Evaluar el impacto de la implementación de la estrategia didáctica.

1.4 Justificación

Los delitos informáticos van en aumento en Ecuador, según las denuncias presentadas en la Fiscalía, desde antes de la pandemia del COVID-19. En el 2017 se registraron 8421 casos, subieron a 9571 y 10270 en el 2018 y 2019 respectivamente, la tendencia se aumentó.

Refiriéndonos a las cifras, desde el año 2014 hasta el 2020, de acuerdo con estadísticasde la Fiscalía General del Estado, se han registrado 821 denuncias por contacto con finalidad sexual con menores de dieciocho años, estos datos son reales y estadísticos en cuanto a temas que se han registrado en la Fiscalía, sin embargo existen muchos temas sobres los riesgos informáticos sobre todo en adolescentes que no tienen una estadística real por parte de ningún organismo del estado, nada se dice por ejemplo sobre el ciber acoso, el grooming, exposición a contenidos nocivos solo mencionando unos pocos riesgos.

Frente a esta situación, se torna de vital importancia generar un espacio didáctico de enseñanza aprendizaje dirigido a jóvenes, maestros y padres de familia que les proporcione herramientas de conocimiento frente a los diferentes tipos de riesgos informáticos que se puedan presentar en la educación, un manejo adecuado de los riesgos informáticos permitirá saber la manera de actuar ante diferentes situaciones que pueden presentarse con el manejo de herramientas tecnológicas en la educación.

El desarrollo de un aplicativo interactivo en línea garantiza que cualquier persona interesada en estos temas pueda ingresar para investigar de una manera entretenida los riesgos de la seguridad informática en la educación, al ser una plataforma la web, la existencia de este aplicativo puede generar un efecto rebote donde muchas más personas puedan acceder a revisar este tipo de información que sin duda alguna es importantes en la actualidad y será un tema imprescindible en el futuro, en vista de que ya se habla sobre el papel de la tecnología en la educación pos pandemia.

La tecnología ha cambiado la forma en la que interactuamos en la sociedad, desde actividades tan simples como envío de cartas, una felicitación de cumpleaños, una llamada telefónica hasta otros tipo de aspectos mucho más complejos, se encuentra en prácticamente todas nuestras actividades, en el mediano plazo la tecnología como la conocemos en la actualidad cambiará de manera radical; se habla de hologramas, realidad virtual, avatares y otras, sin embargo un aspecto importante a considerar como un eje transversal es la seguridad informática. En base a estás consideraciones es oportuno investigar la seguridad informática en la educación con el fin de realizar una contribución en esta temática.

En cuanto a la factibilidad técnica se refiere se investigará sobre una herramienta open source que permita desarrollar una plataforma con diversos tipos de material didáctico interactivo en línea para interesar al estudiante sobre la seguridad informática en la educación. Además, se requiere de un computador que soporte la herramienta que permitirá desarrollar la plataforma. En base a esto se puede decir que existen algunas herramientas open source para desarrollar la plataforma y se dispone del equipo informático por lo que desde el punto de vista técnico el proyecto es totalmente factible. La factibilidad económica al ser una herramienta open source se evita el tema del costo de licencias, el obtener un dominio y el alojamiento en un hosting están dentro de un manejo económico razonable, por lo que desde el punto de vista económico el proyectoes es factible.

Por ende, la presente investigación es viable porque se dispone de los recursos técnicos,económicos, legales y existen fuentes de información para desarrollar el tema.

CAPITULO II
Marco Teórico

2.1 Introducción

La tecnología de la información y comunicación ha influido en los hábitos cotidianos como seres humanos, por ejemplo, la manera de comunicarse, la forma en la que se recepta las noticias, incluso la manera en la que se escucha la música o el ver una película, tomarse una foto o el simple envío de un mensaje, entre otros.

La tecnología como se la conoce hoy ha evolucionado con el tiempo, tanto en hardware como en software, al comienzo el acceso a la tecnología estaba restringido para pocas personas normalmente con conocimientos en informática a costos elevados y recursos de hardware limitados, conforme se han desarrollado nuevas tecnologías, estas se pusieron al alcance de un mayor número de personas a un costo razonable y con un rendimiento del hardware cada vez mejor. La evolución en cuanto al software ha sido similar, al comienzo era una interfaz de texto con líneas de comandos para ejecutar programas y todo fue evolucionando a interfaces gráficas cada vez más fáciles de entender y por lo tanto, de operar para los usuarios.

Sin duda la aplicación que más ha influido en la vida de las personas es el aparecimiento del internet y con ello de un sinfín de aplicaciones al alcance de todas las personas que tengan acceso a esta red.

Con el aparecimiento de los teléfonos celulares cada vez un mayor número de personas tiene acceso a la tecnología en el mundo, según la empresa Statista que es uno de los proveedores líderes de datos de mercado e información sobre los consumidores, en el año 2021, cuatro mil novecientos millones de personas tenían acceso a internet, esto ocurre tan solo 60 años después de su creación.

Referente a este tema Sánchez-Teruel, D., y Robles-Bello, M. A. (2016) exponen: “Las TIC expanden las posibilidades de la comunicación, generan nuevas culturas y posibilitan el desarrollo de otras habilidades y formas de construcción del conocimiento” (p. 190).

Las actividades y aplicaciones que se pueden realizar a través del internet son innumerables, sin embargo, se pueden clasificar en cuanto a su uso se refiere de la siguiente manera:

- Redes y Mensajería.- Facebook, Instagram, Twiter, Whatsapp, medios comunicacionales, chats, correo electrónico, y otros.
- Recreación online.- Youtube, Spotify, Netflix, juegos, apuestas, son algunos de los ejemplos.
- Estudios e investigación.- Información técnica y actualizada, plataformas virtuales, acceso a base de datos, video conferencias, entre otros.
- Compras online.- a través de diferentes plataformas que permiten adquirir bienes o servicios en diferentes partes del mundo desde un computador.

En el año 2001 Marc Presnky en su artículo "Digital Natives, Digital Immigrants" define por primera vez el término nativo digital, refiriéndose a la primera generación que nació con la tecnología, es decir tiene una facilidad natural e intuitiva para el manejo y operación de todo tipo de dispositivos tecnológicos, entre ellos, ordenadores, teléfonos celulares, el uso de internet, mientras que los inmigrantes digitales son todos aquellos que no nacieron en la época de la tecnología pero que por diferentes razones han tenido que acceder a su uso y operación y han terminado adoptando la tecnología en el desarrollo cotidiano de sus actividades.

La tecnología ha evolucionado con el tiempo y cada día se encuentran al alcance de un mayor número de personas alrededor del mundo y dentro de este esquema, su uso acoge un mayor número de niños y adolescentes que tienen acceso a la tecnología y los diferentes usos, sobre todo a través del manejo de internet. Según la empresa DataReportal que presenta análisis gráficos y estadísticos de diferentes fuentes tanto de empresas públicas y privadas, agencias gubernamentales, organizaciones no gubernamentales, para el año 2023, la red social con el mayor número de usuarios es Facebook con un total de dos mil novecientos sesenta millones de cuentas aproximadamente, lo que lleva a dimensionar la magnitud de esta red social. En base a los datos obtenidos por esta misma empresa, se presenta los datos del número de cuentas de las 10 principales y más numerosas plataformas sociales.

Tabla 3.- Número de usuarios por plataforma social

Plataforma Social	Número de usuarios (En millones)
Facebook	2,958
Youtube	2.514
Whatsapp	2.000
Instagram	2.000
Wetchat	1.309
Tiktok	1.051
Facebook Messenger	931
Douying	715
Telegram	700
SnapChat	625

Fuente: Empresa Datareportal (Enero 2023)

Si se revisa los datos en cuanto a plataformas sociales se refiere, en Ecuador se encuentra que, la más popular sigue siendo Facebook, según el estudio presentado por la empresa ecuatoriana Mentinno Group que se dedica a la comunicación, contenidos y publicidad digital y ha sido reconocida como Google Partners awards, el número de usuarios en la mencionada red social es de más de trece millones. Las principales plataformas sociales en el Ecuador según el número de usuarios se detallan en el presente cuadro:

Tabla 4.- Número de usuarios por plataforma social en Ecuador

Plataforma social	Número de usuarios (En millones)
Facebook	13,1
Tiktok	10
Instagram	6,2
Spotify	5,6
Linkedin	3,5
Pinterest	3,1
Snapchat	2
Twitter	1,9
Reddit	0,5

Fuente: Mentinno Group (Diciembre 2022)

En base a los datos difundidos por la misma empresa se analizarán las dos redes sociales con más usuarios en Ecuador, Facebook y Tiktok.

Tabla 5.- Número de usuarios por edades en la plataforma Facebook en Ecuador

Rango de Edades	Porcentaje de usuarios	Número de Usuarios
13 a 17	7,1	930.100
18 a 24	25,2	3’301.200
25 a 34	28,3	3’707.300
35 a 44	18,3	2’393.300
45 a 54	10,7	1’401.700
55 a 64	6,1	799.100
Mas de 65	4,3	563.300

Fuente: Mentinno Group (Diciembre 2022)

Tabla 6.- Número de usuarios por edades en la plataforma Tiktok en Ecuador

Rango de Edades	Porcentaje de usuarios	Número de Usuarios
Menores de 18	25	2’500.000
18 a 24	24,32	2’432.000
25 a 34	24	2’400.000
35 a 44	10	1’000.000
45 a 54	5	500.000
Mayores de 55	3	300.000

Fuente: Mentinno Group (Diciembre 2022)

Si se considera los datos que se presentan en los cuadros y se compara con el número de habitantes que reporta el INEC en su revista “País atrevido: la nueva cara sociodemográfica del Ecuador”, se puede concluir que más, del 80% de la población, comprendida entre 5 y 18 años, dispone de algún tipo de red social y de acceso a internet.

Trucco (2014) afirma que “el aumento de la conectividad en los hogares con jóvenes de edades entre 10 y 19 años es más acelerado que el que registran los hogares compuestos únicamente por mayores de 20 años” (p. 20).

En base a todo el análisis realizado se puede determinar que el acceso a una plataforma social es un tema común en los adolescentes, puesto que, sienten la necesidad de aprovechar los recursos que brindan las diferentes plataformas, es decir, al ser nativos digitales les gusta intercambiar fotos, grabar videos, escuchar música, enviar mensajes, jugar en línea y un sinfín de actividades que se pueden realizar a través del uso de internet, muchas veces la interacción se da entre personas que no conocen y que aparentemente disfrutan de sus mismos intereses, lo que a no dudarlo expone al adolescente a una serie de riesgos que se relacionan con la tecnología.

En línea existen diversos tipos de personas, no exclusivamente adolescentes que se esconden tras un dispositivo tecnológico con el fin de obtener algún tipo de beneficio personal o simplemente el placer de afectar a otras personas, este tipo de acciones se facilitan porque detrás de un computador existe una persona cobijada por el anonimato. La intención de esta investigación es difundir diferentes tipos de riesgos informáticos que pueden afectar a los adolescentes y algunas medidas que se pueden tomar para evitar ser víctima de este tipo de ataques, para de esta manera disfrutar de los beneficios que brinda el internet y sus diferentes tipos de usos y aplicaciones, todo esto mediante una plataforma interactiva que se encuentre en línea y que se pueda acceder a través del internet.

En conclusión y tomando como referencia lo que dicen Arab y Dias (2015) “El uso masivo de internet por parte de los adolescentes y jóvenes lleva entonces a una reflexión sobre los vínculos y a la necesidad de desarrollar un enfoque integrador, que permita visualizar tanto los riesgos como las oportunidades de esta nueva forma de comunicarse en línea” (p. 8).

El campo de la seguridad informática es muy amplio y se intentará investigar el campo desde el punto de vista de los riesgos a los que están expuestos los adolescentes por una falta de conocimiento del tema. En referencia a este tema, hay una frase de Pablo Pérez San José, que utilizó en el 1er. Congreso Internacional menores en las TIC, realizado en Octubre 2009, “…los adultos utilizan internet, los niños viven en internet…”, en tal virtud debemos ser conscientes de los riesgos para prevenirlos, evitarlos y combatirlos, y así aprovechar las grandes ventajas que ofrece internet..”

2.2 Internet

El internet ha posibilitado el funcionamiento de un sinnúmero de aplicaciones en línea, a través de internet en la actualidad una persona puede ver películas, jugar en línea, realizar llamadas, videollamadas, asistir a reuniones, enviar mensajes, buscar la ubicación de un lugar, dirigirse a ese lugar guiado por la aplicación, realizar compras, y una serie de actividades adicionales que se pueden realizar con tener un dispositivo electrónico y una conexión a internet. Pero, ¿cómo empezó todo esto?

Muchos de los grandes avances de la humanidad se han producido después de una guerra y en el caso del internet no fue la excepción, después de la segunda guerra mundial hubo un periodo que se llamó la guerra fría, que fue una época de alta tensión entre las dos grandes potencias de aquella época, Rusia y Estados Unidos, en un conflicto bélico, la información es un activo estratégico y precisamente el comienzo del internet fue la necesidad de un sistema de comunicaciones que sobreviviera a un conflicto.
Al respecto Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (1999) mencionan:

> “A principio de los años 60, la idea flotaba entre diversas instituciones americanas, como el Massachussetts Institute of Technology y la corporación RAND. Leonard Kleinrock del MIT publicó en julio de 1961 el primer trabajo sobre "conmutación

de paquetes" (la tecnología que permitía dividir los datos y que recorrieran rutas distintas). El Pentágono, a través de su Agencia de Proyectos de Investigación Avanzada (ARPA en sus siglas inglesas) financió la puesta en marcha de una prueba práctica. En 1969, el año que el hombre llegó a la Luna, se abría el primer nodo de la red ARPANET, en la Universidad de California en Los Ángeles. La historia podía haber quedado reducida tan sólo a una cuestión de ingenieros de telecomunicación y militares, pero por medio había gente interesada en otras cosas. El segundo nodo fue el del Stanford Research Institute (SRI), donde trabajaba Douglas Engelbart en un proyecto sobre "Ampliación del intelecto humano". Engelbart había inventado el ratón para ordenador un lustro antes, y se preocupaba por el trabajo en colaboración a través del hipertexto. No era un visionario aislado: en el MIT, J.C.R. Licklider ya discutía en 1962 su concepto de "Red Galáctica": un conjunto de ordenadores interconectados para dar acceso a almacenes de datos…"

Este fue al gran inicio, pero al término de la guerra fría se empezó a cambiar la idea de una red de ordenadores para almacenar datos y se empezó a enfocar en una red para compartir información entre personas, es decir, el objetivo se cambió y pasó de ser una gran red de almacenamiento de información a una gran red donde se podía acceder a la información sobre determinados temas de interés. En sus inicios lógicamente se trataban de temas científicos, aunque el desarrollo del internet y todas sus aplicaciones parecen modernos, muchas de las cosas que se utilizan en la actualidad llevan ya más de 50 años de estudio y experimentación, como se puede ver en el estudio realizado por Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (1999) donde dice textualmente: "La cultura llegaba pronto al nuevo medio: en 1971 Michael Hart creaba el Proyecto Gutenberg, para crear y difundir textos electrónicos gratuitamente (el estándar ASCII databa de 1968). En 1972, fecha de la demostración pública de la red apareció el primer programa de correo electrónico, que pronto se convirtió en una de las aplicaciones más usadas: tres años después ya se discutía el problema de cómo bloquear el "correo basura". A propósito: el primer emoticono [-)] se mandó en 1979. La recién creada herramienta de comunicación se empezaba a llenar de actividad humana…".

Pronto la red ARPANET, se empezó a unir con otro tipo de redes terrestres o satelitales para lograr este tema técnico, lo único importante era que compartieran el

mismo protocolo de comunicación, esto lo introdujo Robert Kahn en 1972 y lo llamó Internetting, porque servía para comunicarse entre redes (el término net en inglés). En ese mismo año, se crean los nombres de dominio que permanecen hasta el día de hoy. Y así empezó a evolucionar la red de redes, en 1972 existían 500 servidores conectados, mientras que, para el año de 1992 ya se tenía más de un millón de servidores interconectados, para el año 2017 se calcula más de ocho millones quinientos mil centros de datos que tienen conectados muchas veces cientos de servidores o hasta miles, por lo que, en la actualidad es imposible determinar el número de servidores conectados a esta red. No hay que confundir los servidores con los computadores que son operados por los usuarios que acceden a los diferentes servicios de internet.

Figura 1. Mapeo mundial de los centros de datos que disponen de servidores conectados

2.3 Seguridad informática

El avance de la tecnología en cuanto al hardware se refiere, permitió desarrollar aplicaciones cada vez más sofisticadas a nivel de software, de ahí que, aparece el término de seguridad informática como una forma de proteger la información, en la siguiente tabla se detallan varias definiciones sobre seguridad informática, según diferentes autores:

Tabla 7.- Definiciones de Seguridad Informática

Autores	Año	Título	Definición
Arango Gómez, O. D.	2023	El ABC de la seguridad informática: guía práctica para entender la seguridad digital.	"La seguridad informática se refiere al conjunto de prácticas, herramientas y técnicas diseñadas para proteger la confidencialidad, integridad y disponibilidad de los

			datos e información almacenados y procesados por los sistemas informáticos. Los ataques cibernéticos y las amenazas informáticas, como los virus, el malware y los hackers, pueden comprometer la seguridad de los sistemas informáticos y causar pérdidas financieras, daños a la reputación y riesgos para la privacidad de los usuarios.” (Arango Gomez, O. D.(2023))
Guaña-Moya, J.,	2022	Ataques informáticos más comunes en el mundo digitalizado	“La seguridad informática es la máxima expresión de la protección de los sistemas y datos frente a posibles amenazas y ataques cibernéticos “ (Guaña-Moya, J.,)
González Londoño, J.	2020	Estudio del estado actual de la seguridad informática en las organizaciones de Colombia.	“Se refiere a los procedimientos implementados para fortalecer la seguridad de los recursos tanto físicos como lógicos de un sistema informático con el fin de evitar que se vea comprometido el principio de autentificación garantizando que quienes acceden a la información son realmente los autorizados para ello. Entre estos se encuentran los servidores, equipos de cómputo, software, bases de datos y los entornos físicos donde se encuentran ubicados dichos elementos.” (González Londoño, J. (2020))

Sisti, M. A., & Majowka, P. D	2020	Seguridad Informática: La Protección de la Información en una Empresa Vitivinícola de Mendoza	"El proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización", (Sisti, M. A., & Majowka, P. D (2020)).
Demartini, M. V. N., & Ríos, M. J	2019	El impacto generado por la seguridad informática en las PYMES de Mendoza	La seguridad informática es un área de la informática que se enfoca en la protección de la infraestructura, computación, información contenida o circulante en un ordenador o red de ordenadores respectivamente. Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, con el fin de mantener un sistema de información seguro y confiable. (Demartini, M. V. N., & Ríos, M. J (2019))
Romero Castro M, Figueroa Morán G. Vera Navarrete D. Álava Cruzatty J. Parrales Anzúles G. Álava Mero C. Murillo Quimiz A. Castillo Merino M.	2018	Introducción a la seguridad informática y el análisis de vulnerabilidades	"La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la

	tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad." (Romero Castro M., Figueroa Morán G. Vera Navarrete D. Álava Cruzatty J. Parrales Anzúles G. Álava Mero C. Murillo Quimiz A. Castillo Merino M. (2018)

Fuente: Propia

A medida que el avance de la tecnología permitía ir desarrollando nuevas aplicaciones que funcionan a través del internet, aparecen nuevos términos que conciernen a la seguridad de la información, como por ejemplo, cibercrimen, ciberdelincuente o ciberdelito, que no es más que una descripción rápida de actividades no legales que se pueden cometer en el ciberespacio, es decir en el uso de diferentes aplicaciones a través del internet. Como dice Subijana Zunzunegui (2008) acerca del ciberdelito: "se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y, se benefician de lagunas de punibilidad que pueden existir en determinados estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas" p. (171).

Con esta introducción se tomará como referencia la definición técnica de IBM (2022) para la seguridad de la información que textualmente dice: "La ciberseguridad es la práctica de proteger los sistemas más importantes y la información confidencial ante ataques digitales. También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad están diseñadas para combatir las amenazas a sistemas en red y aplicaciones, que se originan ya sea dentro como fuera de una organización".

Otra definición técnica importante a considerar es la que dice en la norma ISO 27001 (2017), que es un estándar internacional en la cual se establece los requisitos para la implementación de un sistema de gestión de seguridad de la información y textualmente dice: "La ciberseguridad tiene como foco la protección de la información digital que vive

en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información".

Estas dos definiciones son las más técnicas en cuanto se refiere a la seguridad de la información de manera general, pero, este caso de estudio se enfoca en lo referente a los riesgos que corren los niños y adolescentes en el manejo de los diferentes recursos tecnológicos que promueve el internet.

Una definición sobre seguridad informática que abarca tanto la parte empresarial cuanto lo referente a los usuarios de todas las edades es la que dicta la UIT, que es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación y sus siglas significan Unión Internacional de Telecomunicaciones, define en sus recomendaciones UIT-T X.1205 (2008) a la ciberseguridad como: "El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno". Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedias, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

- Disponibilidad;
- Integridad, que puede incluir la autenticidad y el no repudio;
- Confidencialidad." (p. 3)

La educación de los niños y adolescentes de manera general siempre ha sido una preocupación de los padres a través de los tiempos, sin embargo, sobre todo, por la brecha generacional en temas tecnológicos, el campo de la seguridad de la información está siendo desapercibida.

Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019) respecto a la ciberseguridad y los adolescentes dicen: "La temática de ciberseguridad, actualmente, en razón del uso de

las redes sociales por parte de la niñez y la adolescencia, debe ser un tema de discusión y análisis familiar, mediante el empleo de metodologías prácticas y contextualizadas, innovadoras y significativas, que permitan dar solución a problemáticas relacionadas con los peligros en la red a los que se enfrenta la población de interés". (p. 21)

A manera de conclusión se puede decir que, la seguridad en la información para adolescentes es sobre todo un conjunto de buenas prácticas que se deben seguir en el uso de los diferentes recursos tecnológicos, para que los adolescentes no se encuentren expuestos a una serie de riesgos informáticos.

2.4 Riesgos informáticos

El número de aplicaciones y usos que se le puede dar a la navegación en internet es muy amplio, por lo que un usuario normal está expuesto a una serie de riesgos informáticos, con mayor razón los niños y adolescentes que pasan muchas horas al frente de dispositivos electrónicos, sean estos: computadores de escritorio, portátiles, tablets, teléfonos inteligentes, entre otros, prácticamente sin ningún tipo de control por parte de los docentes o de los padres de familia, lo que multiplica su exposición a diferentes tipos de riesgos digitales. En resumen, el riesgo digital se define como aquellas consecuencias no esperadas resultante del uso de la tecnología. Se presenta un análisis de los principales riesgos a los que se encuentran expuestos los adolescentes, producto de la adopción de nuevas tecnologías en la vida diaria de cada uno de ellos.

2.4.1 Ciberbulling

Para analizar el ciberbulling como uno de los riesgos informáticos a los que se encuentran expuestos los adolescentes, a manera de introducción en la tabla siguiente se muestran algunas definiciones de diferentes autores sobre el tema:

Tabla 8. Definiciones de Ciberbulling

Autores	Año	Título	Definición
Microsoft México	2022	¿Cómo proteger a tus niños y adolescentes de	"El ciberbulling es el uso de la tecnología para demostrar

		los riesgos en línea? Guía de ciberseguridad para padres de familia	comportamientos agresivos y de manera repetida con el fin de causar burla, degrado o acoso a alguien menos poderoso.” (Microsoft México (2022))
Álvaro Cabrera, E	2022	Bullying y Ciberbullying en adolescentes de Educación Secundaria Obligatoria: incidencia y variables sociales asociadas.	“El ciberbullying es el uso de información electrónica y medios digitales utilizados para acosar sicológicamente a una persona o a un grupo de personas de manera reiterada, agresiva y de forma intencional.” (Álvaro Cabrera, E(2022))
Basante	2020	Riesgos digitales	“El cyberbullying es el acoso por medio de dispositivos digitales que se realiza entre pares” (Basante (2020))
Alvites-Huamaní	2019	Adolescencia, cyberbullying y depresión, riesgos en un mundo globalizado.	“Las TICs han elevado el bullying al cyberbulling basados en una amplia audiencia y encubiertos en el anonimato.” (Alvites-Huamaní (2019))
Cardozo, G., Dubini, P., & Lorenzino, L.	2017	Bullying y cyberbullying: un estudio comparativo con adolescentes escolarizados.	“El cyberbullying es la intencionalidad de causar daño. El acoso escolar se extiende al acoso cibernético de modo que los diversos problemas escolares entre adolescentes se trasladan al ciberespacio.” (Cardozo, G., Dubini, P., & Lorenzino, L.(2017))
Garay, R., Ochoa, G., Cantero, F., & Ramos, N.	2012	Violencia, Victimización y Cyberbullying en adolescentes escolarizados/as: una perspectiva desde el Trabajo Social.	“De manera literal el ciberbullying no es un tema nuevo, solo que ha cambiado la manera de hacerlo por el acceso a las nuevas tecnologías, es decir son manifestaciones de violencia entre pares con el uso de nuevos recursos digitales.” (Garay, R., Ochoa, G., Cantero, F., & Ramos, N. (2012))

Fuente: Propia

El uso de la tecnología en los adolescentes especialmente de los teléfonos celulares inteligentes es una nueva forma de socialización entre los mismos, esto les ha permitido pasar gran parte del tiempo conectados al internet en diferentes aplicaciones.

Estas aplicaciones les facilita realizar actividades que hasta hace menos de 20 años eran impensables o poco comunes, por ejemplo, el mismo hecho de hablar por teléfono sin necesidad de que esté conectado a ningún tipo de cable, tomar una foto de las actividades que realizan en cualquier lugar donde se encuentren y que la foto esté lista en ese mismo momento o grabar un video. Actividades que se debería usar para entretenimiento entre adolescentes y que pueden terminar en un riesgo, pues hay quienes utilizan estas actividades para agredir, difamar, insultar o causar daño de manera deliberada.

Pasando de esta manera del bullying al cyberbullying, por ejemplo, una simple foto con un adecuado software de edición podría hacer que los personajes que intervienen en esta foto pasen hacer la burla de un determinado grupo social, con el agravante de que el cyberbullying se lo puede hacer las 24 horas del día, sin que el implicado se encuentre presente y la foto truncada incluso, podría difundirse a nivel mundial con las diferentes plataformas sociales existentes, lo que puede ocasionar daños irreparables en los implicados. Además, el autor intelectual de la foto podría tener una cuenta falsa, es decir, no es necesario tener una identificación falsa lo que hace aún más difícil el detectar al agresor.

> Alvites-Huamaní, C. G. (2019) sobre el cyberbullying manifiesta:
>
> "Las TIC han generado un uso indeseable de estos medios al haber extrapolado el bullying a un ciberbullying, caracterizado este último por ser un fenómeno oculto, con ciertos rasgos específicos: amplia audiencia (las redes sociales son infinitas), el anonimato (no se requiere tener una identidad o tener falsas credenciales) y la invisibilidad que la red permite (privilegio de darse en cualquier lugar y momento al permitir que se traspasen los límites temporales y físicos). Los mensajes publicados en la red son imperecederos (almacenados por periodos largos o durante toda la vida) y se cargan con rapidez y comodidad, debido a que las TIC pueden propagarlos y reenviarlos de manera rápida y sencilla. Además, las víctimas de ciberbullying sufren de insultos electrónicos, hostigamiento, denigración, suplantación, exclusión, ciberpersecución y difusión de aspectos

personales e íntimos sin su autorización. Esto ocurre todo el día y de forma repetitiva, en todos los medios tecnológicos e internet, lo que ha generado un deterioro en sus estados anímicos hasta el suicidio de aquellos que la padecen"

En resumen, para Basante (2020) "El cyberbullying es el acoso o intimidación a través de los diferentes dispositivos inteligentes (celular, computador, tabletas, consolas, entre otros) que se realiza entre pares".

2.4.2 Grooming

Con el aparecimiento de redes sociales la forma de comunicarnos los seres humanos ha sufrido cambios sustanciales, sin embargo, entre los adolescentes el cambio ha sido drástico, porque la virtualidad ha reemplazado a la presencialidad, por lo que el uso de redes sociales entre adolescentes para relacionarse es primordial, esto ha generado la exposición a riesgos como el grooming, por lo que, a continuación se muestran definiciones de diferentes autores sobre el tema.

Tabla 9.- Definiciones de Grooming

Autores	**Año**	**Título**	**Definición**
Calvete, E., Orue, I., & Gámez-Guadi, M.	2022	Una intervención preventiva para reducir el riesgo de grooming online entre los adolescentes. Psychosocial Intervention	"Es el abuso sexual a adolescentes por parte de adultos en línea, es decir a través de las aplicaciones de internet con consecuencias negativas para las víctimas". (Calvete, E., Orue, I., & Gámez-Guadi, M.(2022)).
Lachaise, S. M., & Massa, A.	2022	Hablemos sobre grooming.	"El grooming es el abuso sexual a niños y adolescentes que lo realiza una persona mayor de edad con el uso de las nuevas tecnologías y las diferentes aplicaciones como son redes

			sociales, juegos en línea, chats entre otros. Es un acto de acoso progresivo, en el cual el adulto establece un vínculo de confianza y control emocional con el menor, basado en manipulaciones y engaños; uno de sus principales objetivos es obtener material de abuso sexual contra los menores de edad". (Lachaise, S. M., & Massa, A.(2022))
Ruiz, M. S.	2022	Maltrato de la población adolescente a través de las TICS (grooming, sexting, ciberbullying)	"El grooming es la acción ejercida deliberadamente por un adulto (o dos niños donde pueda establecerse una relación de poder y un control emocional) sobre un niño, siendo el contenido del acoso sexual. El fin último es obtener imágenes de pornografía infantil o cometer abuso sexual. Por tanto, para considerarse grooming debe existir contenido sexual y obtenerse mediante coacción". (Ruiz, M. S.(2022)).
Choi, HJ, Mori, C., Van Ouytsel, J., Madigan, S. y Temple, JR	2019	Participación de adolescentes en sexting durante 4 años y asociaciones con la actividad sexual. *Diario de Salud Adolescente, 65* (6), 738-744.	"El grooming es un proceso en línea mediante el cual un adulto manipula a un menor de edad usando el internet con el fin de abusar sexualmente del menor". (Choi, HJ, Mori, C., Van Ouytsel,

			J., Madigan, S. y Temple, JR (2019))
Estiarte, C. V.	2017	Predadores sexuales online y menores: grooming y sexting en adolescentes. e-Eguzkilore,	"Grooming es la conducta consistente en la cual una persona adulta intenta hablar en línea con un menor de edad en contra de su voluntad, o le pide hablar sobre sexo, solicita información sexual o que realice alguna conducta sexual no deseada. Si el groomer es otro menor de edad este autor no considera grooming las acciones antes mencionadas". (Estiarte, C. V.(2019))
Santisteban, P. y Gámez, M.	2017	Online Grooming y Explotación Sexual de Menores a Través de Internet	"Es la venta y distribución de material pornográfico en línea." (Santisteban, P. y Gámez, M. (2017)).

Fuente: Propia

Montalvo, Peñalva & Itziar (2015) mencionan que "una de las principales actividades realizadas a través de la red se relaciona con el desarrollo de las relaciones sociales. Así mismo actualmente se observa una sobre saturación de información en la red, superando incluso a la radio, televisión y prensa. El exceso de contenido distribuido por la Internet y redes sociales deja al usuario expuesto a demasiada información que supera la capacidad de procesamiento y asimilación cognitiva. Por lo que cada individuo debe generar nuevas formas de ingreso de información a niveles manejables".

El uso de las redes sociales se ha popularizado sobre todo en los adolescentes para exponer sus actividades de manera gráfica, sea a través de fotos, videos u otro tipo de aplicaciones, que además puede incluir efectos, letras y otro tipo de características, gracias a la facilidad de software de edición que ahora existen, e incluso se pueden cargar

estas aplicaciones en los teléfonos celulares. Esto ha permitido que las relaciones sociales entre adolescentes cambien del modo presencial al modo virtual, intercambian mucha información a través de sus teléfonos celulares y otro tipo de dispositivos electrónicos, en resumen, empiezan a divulgar su vida social en las redes, lo que facilita la posibilidad de sufrir algún tipo de delito digital o acoso cibernético.

La exposición en redes de la vida social e incluso a veces íntima facilita la posibilidad de sufrir otro tipo de acoso llamado grooming, que se lo entiende cuando un adulto, aprovechando el entorno virtual y el anonimato persuade, convence y victimiza sexualmente a un menor de edad, en ciertos casos incluso se puede pasar del plano virtual al plano físico al concretarse una cita por medios digitales, el objetivo final de todo esto es obtener un rédito económico.

Santisteban y Gámez (2017) lo definen: "El Grooming permite la elaboración de material pornográfico para la venta y distribución on line. Actualmente, se han reportado múltiples casos de este tipo que ha llevado a la creación de varias campañas publicitarias en Latinoamérica. Es un fenómeno que va creciendo de forma silenciosa entre la población juvenil y deja como resultado consecuencias evidenciables para el resto de la vida".

2.4.3 Sexting

Otro riesgo informático a los que se encuentran expuestos los adolescentes es el sexting, el cual es una variación del grooming, para conocer más sobre este tema se analizan definiciones de diferentes autores.

Tabla 10.- Definiciones Sexting

Autores	**Año**	**Título**	**Definición**
Microsoft México	2022	¿Cómo proteger a tus niños y adolescentes de los riesgos en línea? Guía de ciberseguridad para padres de familia.	"Sexting es el intercambio de mensajes, imágenes, videos de carácter sexual explícito". (Microsoft México (2022))

Alonso Mezarina, N., & Orcon Abregu, X. M.	2022	Sexting y autoestima en estudiantes de una universidad privada de Lima Norte,	"Sexting es el envío y recepción de imágenes o videos de contenido sexual a través de smartphones o dispositivos electrónicos ya sean computadoras o laptops y que se da de forma virtual y voluntaria". (Alonso Mezarina, N., & Orcon Abregu, X. M. (2022))
Alcantara	2019	Palabras invasoras, el español de las nuevas tecnologías.	"El sexting es una forma de acoso cibernético donde el protagonista es el adolescente y el victimario es el acosador. En tal virtud el sexting es el intercambio de imágenes sexuales a través de dispositivos, la forma más común de sexting es el selfie con fotos donde la persona hace posturas sugerentes." (Alcántara (2019))
Contreras, C. T. M., & Herrera,	2017	Sexting practicado por adolescentes: su morfología en Facebook. *International*,	"El sexting es un intercambio de mensaje a través de conversaciones privadas por medios digitales que tiene contenido sexual de manera explícita o de forma implícita. El contenido puede contener solo texto o imágenes o videos, de las personas que intervienen en el intercambio de mensajes". (Contreras, C. T. M., & Herrera (2017))
Estiarte, C. V.	2017	Predadores sexuales online y menores: grooming y sexting en	"El sexting, por su parte, expresa un neologismo en que se contraen los terminos "sex" y "texting".

	adolescentes. e-Eguzkilore,	Constituye la designación que han empleado los medios de comunicación y los investigadores para referirse a las comunicaciones de contenido sexual que incluyen tanto mensajes de texto como imágenes que son transmitidas empleando teléfonos móviles y otros medios electrónicos". (Estiarte, C. V. (2017)).

Una variación del grooming es el sexting que no es más que el intercambio de cualquier tipo de mensajes, fotos o videos con cierto contenido erótico o de plano sexual generalmente entre adolescentes. La diferencia es que esto ocurre normalmente entre iguales, es decir entre personas que tienen algún tipo de relación sentimental. Por lo regular, no existe ningún tipo de interés económico. El riesgo se produce cuando se termina la relación y uno de los dos miembros de la pareja decide hacer públicas las fotos a través de cualquier red social. Algunos autores determinan que esta es una nueva forma que tienen los adolescentes para expresar y explorar su sexualidad.

Según mencionan (Farber, Shafron, Hamadani, Wald y Nitzburg 2012): "El envío de imágenes sexualmente sugestivas tanto de desnudos como de semidesnudos se ha vuelto una práctica considerada entre los adolescentes como común a su edad, que otorga una amplia popularidad por la apreciación de la sensualidad, por lo que es importante durante su etapa de crecimiento y que no genere grandes problemas".

El sexting en particular y los riesgos digitales en general, son temas de actualidad tanto es así que el diario El Comercio, en su edición escrita y digital del 01 de diciembre del 2022 emite un reportaje titulado: "Extorsión por 'sexting' y las apps espías entre los ocho tipos de violencia más comunes"[1]

[1] Dirección web del reportaje: https://www.elcomercio.com/tendencias/tecnologia/extorsion-sexting-apps-espia-ciberviolencia-comunes.html

Para Contreras, C. T. M., & Herrera, (2017), el sexting es el "intercambio de mensajes en alguna conversación privada (inbox) por medio de algún medio electrónico, con contenido sexual explícito o implícito, ya sea con texto y/o imagen creada por el autor, en donde se muestra desnudo o semidesnudo" (p. 198).

2.4.4 Cibersexo

El cibersexo es un tema importante que se debe considerar cuando se habla de riesgos informáticos entre adolescentes, el término se refiere a la virtualidad, en la siguiente tabla a manera de introducción se analizan definiciones de diferentes autores sobre el tema:

Tabla 11. Definiciones de Cibersexo

Autores	**Año**	**Título**	**Definición**
Madridiario (Página web)	2021	Qué es el cibersexo y con quién es mejor hacerlo.	"El cibersexo es cuando dos o más personas tienen sexo, y su único contacto es virtual, a través de redes tecnológicas. Intercambian llamadas, video llamadas o mensajes de contenido erótico explicito entre los participantes." (Madridiario (Página web)(2021)).
Rosas Murcia, A. G.	2021	Percepción del cibersexo desde un contexto sociocultural	"El cibersexo se define como una serie de conductas donde no se establece ningún tipo de contacto físico, sino que tiene como fin compartir y consumir todo tipo de contenido íntimo, sexual y pornográfico mediante dispositivos tecnológicos con otras personas, que se clasifica como una conducta riesgosa, pues deja este tipo de

			materiales navegando por la red." (Rosas Murcia, A. G. (2021)).
Aguirre Giraldo, C. A., & Rojas Riascos, K. J	2021	El Cibersexo en mujeres universitarias del distrito de buenaventura.	"El cibersexo es un concepto que comprende y engloba diversas prácticas sexuales que se originan en un campo cibernético, tecnológico y virtual". (Aguirre Giraldo, C. A., & Rojas Riascos, K. J (2021)).
García-Barba, M., Nebot-Garcia, J. E., & Giménez-García, C.	2019	Conductas sexuales de riesgo y uso del cibersexo. Comparación entre diferentes perfiles de uso del cibersexo	"El cibersexo es el uso de internet con fines sexuales, puede ser una actividad en solitario como mirar u observar videos u imágenes eróticas o con la implicación de otra persona a través de chats o video llamadas." (García-Barba, M., Nebot-Garcia, J. E., & Giménez-García, C. (2019)).
Calvo, J. C., Arnal, R. B., Llario, M. D. G., Mengual, V. M., & Sanchez, P. S.	2014	Internet, cibersexo y consumo de alcohol: estudio preliminar en adolescentes	"El cibersexo, entendido como el uso de internet con objetivos de gratificación sexual incluye actividades que pueden ir desde el visionado de pornografía hasta la interacción sexual con otros usuarios por medio de chats o webcams.". (Calvo, J. C., Arnal, R. B., Llario, M. D. G., Mengual, V. M., & Sánchez, P. S(2014)).

Fuente: Propia

Es una manera de sexo virtual (no existe ningún tipo de contacto físico) donde dos o más personas se envían mensajes de carácter sexual explícito tratando de recrear un contacto sexual real. En los mensajes puede existir incluso audios o sonidos para hacer más real la virtualidad, en caso de que exista acuerdo entre los participantes se puede

admitir incluso encender las cámaras de los dispositivos. Los diferentes participantes van emulando una situación real de manera tal que estimulan los deseos y las fantasías de los participantes virtuales. Este tipo de actividad se ha expandido en el mundo entero gracias a las facilidades de interconexión que brinda el internet, en esta red de redes existen muchísimos chats dedicados a este tipo de actividades. Cabe aclarar que este tipo de riesgos afecta no solamente a los adolescentes sino a cualquier persona indistintamente de la edad.

Figura 2. Captura de Pantalla de una aplicación chat de cibersexo en internet.

En conclusión, como afirma Aguirre Giraldo, C. A., & Rojas Riascos, K. J(2021) "el cibersexo es un concepto que comprende y engloba diversas prácticas sexuales que se originan en un campo cibernético, tecnológico y virtual, por esto el cibersexo se puede entender como una nueva forma o variante sexual que ha tenido una gran acogida y cada vez está ganando espectadores y curiosos, como tal la palabra cibersexo no tiene una conceptualización clara ya que la significación del mismo puede estar ligada a subjetividades, sin embargo, se considera cibersexo cuando dos o más personas comienzan a mantener encuentros de carácter sexual en plataformas virtuales, es allí donde la imaginación y el erotismo juegan un papel muy importante en la calidad y el disfrute de la experiencia ya que se carece obviamente del referente físico que para algunos es determinante a la hora de mantener relaciones sexuales." P. (22)

2.4.5 En las redes sociales

Las redes sociales han permitido que la comunicación sea prácticamente instantánea en cualquier lugar del mundo donde uno se encuentre, desde un simple diálogo entre dos personas hasta la difusión de una noticia, se lo hace prácticamente en segundos. A continuación, se revisa lo que entienden por redes sociales diferentes autores:

Tabla 12. Definiciones de redes sociales

Autores	Año	Título	Definición
Lardies, F., & Potes, M. V.	2022	Redes sociales e identidad: ¿desafío adolescente?	"Son plataformas de interacción social se emplean como herramientas para responder a las demandas culturales contemporáneas entre las que cabe destacar: la exhibición de la intimidad, la producción de un espectáculo del yo, el consumo de la vida ajena, la mirada del otro, la búsqueda de aprobación, entre otras". (Lardies, F., & Potes, M. V. (2022)).
Murillo Agudelo, A. I	2022		"Las redes sociales son un medio de comunicación informática rápida, por el cual las personas pueden compartir todo tipo de información ya sea audiovisual o por texto." (Murillo Agudelo, A. I (2022)).
Reynoso, B. L. G.	2022	Dependencia a las redes sociales en adolescentes de	"Las redes sociales son un conjunto de plataformas en internet que proporcionan comunicación accesible y así

		tercero básico de un colegio privado.	mismo interacción entre los individuos.” (Reynoso, B. L. G. (2022))
González Forte, M.	2022	Redes sociales y salud mental	“La red social es un sistema utilizado por un conjunto de personas con un objetivo principal, compartir información e interactuar entre ellos, generando relaciones sociales y creando perfiles de identidad.” (González Forte, M. (2022))
segu-kids.org	2015	Redes Sociales	“Una **red social** es un conjunto de usuarios relacionados a través de una plataforma en común, mediante la cual mantienen relaciones de forma virtual, que pueden desencadenar relaciones en el mundo físico”. (segu-kids.org (2015)).
Real Academia Española	2014	Redes Sociales. Definición 1.	“Se entiende por redes sociales al Servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base a criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir

	información, imágenes o vídeos, permitiendo que estas publicaciones sean accesibles de forma inmediata por los usuarios de su grupo." (Real Academia Española (2014)).

Fuente: Propia

Las redes sociales son una plataforma de comunicación entre personas que rompe los límites de las fronteras y con un alcance a nivel mundial. El acceso a un mayor número de personas diariamente a internet y el aparecimiento de los teléfonos inteligentes ha facilitado el auge y popularidad del uso estas redes. Otro de los efectos del uso de redes sociales ha sido la casi desaparición del teléfono de línea, puesto que las personas prefieren hacer una videollamada sin tener que conectarse a ningún cable y además, la misma no tiene costo puesto que se lo hace a través del internet.

Respecto a las redes sociales Hernández y Castro (2015) expresan: "permiten a los usuarios compartir con otros cibernautas todo tipo de información, aficiones, creencias e ideologías; facilitan las relaciones entre las personas, evitando así cualquier tipo de barrera temporal, cultural o física; brindan la oportunidad de mantener y profundizar relaciones creadas de manera presencial y sirven para encontrar apoyo en temas sensibles"

En referencia a los jóvenes y su relación con las redes sociales Chuquitoma (2017) dice: "Por otra parte, la adolescencia es una etapa del desarrollo humano, caracterizada por la búsqueda de la identidad, donde necesita de relaciones con sus coetáneos; las redes sociales son un medio propicio para el establecimiento de estos vínculos, incluso para los más tímidos; en este espacio digital pueden actuar de forma más espontánea y libre; logran descubrir personas con iguales gustos, preferencias y sentimientos".
Las redes sociales más usadas por los adolescentes según diferentes estudios son, Tiktok, Facebook e Instagram.

Según Lardies, F., & Potes, M. V. (2022), "se pueden categorizar las redes sociales online en cuatro tipos: las de carácter profesional como LinkedIn (plataformas de empleo) y/o Research Gate (colaboración científica); las de carácter personal, como Pinterest (plataforma para la inspiración artística); YouTube (para la publicación de videos) y WhatsApp (plataforma de mensajería instantánea); y las de carácter social, como Instagram, Facebook, Snapchat, Twitter, Tinder, Twitch, Tiktok P(6).

El uso inadecuado de las redes sociales también trae consigo ciertos riesgos digitales, el primero, que los adolescentes pueden perder de vista las relaciones y sentimientos reales, conversar con otros amigos u otras personas de diferente edad en forma presencial, la afectividad, el comportamiento porque el estar detrás de la pantalla les puede hacer perder las experiencias de la vida real. Además, se debe considerar que al estar detrás de una pantalla puede conseguir cierto tipo de emociones placenteras que son más complejas de obtener en la vida real. Otro aspecto que se debe considerar es la gran brecha digital que existe entre los adolescentes y sus padres, lo que trae como consecuencia una mayor dificultad de estos para poder guiarles.

El segundo riesgo importante que se presenta en las redes sociales es la inadecuada configuración de las cuentas, permitiendo que cualquier persona pueda acceder a información personal como son por ejemplo, fecha de nacimiento, nombres, intereses, gustos, escuela o colegio donde se educan y fotos, etiquetando a compañeros y familiare,s lo que facilita el cometimiento de otro tipo de delitos. En este aspecto se debe considerar también la posibilidad de que ciertos usuarios creen cuentas falsas y que alimenten la misma con información falsa, puesto que ninguna red social posee algún método para verificar la veracidad de la información, esto puede generar que se esté intercambiando información entre una cuenta real y con datos verídicos, con otra persona que tiene una cuenta, para intentar causar algún tipo de daño digital o presencial.

Un tercer riesgo del que se habla en los diferentes trabajos de investigación es el gran número de horas que pasan los adolescentes en el uso de redes sociales, sobre todo como un pasatiempo sin darle ningún tipo de uso académico, lo que termina provocando en muchos casos en una adicción a las redes sociales.

Según (Echeburua y Corral, 2010) cuando un adolescente presenta adicción a una plataforma social realiza la mayor parte de estas actividades:

- Dormir menos de 5 horas por estar conectados a las plataformas sociales.
- Descuidar otras actividades importantes, como el contacto con la familia, las relaciones sociales, el estudio o el cuidado de la salud.
- Recibir quejas en relación con el uso de la Red o del "smartphone" de alguien cercano, como los padres o los hermanos.
- Pensar en la Red o en el "smartphone" constantemente, incluso cuando no se está conectado, y sentirse irritado excesivamente cuando la conexión falla o resulta muy lenta.
- Intentar limitar el tiempo de conexión, pero sin conseguirlo, y perder la noción del tiempo.
- Mentir sobre el tiempo real que se está conectado o jugando un video juego.
- Aislarse socialmente, mostrarse irritable y bajar el rendimiento en los estudios.
- Sentir una euforia y activación anómalas cuando se está delante del smartphone.

En conclusión, las plataformas sociales utilizadas de manera adecuada pueden brindar al adolescente una serie de oportunidades y beneficios que aporten en sus actividades diarias, pero este mismo uso, sin ninguna guía o control les expone a riesgos innecesarios tanto en el plano virtual como en el plano real.

2.4.6 En los juegos en línea

En la actualidad se dispone de una variedad infinita de juegos en línea y para acceder al mismo solo se requiere dos condiciones: Conexión a internet y un dispositivo electrónico, para una mejor comprensión de lo que significa los juegos en línea, se analizan algunas definiciones en la tabla siguiente:

Tabla 13. Definición de Juegos en Línea

Autores	Año	Título	Definición
Solorzano, N. I., Moscoso Poveda,	2019	Evolución de Videojuegos y su Línea Gráfica, un	"Los videojuegos son un recurso tecnológico al cual se le está reconociendo su

S., & Elizalde Ríos, E.		enfoque entre la Estética y la Tecnología	utilidad desde otros puntos de vista, particularmente su uso en las aulas como herramienta de apoyo educativo. Se discute que los videojuegos con una buena planificación, proporcionan situaciones muy creativas que bien conducidas contribuyen o incentivan a la exploración, la investigación y los descubrimientos". (Solorzano, N. I., Moscoso Poveda, S., & Elizalde Ríos, E. (2019)).
Amador T.G.	2018	Agresividad e impulsividad en usuarios de videojuegos Online	"Los juegos masivos multijugador en línea (MMO por sus siglas en inglés), son juegos en donde existe una gran cantidad de usuarios que juegan en tiempo real a través de una conexión a internet. Este tipo de juegos se debe colaborar entre si y se compite contra un equipo enemigo para lograr objetivos propuestos según la modalidad del juego." (Amador T.G. (2018)).
Rivera Arteaga, E., & Torres Cosío, V	2018	Videojuegos y habilidades del pensamiento	"Un videojuego es un juego electrónico en el que una o más personas interactúan. Su interfaz es por medio de una pantalla, de ahí su nombre "videojuego",

			el cual ha ido evolucionando gracias al avance de las tecnologías, alcanzando mayor complejidad y robustez. Puede implementarse en una o más plataformas, como una computadora, una consola, un dispositivo portátil (un teléfono móvil, tableta), árcade (máquinas de videojuegos adaptadas para locales públicos), etc." (Rivera Arteaga, E., & Torres Cosío, V. (2018)).
Corral, E. M.	2017	El videojuego y las nuevas tendencias que presentan al mercado de la comunicación.	"Reducido a su esencia formal, un juego es una actividad entre dos o más personas con capacidad para tomar decisiones que buscan alcanzar unos objetivos dentro de un contexto limitado. Una definición más convencional es aquella en la que un juego es un contexto con reglas entre adversarios que intentan conseguir objetivos." (Corral, E. M. (2017)).
segu-kids.org	2015	Juegos en línea	"Los juegos en línea son aquellos a los que se puede acceder desde la web y a los cuales se puede jugar conectados a Internet. Puede tratase de juegos web tradicionales ejecutados en un navegador web y en los cuales

	no necesitas instalar nada extra o; de juegos multijugador o de rol, en los que se juega con otras personas conectadas (estos pueden requerir instalación de algún tipo de programa).” (segu-kids.org. (2015)).

Fuente: Propia

Una de las necesidades básicas del ser humano desde que nace es el juego, un bebé se empieza a entretener con sus manos, mirando y escuchando diferentes sonidos, conforme avanza en edad sus juegos van cambiando, así como la manera como interactúa en el juego. Existen diferentes tipos de juegos como los tradicionales, de mesa, deportivos, de azar, populares, los infantiles, los videojuegos entre otros, pero para cada uno de estos juegos se requiere la presencia física de los jugadores, siempre ha sido así.

Esta realidad ha empezado a cambiar en los últimos veinte años con la ayuda de la tecnología y la presencia de los juegos en línea, que no es más que muchos jugadores ingresen al mismo, independientemente del lugar en donde se encuentren, muchos de estos juegos requieren la formación de equipos para vencer a sus oponentes, es decir intervienen jugadores desconocidos con un objetivo común. Los jugadores no se ven, no se conocen, incluso entran con un alias al juego, pero persiguen el objetivo común, que es ganar e incluso dependiendo del juego, pueden comunicarse entre jugadores.

Una variación importante de los juegos en línea y que cada vez toma mayor fuerza en los adolescentes, son los juegos de azar en línea.

Un aspecto imprescindible para poder jugar es que, el usuario debe mantener una conexión activa a internet. Los juegos se vuelven cada vez más atractivos en cuanto a interfaces de usuario se refiere, conforme la tecnología avanza en el tiempo. Se habla hoy de imágenes en tres dimensiones y cierto tipo de juegos emula la realidad virtual, haciéndolo más atractivo para los jugadores, sobre todo, los jóvenes.

Figura 3. Interface referencial del juego Pacman (1980) y Pacman 3D (2005)

Según Ferrer (2019), las estrategias para atraer jugadores son múltiples y una de ellas es "el incentivo económico, presentado en forma de bonos gratuitos limitados o monedas virtuales para lograr mejoras en el juego que se obtiene a través de micro pagos", es decir, pagos poco representativos que pueden ir desde un dólar, si se considera la cantidad de jugadores que se pueden obtener alrededor del mundo, en realidad el negocio de los juegos es muy lucrativo.

(Pérez et al., 2018) en referencia al mismo tema dice: "Por otra parte, se incita a jugar presentando la actividad como una oportunidad de vivir experiencias agradables, entablar relaciones afines y demostrar destrezas. Se denomina cross-play a la opción de compartir con personas un rato de entretenimiento, junto a otros jugadores ubicados en lugares distintos y que no usan la misma marca de ordenador o consola"

Cierto tipo de juegos debidamente guiados pueden ser un aporte importante en la formación social, sin embargo, los riesgos que presentan para los adolescentes los juegos en línea y los juegos de azar son varios, pero el más importante es la adicción al juego. Normalmente una persona suele perder la noción del tiempo cuando está con algún tipo de dispositivo tecnológico, sobre todo los teléfonos celulares, el adolescente en los juegos en línea pierde totalmente la noción del tiempo y en un momento determinado esto puede generar ansiedad ,cuando no dispone de ningún tipo de conexión para el juego, se ha llegado a comprobar en diferentes estudios que, incluso pueden perturbar la personalidad de los adolescentes.

Se ha realizado la búsqueda en diferentes enlaces de investigación y no se ha encontrado estudios sobre la adicción a los juegos en este país, sin embargo, existen países donde hay investigaciones incluso a nivel gubernamental. En España, el Ministerio de Sanidad, Consumo y Bienestar Social (2017-2024) textualmente dice: "la conjunción de

la expansión tecnológica y la difusión de juegos mediante estrategias de marketing, cuyo público objetivo son personas jóvenes, ha propiciado un crecimiento en el número de individuos afectados por la adicción al juego, así como una modificación en el perfil de los sujetos afectados, principalmente en la modalidad online (menor edad, nivel educativo superior y un aumento de la cantidad de chicas que presentan conductas adictivas relacionadas con los juegos de apuesta)".

Otro riesgo importante se presenta cuando ciertos juegos en línea tienen la modalidad que se conoce como "freemium", lo que significa que se puede acceder libremente al mismo, sin embargo, existen ciertas fases o etapas del juego, para lo cual se requiere un pago, normalmente esto se lo hace con tarjeta de crédito. La mayoría de juegos, una vez que se hace un pago, guarda automáticamente los datos de la tarjeta de crédito, cuando el adolescente avanza en el juego, simplemente le hace la pregunta si quiere comprar una nueva arma o abrir un nuevo pasaje del juego, en el momento que el adolescente responde que sí, ya no se requiere de los datos de la tarjeta de crédito, la compra se hace automáticamente y al final llega el corte del pago a la tarjeta de crédito.

En resumen, no es una buena práctica realizar una compra con tarjeta para abrir una determinada fase de un juego, es preferible pagar una sola suscripción por un juego un determinado tiempo.

2.4.7 En el cyber

En la actualidad y debido a la gran penetración que ha tenido el internet en las diferentes zonas de la población mundial, sin que Ecuador sea una excepción, prácticamente los cyber han desaparecido, es importante analizar sin embargo, algunas definiciones para entrar en contexto con diferentes riesgos informáticos que se pueden encontrar en los pocos cyber que aún funcionan en diferentes lugares.

Tabla 14. Definición de Cybercafé

Autores	Año	Título	Definición
Castro Bravo, N. I.	2020	Creación de Cyber Café en el cantón Baba	"La expresión ciber es un prefijo tomado de la palabra cibernética. El ciber es un establecimiento que posee una concentración de tecnología avanzada, como, por ejemplo: computadores, internet, entre otros." (Castro Bravo, N. I.(2020)).
López-Bonilla, M. G.	2019	Los jóvenes en el cibercafé: entre la literacidad tradicional y las nuevas literacidades	"Los "cybercafés" hacen referencia a una variedad de espacios sociales cuyo objetivo principal es proveer acceso a computadoras y a internet." (López-Bonilla, M. G.(2019)).
Lachimba, E. M.	2016	Creación de un cyber café en el sector de Carcelén en la ciudad de Quito	"Un cybercafé' (de ciber- y café), cyber café o café Internet es un local público donde se ofrece a los clientes acceso a Internet y, aunque no en todos, también servicios de bar, restaurante o cafetería. Para ello, el local dispone de computadoras y usualmente cobra una tarifa fija por un período determinado para el uso de dichos equipos, incluido el acceso a Internet y a diversos programas, tales como procesadores de texto,

			programas de edición gráfica, copia de CD o DVD, etc." (Lachimba, E. M.(2016)).
Murolo, N. L.	2015	Jóvenes del conurbano bonaerense sur, tecnologías y usos del cyber	"Los cyberlocales son comercios donde se alquilan computadoras con conexión a Internet atendiendo a un fraccionamiento por tiempo de uso. Estos espacios privados, de acceso público, proliferaron a finales de los años noventa y comienzos de los 2000 a la luz de la masificación de Internet para usos cada vez más comunes." (Murolo, N. L. (2015)).
segu-kids.org	2015	En el Cyber	"Un Cyber, Cybercafé o cybercentro es un local público en el cual se disponen de computadoras con o sin juegos, con la capacidad de navegación por Internet y otras aplicaciones. La persona que asiste al mismo paga una tarifa por un determinado tiempo de uso de una computadora u otro dispositivo." (segu-kids.org (2015)).

Fuente: Propia

El cyber o cyber café es un lugar donde existen un conjunto de computadores interconectados en red y que tienen acceso a internet, donde una persona puede acudir para alquilar un equipo y desarrollar diferentes actividades en línea o fuera de línea. En la actualidad, es cada vez más difícil encontrar este tipo de lugares, porque el acceso a

internet a través de los teléfonos celulares se ha popularizado en una cantidad cada vez mayor de población, lo que ha contribuido para que muchos locales que prestaban este servicio, se cierren definitivamente.

Las actividades que se pueden desarrollar en estos lugares son diversas, por ejemplo, se puede jugar en línea, navegar en internet y todas sus posibilidades, pero también se pueden hacer actividades sin el uso de internet, por ejemplo usar software ofimático, hacer videollamadas entre otras actividades que se pueden realizar.

A pesar de que, como se ha mencionado, cada vez quedan menos cyber, existen riesgos en este tipo de locales y el principal es que, los computadores son de uso público, es decir cualquier persona puede haber usado antes que cualquiera el computador y el riesgo principal de utilizar este tipo de lugares es que, pueden tener instalados ciertas aplicaciones para leer usuarios y contraseñas y de esta manera pueden obtener datos a los correos, plataformas sociales e incluso en ciertos casos, acceso a cuentas bancarias.

Otro riesgo importantes es que si se ingresa a dispositivos electrónicos personales en equipos públicos, estos pueden contaminarse con virus informáticos o de otro tipo de software malicioso, lo que produciría la propagación de programas no deseados en los computadores personales.

2.4.8 Phishing

Este riesgo no afecta de manera significativa a los adolescentes, porque el fin de esta técnica sobre todo, es obtener beneficios económicos, sin embargo, es importante conocerla por la afectación que puede tener este tipo de delito en la vida de las personas.

Tabla 15.-Definición de Phishing

Autores	**Año**	**Título**	**Definición**
Bastidas Jácome, C. D., & Paredes Sevillano, F. E.	2022	Prototipo de un sistema anti-phishing basado en herramientas open source o de bajo costo	“El phishing es un tipo de ingeniería social que busca realizar la suplantación de la identidad de un lugar, empresa o persona; con la finalidad de robar información confidencial,

		para la Empresa Intercommerce SA	sobre todo las credenciales de acceso para la cuenta en la entidad real. A pesar de que existen muchas variantes en los ataques de tipo phishing, todos buscan obtener datos valiosos de forma fraudulenta a través de la suplantación de identidad.” (Bastidas Jácome, C. D., & Paredes Sevillano, F. E.(2022)).
Guaña-Moya, J., Chiluisa-Chiluisa, M. A., del Carmen Jaramillo-Flores, P., Naranjo-Villota, D., Mora-Zambrano, E. R., & Larrea-Torres, L. G	2022	Ataques de phishing y cómo prevenirlos	“El phishing es un tipo de ataque de ciberseguridad por medio del cual los expertos informáticos (phisher), de manera malintencionada, envían mensajes haciéndose pasar por una persona o entidad de confianza, con la finalidad de manipular a los usuarios, propiciando que realice acciones como instalar un archivo malicioso, hacer clic en un enlace falso o divulgar información confidencial como credenciales de acceso.” (Guaña-Moya, J., Chiluisa-Chiluisa, M. A., del Carmen Jaramillo-Flores, P., Naranjo-Villota, D., Mora-Zambrano, E. R., & Larrea-Torres, L. G (2022)).

Barroso Beltri, V.	2021	Análisis y Simulación de un Ataque de Phishing	"El Phishing, llamado así por una comparación con la pesca (fishing en inglés), es también llamado, en ocasiones, Brand Spoofing (Suplantación de Identidad de una marca). Se distribuye generalmente mediante correos de Spam y es, además, considerado fraude y falsificación en gran cantidad de países. Es el acto de enviar correos falsificados a un usuario, imitando un servicio legítimo, en un intento de estafar al destinatario para difundir información privada como la de una tarjeta de crédito o las credenciales de un servicio." (Barroso Beltri, V. (2022)).
Barreiro Herrera, D. A.	2020	Detección de phishing en etapa de detección temprana utilizando características relacionadas a la marca afectada	"Se demomina pishing a un conjunto de técnicas utilizadas en el campo de la ingeniería social que busca persuadir a las personas a entregar información sensible o ingresar a su sistema, cabe mencionar que aunque en la bibliografía se relaciona mucho al pishing a correos electrónicos, esta no es la única manera de dispersar URLs maliciosas, redes sociales, mensajes de texto, suplantación

			de identidad y anuncios son algunos de los mecanismos mayormente conocidos objeto de estudio en la literatura.” (Barreiro Herrera, D. A. (2020)).
Lizarraga, J. R. P., Hernández, J. A. L., Garay, M. A. B., Navarro, A. F., & Espinoza, D. E. F.	2019	Protocolo para la prevención de ataques de phishing	“Es un tipo de malware o un término para que alguien envía un correo electrónico falsificado a las víctimas al azar para tratar de obtener información personal sobre ellos. Más específicamente en la informática, el phishing es una actividad criminal utilizando técnicas de ingeniería social para adquirir fraudulentamente información sensible como nombres de usuario y contraseñas, tratando de engañar a los usuarios de sitios web populares enviándolos por correo electrónico versiones falsas de la web para dar a sus credenciales.” (Lizarraga, J. R. P., Hernández, J. A. L., Garay, M. A. B., Navarro, A. F., & Espinoza, D. E. F. (2019)).
Valle Matute, J. C.	2013	El delito informático de Phishing	“El phishing es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario,

	contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.” (Valle Matute, J. C. (2013)).

Fuente: Propia

Por definición, el phishing es una técnica de tipo electrónico que busca adueñarse de información ajena, con el fin de obtener datos personales y en última instancia, un rédito económico

Lira Oscar (2019) afirma que “el Phishing es una acción de engaño por medio de páginas electrónicas y el uso de enlaces electrónicos, integrado a un correo electrónico o mensajería instantánea, de la cual busca obtener datos personales o financieros” (p. 66), es decir, se busca obtener información sensible sea de carácter personal o en el caso de empresas, de carácter jurídico con el objeto de poder llevar a cabo el delito informático.

Las técnicas para obtener este tipo de información sensible e importante son múltiples, a continuación se detallan las más utilizadas:

- Spear phishing, saber a qué organización o persona se va a realizar el ataque, se hace una investigación previa para mejorar las posibilidades de éxito y que la organización o el usuario caiga en la trampa.
- Correo electrónico o correo spam, consiste en enviar correos con el nombre de algún tipo de institución y se le solicita llenar algún formulario, para obtener información de carácter personal. Por ejemplo, un correo del tipo funcion_judicial@gmail.com y le advierten que la persona ha sido denunciada por el cometimiento de un delito, le solicitan llenar el formulario con el fin de enviar los avisos judiciales para continuar con el trámite, dado el poco conocimiento informático que tienen las personas, suelen asustarse y llenar dicho formulario, el primer error es no conocer las extensiones de los correos de carácter gubernamental, que aquí en el Ecuador deberán tener la extensión final gov.ec.

Figura 4. Imagen de un correo real con la técnica de pishing.

- Entrega basada en la web, técnica más sofisticada de todas y consiste en emular una página web de una determinada institución con un pequeño cambio imperceptible para el usuario, este cree que está en la página de la institución y empieza a ingresar los datos, y en realidad lo que ocurre es que se encuentra transmitiendo los datos para que luego sean utilizados en una estafa.

Otras técnicas de phishing son secuestro de sesión, troyanos, software malicioso, Smishing. (suplantación de identidad por SMS), vishing, inyección de contenidos, manipulación de enlaces, y otras.

Masaquiza (2021) dice: “El phishing actúa basado en ingeniería social, es un acto delictivo que no tortura, no presiona, no obliga; lo que en realidad hace es generar una especie de estado mental de preocupación o anímico” p(19).

2.4.9 En el internet

A través del aparecimiento de la red de redes se han creado una gran cantidad de aplicaciones para diferentes usos, es el aparecimiento del internet lo que ha multiplicado los riesgos informáticos, por lo cual, es conveniente analizar las definiciones de algunos autores:

Tabla 16. Definición de internet

Autores	Año	Título	Definición
Asensio, P. A	2022	Derecho privado en el internet	"Internet es un elemento clave de la llamada sociedad de la información pues facilita los más variados servicios electrónicos interactivos y la comunicación de todo tipo de sistemas de informaciones (texto, sonidos, imágenes y video…). En el plano técnico internet constituye un entramado mundial de redes conectadas entre si de un modo que hace posible la comunicación instantánea o casi instantánea desde cualquier dispositivo conectado a una de esas redes con otros situadas en otras redes del conjunto, por lo que se trata de un medio de comunicación global." (Asensio, P. A (2022)).
Marulanda J.	2022	Fundamentación del derecho al acceso a internet: tratamiento desde la libertad de expresión en el ordenamiento jurídico colombiano	"Internet es la unión de todas las redes y computadoras distribuidas por todo el mundo, por lo que se podría definir como una red global en la que se conjuntan todas las redes que utilizan protocolos TCP/IP y que son compatibles entre sí.". (Marulanda J. (2022))

Real Academia de la Lengua	2022	Diccionario de la lengua española	"Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación" (Real Academia de la Lengua (2022)).
Salinas, M. G. T	2019	Internet como servicio público.	"Es un nuevo espacio de comunicación que permite la interacción de los seres humanos a través de computadoras principalmente. Sin dejar de tener presente que también permite la comunicación entre otros accesorios tecnológicos." (Salinas, M. G. T (2019)).
Villota García, S. C., Zamora López, G. G., & Llanga Vargas, E. F.	2019	Uso del internet como base para el aprendizaje.	Los autores citando a Castells mencionan que "el internet se puede definir como un grupo de redes de ordenadores que se encuentran interconectadas, pero su funcionamiento no se adapta a un solo tipo de ordenador tratando de un sistema dinámico y flexible, que puede ser adaptado a distintos contextos. Estas redes son por sí universo de la tecnología, en donde convergen diversas ramas como la telefonía, microprocesadores, fibra óptica, satélites, electrónica, video, televisión,

	imágenes, realidad virtual, hipertexto.” (Villota García, S. C., Zamora López, G. G., & Llanga Vargas, E. F. (2019)).

Fuente: Propia

El internet como se ha explicado, es la red de redes sobre la cual funcionan una serie de aplicaciones, sin embargo, la sola navegación trae consigo el exponerse a ciertos riesgos digitales.

El internet en la actualidad es un conjunto de textos, imágenes, videos, sonidos, animaciones, sobre la cual una persona puede navegar en constante búsqueda de información sobre cualquier tema, se puede acceder a los diferentes documentos a través de los que se conoce como hipervínculos y al software que permite acceder al internet para visualizar los documentos se le conoce como browser en inglés o navegador en español. Pese a que el buscador de información más conocido y utilizado en todo el mundo es Google, existen al menos otra decena de buscadores como son Bing, DuckDuckGo, Archive.org, StartPage, Gibiru, Qwant, Yahoo Search, Ask.com, solo para mencionar algunos buscadores.

El internet es una excelente herramienta que les permite a los niños y adolescentes navegar y buscar información útil para su educación o para sus pasatiempos preferidos, sin embargo, el realizar la búsqueda sin criterio, puede llevar a ciertos resultados equivocados, se debe considerar además que, la mayoría de niños y adolescentes pueden navegar libremente y sin ningún control a través del internet.

Existen varios riesgos para los jóvenes al navegar en búsqueda de información por el internet, pero el principal es, el acceder a información equivocada o no deseada. El dar un clic en un enlace no adecuado, puede llevar a acceder a material pornográfico, a páginas de violencia, drogas, juegos en línea o a contactar con personas no deseadas. Otro riesgo importante es el tiempo en el cual puede pasar una persona navegando en el internet en actividades de ocio o poco productivas, lo cual también va a generar adicciones. Una de las formas en las cuales se puede acceder a lugares no deseados o a información

incorrecta es incluso, a través de páginas de información adecuada que, sin embargo, presentan propaganda no debida y que permite acceder a otro tipo de información.

En resumen, Melamud A, Otero P, Nasanovsky J, Stechina D, Goldfarb G, Svetliza J. (1999) dicen: "En la última década, niños y adolescentes han aprendido hábilmente el manejo de las computadoras; sin embargo, aunque pueden ser usuarios experimentados, ignoran y pueden manejar incorrectamente los peligros que su uso implica. Algunos autores consideran que este riesgo es comparable a una "nueva epidemia del siglo XXI".

Figura 5. Captura de pantalla Diario el Comercio. Fecha 06 - abril - 2023

Como se puede observar en la Ilustración 5, pese a que se busca información en un diario de circulación nacional como El Comercio y es una página con certificación de seguridad de tipo https, en esta página y a manera de propaganda se puede acceder a una página de apuestas deportivas, por este motivo, se debe tener especial cuidado cuando los niños y adolescentes navegan en internet, puesto que pueden llevar a enlaces no deseados.

2.4.10 En redes P2P

Las redes P2P son un tipo especial de redes que los adolescentes ocupan para compartir información, son redes donde sus dispositivos no manejan ningún tipo de prioridad, es decir, no existe una estructura cliente servidor, antes de analizar los riesgos informáticos que se pueden producir en este tipo de redes, se revisará las definiciones de algunos autores:

Tabla 17. Definición de redes P2P

Autores	Año	Título	Definición

López Pérez, E	2022	Redes P2P y ciberdelincuencia	"Una red P2P, cuyas siglas significa red de pares o red entre iguales en inglés, es una red en la que los nodos cumplen la función de servidores y de clientes al mismo tiempo, sin que exista ningún tipo de jerarquía al respecto. Así, en una red de estas características cada ordenador o dispositivo estaría en un plano de igualdad con los demás, provocando la existencia de una comunicación de tipo horizontal." (López Pérez, E (2022)).
Ospina, M.	2022	Sistemas distribuidos, escalabilidad y distribución de los datos.	"La arquitectura P2P es como si uniéramos al cliente y al servidor en una sola aplicación, facilitando la conexión a otras computadoras de la red para consumir los recursos expuestos por los otros nodos de la red. Pero al mismo tiempo, esta arquitectura funciona como un servidor, lo que permite que otros nodos se conecten a nuestro software para leer los recursos que nosotros exponemos." (Ospina, M. (2022)).
Cano Vázquez, P.	2020	Aplicación P2P de comunicación y organización de	"Son redes de ordenadores que se comportan como iguales entre sí. Los distintos elementos que

		grupos con compartición de ficheros.	participan en la red se denominan Nodos. Los nodos interactúan entre sí de tal forma que unas veces actúan como servidores de información y otras como clientes que solicitan información. De esta forma, la responsabilidad de almacenamiento y administración de la información se reparte entre todos los nodos que forman parte de ella. Las redes P2P se encuentran superpuestas a una red pública (por ejemplo, Internet) y un nodo puede comunicarse con cualquier otro nodo de la red, para intercambiar información en cualquier formato." (Cano Vázquez, P. (2020)).
Cantos Agudo, J. C.	2020	Red P2P centralizada para el streaming de vídeo almacenado	"Las redes P2P se basan entre la conexión directa entre clientes o nodos, aprovechando sus capacidades, quitando trabajo al servidor y evitando problemas de escalabilidad" (Cantos Agudo, J. C. (2020)).
Castaño Duque, M. R.	2020	Impacto del esquema del mercado P2P en el mercado eléctrico colombiano.	"Las redes P2P son una tecnología disruptiva para aplicaciones distribuidas a gran escala que ha ganado un gran interés últimamente debido al

	éxito que ha tenido el intercambio de contenido P2P, la transmisión de medios y las aplicaciones de telefonía. Las arquitecturas subyacentes comparten características como la descentralización, el intercambio de recursos del sistema final, la autonomía, la virtualización y la auto organización.” (Castaño Duque, M. R. (2020)).

Fuente: Propia

Las redes P2P es un tipo de conexión que permite a dos usuarios conectarse entre sí con el objeto de compartir información. Es decir, es una conexión entre iguales donde ninguno es cliente y ninguno es servidor.

Las redes P2P desde sus orígenes han trabajado en el límite de lo legal y lo ilegal, porque, por ejemplo un familiar puede ir de vacaciones algún lugar y realizar filmaciones de las diferentes actividades que realicen durante su estancia en ese sitio y luego a través de los aplicativos P2P compartir la grabación final con sus familiares en diferentes lugares del mundo, lo cual es claramente legal; sin embargo, en la parte oscura del uso de este tipo de redes está el compartir información protegidas con alguno de los diferentes tipos de licencia intelectual, lo cual es ilegal. Algunos aplicativos han sido demandados por este tipo de prácticas.

En la actualidad los aplicativos P2P más utilizados eMule, Soulseek o BitTorrent, entre los adolescentes; el término P2P es muy popular, así como las diferentes aplicaciones que se utiliza para aprovechar las ventajas de este tipo de red.

El principal riesgo que se corre cuando se trabaja con estas redes es el bajar información no deseada o no comprobada, es decir lo que se conoce como fake, que es un término donde se indica por ejemplo, que se va bajar información sobre la fauna de Galápagos, pero al momento de revisar la información, resulta ser una broma jocosa, en

este caso solamente se trató de una pérdida de tiempo, pero existen riesgos graves, por ejemplo que el video ya no sea una broma sino material pornográfico con menores de edad, en este caso, además del tipo de contenido no permitido para adolescentes se puede incurrir en temas de tipo legal, al difundir información no permitida.

Otro riesgo importante en este tipo de redes es, bajar información con software malicioso o malware que van a dañar el computador personal, se debe considerar, además, que el antivirus no necesariamente puede rastrear a todo tipo de software malicioso.

López (2021) citando a Catá del Palacio (2014) dice: "la red oscura P2P más utilizada se llama Freenet. Es totalmente anónima y distribuida, diseñada como un almacén de datos distribuidos por lo que se han construido sobre ella un gran número de programas y aplicaciones que permiten la publicación de una página web desde el anonimato, por ejemplo. Es prácticamente imposible e inviable eliminar un contenido, puesto que, la información como se ha especificado antes, está distribuida, lo cual es un verdadero problema cuando se tratan de archivos delictivos, como puede ser la pornografía infantil, que nunca dejará de estar accesible en esta red. Sin embargo, se trata de una gran herramienta cuando se quiere evitar la censura"

2.4.11 Otros tipos de riesgos

Se han detallado los principales riesgos digitales a los que están expuestos los adolescentes, sin embargo, existen otro tipo de riesgos que se debe tener en cuenta que, aunque no les afecta de manera directa, puede llegarles a suceder en algún momento. Se detallan a continuación algunos riesgos adicionales con una breve descripción:

- Robo de identidad.- este es un riesgo digital en donde se busca a través de ingeniería social u otro tipo de software adueñarse de los datos personales con el objeto de realizar transacciones financieras.
- Pedofilia.- se ha expuesto mucho que uno de los riesgos a los cuales se encuentran expuestos los adolescentes es el acceso a hipervínculos de información no deseada como es el caso de la pornografía, la pedofilia es una variación de la pornografía en el sentido de que estimula a menores de edad a participar en fotos, videos de carácter sexual. El acceso a la tecnología puede permitir a un adulto de forma

anónima ganarse la confianza de un menor de edad y lograr este tipo de cometido indebido e ilegal.

- Spam.- se lo define como un mensaje que no se ha solicitado y que ha sido enviado de manera masiva por correo electrónico generalmente con fines publicitarios y el riesgo principal es recibir información no deseada y en algún momento si no existe una adecuada gestión de correo electrónico que este colapse por llegar al límite de espacio disponible.

2.5 Marco Legal

Declaración Universal de los Derechos Humanos La educación es registrada como derecho en la Declaración Universal de los Derechos Humanos (1948) la cual instituye en su artículo 26:

1. Toda persona tiene derecho a la educación. La educación debe ser gratuita, en todos los niveles de educación. La instrucción elemental será obligatoria. La instrucción técnica y profesional habrá de ser generalizada; el acceso a los estudios superiores será igual para todos, en función de los méritos respectivos.

2. La educación tendrá por objeto el pleno desarrollo de la personalidad humana y el fortalecimiento del respeto a los derechos humanos y a las libertades fundamentales; favorecerá la comprensión, la tolerancia y la amistad entre todas las naciones y todos los grupos étnicos o religiosos, y promoverá el desarrollo de las actividades de las Naciones Unidas para el mantenimiento de la paz.

3. Los padres tendrán derecho preferente a escoger el tipo de educación que habrá de darse a sus hijos (Declaración Universal de los Derechos Humanos, 1948, p.6).

Objetivo No. 4 de desarrollo Sustentable de la ONU.- Garantizar una educación inclusiva, equitativa y de calidad y promover oportunidades de aprendizaje durante toda la vida para todos

Ya en el ámbito interno también se habla de la educación como un derecho esencial del ser humano y está garantizado en la Constitución del Ecuador elaborada en Montecristi en el año 2008 y en su artículo 3, título 1, dice:

Art. 3.-Son deberes primordiales del Estado:

1. Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales, en particular la educación, la salud, la alimentación, la seguridad social y el agua para sus habitantes.

De manera adicional en los artículos 26 y 27 en cuanto se refiere a Educación se detalla lo siguiente:

Art. 26.- La educación es un derecho de las personas a lo largo de su vida y un deber ineludible e inexcusable del Estado. Constituye un área prioritaria de la política pública y de la inversión estatal, garantía de la igualdad e inclusión social y condición indispensable para el buen vivir. Las personas, las familias y la sociedad tienen el derecho y la responsabilidad de participar en el proceso educativo.

Art. 27.-La educación se centrará en el ser humano y garantizará su desarrollo holístico, en el marco del respeto a los derechos humanos, al medio ambiente sustentable y a la democracia; será participativa, obligatoria, intercultural, democrática, incluyente y diversa, de calidad y calidez; impulsará la equidad de género, la justicia, la solidaridad y la paz; estimulará el sentido crítico, el arte y la cultura física, la iniciativa individual y comunitaria, y el desarrollo de competencias y capacidades para crear y trabajar.

La educación es indispensable para el conocimiento, el ejercicio de los derechos y la construcción de un país soberano, y constituye un eje estratégico para el desarrollo nacional.

En la misma constitución en mención y en cuanto a tecnología se refiere en el Artículo 16, Inciso 2 textualmente dice:

Artículo 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

2. El acceso universal a las tecnologías de información y comunicación.

En referencia al mismo tema en el artículo 298 en la parte concerniente se menciona:

Art. 298.- Se establecen pre asignaciones presupuestarias destinadas a los gobiernos autónomos descentralizados, al sector salud, al sector educación, a la educación superior; y a la investigación, ciencia, tecnología e innovación en los términos previstos en la ley. Las transferencias correspondientes a pre asignaciones serán predecibles y automáticas.

En el artículo 347 en el inciso 8 se menciona:

Art. 347.- Sera responsabilidad del estado

8. Incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales.

Como se puede analizar según los artículos citados tanto la educación como el acceso a las tecnologías de la información y comunicación se encuentran garantizada en la constitución de la República del Ecuador, incluso en el Artículo 347 se habla de incorporar las tecnologías de la información y comunicación en el proceso educativo, pero con esta incorporación viene un aspecto que no es tratado en la constitución como son los riesgos en el uso de la tecnología en general y en el proceso de enseñanza aprendizaje en particular.

En el Ecuador no existe una normativa puntual en cuanto a seguridad informática se refiere, es decir que cubran los aspectos de ciberseguridad, ciberinteligencia y ciberdefensa, sin embargo se han emitido disposiciones jurídicas que permiten de alguna manera cubrir los aspectos mencionados y la entidad encargada de hacerlo es el Ministerio de Telecomunicaciones y de Sociedad de la Información.

El Acuerdo Ministerial No. 020 – 2019 de fecha 2 de septiembre del 2019 en la parte pertinente textualmente dice:

“Que, con informe técnico del 2 de septiembre de 2019, aprobado por el Subsecretario de Estado – Gobierno Electrónico se recomienda: “Expedir mediante Acuerdo Ministerial la política de seguridad de la información debido a la necesidad de gestionar de manera coordinada la seguridad de la información en las entidades del Ejecutivo, ya que cada vez surgen nuevas amenazas y se revelan vulnerabilidades e incidentes de seguridad que tienen efectos considerables en la sociedad”” acuerda

Art. 1.- Expedir la política de seguridad de la información para implementar medidas preventivas y reactivas que permitan resguardar y proteger la información que reposa en las entidades de la administración pública central, institucional y que dependen de la función Ejecutiva.

El Acuerdo Ministerial 006 – 2021 de fecha 27 de Abril del 2021 en la parte pertinente nos indica:

“Que, la Política Ecuador Digital está compuesto por tres programas: Ecuador conectado, Ecuador eficiente y ciberseguro; y, Ecuador innovador y competitivo. El programa Ecuador eficiente y ciberseguro tiene como objetivo proteger a la sociedad frente a las amenazas cibernéticas, generar confianza en el uso del internet y fomentar el desarrollo económico y social basado en el uso de las Tecnologías de la Información y de la Comunicación (TIC)” Acuerda

Art. 1.- Publicar la Política de Ciberseguridad, que se encuentra anexa y que forma parte integral del presente Acuerdo Ministerial.

Finalmente el 21 de mayo del 2021 en el Registro Oficial No. 469 se publicó la “Ley orgánica de datos personales”, cuya finalidad es garantizar el ejercicio del derecho a la protección de datos personales.

CAPITULO III
Marco Metodológico

3.1 Descripción del área de estudio / Grupo de estudio

El colegio universitario UTN es el lugar donde se desarrollará esta investigación se encuentra ubicada en la ciudad de Ibarra, cantón Ibarra, parroquia el Sagrario, provincia de Imbabura, en la calle Ulpiano de la Torre 2-30 y calle Jesús Yerovi, su oferta educativa incluye educación básica superior y bachillerato general unificado.

Para el desarrollo de la investigación se considerará a los alumnos de tercero de bachillerato general unificado y la misma se la realizará en coordinación con el responsable del área de TIC.

Como un aporte adicional la aplicación interactiva en línea estará disponible en cualquier momento para alumnos, padres de familia y docentes que deseen conocer y aprender de manera lúdica sobre los riesgos informáticos.

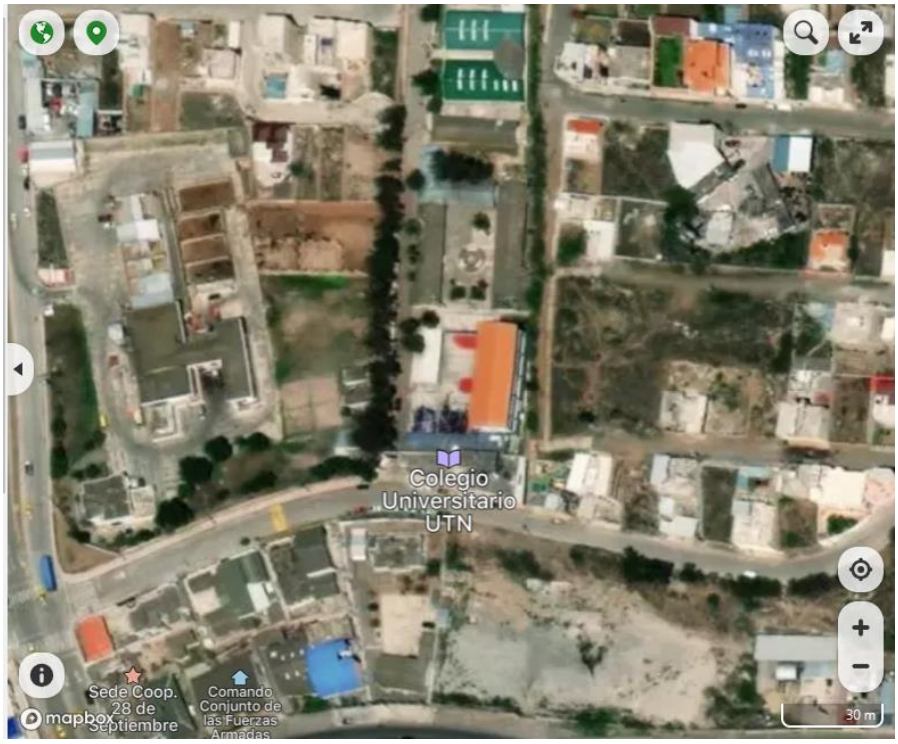

Figura 6. Ubicación del colegio Universitario UTN

El 29 de noviembre de 1988 el Ministerio de Educación expide el Acuerdo Ministerial Nro. 278 que en el Art. 1 señala: “Autorizar el funcionamiento del colegio de

ciclo básico “Sin Nombre” anexo a la Facultad de Ciencias de la Educación de la Universidad Técnica del Norte, en la ciudad de Ibarra provincia de Imbabura, a partir del año lectivo 1988 – 1989 destinado a la práctica docente”, como colegio Anexo a la Universidad Técnica del Norte. Las primeras labores académicas iniciaron en el mes de agosto de 1989 con 45 estudiantes y 3 docentes.

El Honorable Consejo Universitario en el año 1.992 resuelve designarle al Colegio con el nombre de “Milton Reyes”, así permaneció hasta que el 11 de agosto de 2003, fecha en la que se cambia el nombre de Colegio Anexo “Milton Reyes” a Colegio Universitario UTN.

El 3 de septiembre de 2015 la Coordinación Zonal de Educación, autoriza el permiso de funcionamiento al Colegio de Bachillerato Universitario UTN, con oferta educativa de Educación General Básica y Bachillerato General Unificado en Ciencias, con sostenimiento particular, teniendo como promotora a la Universidad Técnica del Norte.

Con fecha 3 de agosto de 2022, la Coordinación Zonal de Educación mediante Resolución Nro. MINEDUC – CZ1-2022-00353-R resuelve renovar la autorización de funcionamiento del Colegio de Bachillerato Universitario UTN, a partir del año 2022 – 2023.

El Colegio Universitario UTN en la actualidad cuenta con 596 estudiantes repartidos entre educación general básica y bachillerato general unificado.

3.2 Enfoque y tipo de la investigación

El tipo de enfoque que tiene la investigación es cualitativo, porque se sustentará en el marco teórico para desarrollar la plataforma en línea. El marco teórico se obtendrá de diferentes fuentes documentales como son libros, base de datos, artículos científicos, y demás documentación que nos permita desarrollar un sustento adecuado para el desarrollo de la aplicación interactiva.

Una vez que la plataforma informática se encuentre desarrollada será propositiva porque permitirá aplicar de forma práctica los conocimientos teóricos a través de los diferentes tipos de material didáctico implementado.

Como una observación adicional para llegar a la construcción de la herramienta en línea pasará por otro tipo de investigación como es la documental y la de campo.

3.3 Definición de variables de investigación

Las variables que se determinan para el desarrollo de esta investigación denominada diseño de estrategias didácticas para la prevención de riesgos tecnológicos relacionados a la seguridad informática dirigido a estudiantes de tercero de bachillerato se detallan en la siguiente tabla:

Tabla 18. Definición de variables de investigación

Variable Dependiente	Estrategias de seguridad informática para los actores del proceso de enseñanza aprendizaje
Variable Independiente	Plataforma interactiva en línea Competencias digitales Conocimientos sobre navegación en internet.

Variable	**Indicador**	**Instrumento**	**Fuente**
Plataforma interactiva en línea	Recursos tecnológicos Estrategias didácticas Infraestructura TICs	Encuesta Entrevista	Alumnos Docente TICs
Competencias digitales	Recursos digitales Conocimiento TICS Estrategias interactivas	Encuesta	Alumnos
Conocimientos sobre navegación en internet	Conocimiento básicos de TICS	Encuesta	Alumnos

3.4 Método de investigación

Los métodos de investigación utilizados para el desarrollo del presente trabajo en lo que se refiere al análisis, síntesis y recopilación de la información son:

3.4.1 Método analítico

En la presente investigación se utilizó este método pues en el área de la seguridad informática se desarrollan los riesgos digitales a los que se encuentran expuestos los adolescentes, en base a una explicación detallada de cada uno de ellos y ejemplos para cada de los riesgos mencionados en el presente trabajo. Esto se lo realiza en base a una investigación en diferentes tipos de fuentes como son bases de datos documentales, artículos científicos, libros y otro tipo de estudios de diferentes tipos de organizaciones sobre el tema de estudio.

Además como parte de este método se determinó la metodología con la que se llevará a cabo la plataforma interactiva en línea, la misma que se encuentra como anexo al presente documento.

3.4.2 Método sintético

Este método se utiliza de forma ligada al método analítico, y como resultado de este proceso se determinan estrategias para cada uno de los actores del proceso de enseñanza aprendizaje; maestros, estudiantes, autoridades y padres de familia, además se realiza la implementación de una plataforma en línea que nos permite aprender sobre el tema con diferentes tipos de estrategias didácticas.

3.5 Técnicas de investigación

Las técnicas de investigación para la obtención de los datos e información aplicados al proceso de investigación de diseño de estrategias didácticas para la prevención de riesgos tecnológicos relacionados a la seguridad informática se detallan a continuación.

3.5.1 Encuesta

La encuesta permitió la recolección de la información sobre el grupo objetivo para para determinar el nivel de conocimiento de los alumnos sobre la seguridad informática y los riesgos digitales a los cuales están expuestos.

Después de una breve capacitación sobre el manejo de la plataforma en línea y después de que los alumnos hayan realizados las diferentes actividades de la misma se

procede a realizar una nueva encuesta vía formulario a través de la misma plataforma para poder realizar un estudio comparativo.

3.5.2 Entrevista

Está técnica se utilizó para entrevistar al docente de TI, para conocer la infraestructura tecnológica de la unidad educativa tanto a nivel de hardware como de software, su infraestructura de red, políticas de uso de equipos y otro tipo de información respecto a los aspectos tecnológicos.

3.5.3 Plataforma en línea

Además de los estudiantes trabajar en la plataforma para aprender sobre los riesgos digitales a los que se encuentran expuestos, en la misma se aplicó una encuesta posterior al uso de la plataforma para verificar los conocimientos adquiridos y poder realizar un análisis de como evolucionaron los conocimientos.

En resumen los instrumentos de investigación que se utilizaron para la obtención de la información fueron:

- Cuestionario de encuesta.
- Cuestionario de entrevista.

3.6 Proceso de la investigación

El proceso utilizado en el desarrollo de trabajo de investigación para diseñar estrategias didácticas para la prevención de riesgos tecnológicos relacionados a la seguridad informática dirigido a estudiantes de tercero de bachillerato, fue a través de tres fases que se detallan a continuación:

Fase 1.- Recopilar bases teóricas y conceptuales de la problemática de la seguridad informática con especial énfasis en la educación.

En base a diferentes fuentes de información de bases de datos documentales, artículos científicos, tesis, libros y otras fuentes de información bibliográfica se levantará un marco teórico adecuado sobre la temática de la seguridad informática y los principales riesgos a los que se encuentran expuestos los alumnos, profesores y padres de familia.

Fase 2.- Desarrollar estrategias didácticas en una plataforma tecnológica interactivasobre seguridad informática dirigido a estudiantes de tercero de bachillerato

Con la información recabada en la fase 1 se definirá los elementos didácticos a desarrollarse en la plataforma y el temario a implementar en la misma, en base a esto se hará un diseño de la plataforma y su respectiva construcción para su implementación final Dentro de esto se obtendrá un dominio web, y se montará dentro de un servidor para que la aplicación se encuentre en línea con una disponibilidad de 99.6 %.

En esta fase se escoge la herramienta de software que nos ayudará a desarrollar la plataforma interactiva en línea, un aspecto importante a considerarse en este punto el tipo de licenciamiento de la herramienta a utilizar, se debe considerar además que tipo de material didáctico se puede utilizar y si se pueden realizar vía programación cambios que nos ayuden a personalizar la plataforma. La plataforma interactiva tiene que ser con una interfaz amigable e intuitiva sin embargo en el grupo de investigación se realizará una capacitación para el manejo adecuado de la mima con el fin de mejorar los resultados de la investigación.

Fase 3.- Evaluar el impacto de la implementación de la estrategia didáctica.

Para evaluar la plataforma tecnológica sobres los riesgos informáticos en la educación se sostendrá en la metodología de aprender haciendo, resultando útil para los estudiantes del Tercer año de Bachillerato y para todos los actores del proceso de enseñanza aprendizaje que tengan interés en el tema. La lectura, la escritura y la participación interactiva dentro de la plataforma a través de diferente tipo de material didáctico.

Al ser una plataforma en línea estará disponible para todos los actores del proceso de enseñanza aprendizaje que deseen aprender sobre el tema.

Consecuentemente estos procesos de intercambio de conocimientos y experiencias permitirán a los alumnos participar activamente de un aprendizaje colaborativo.

CAPITULO IV
Resultados y discusión

En este capítulo se analizan los resultados de las encuestas aplicadas a los estudiantes. El proceso fue el siguiente, se realiza una primera evaluación a los estudiantes para ver el conocimiento que tienen los mismos sobre la seguridad informática y los riesgos digitales. De manera posterior se les explica el funcionamiento de la plataforma interactiva y los diferentes materiales didácticos de la misma, se les permite trabajar en el software y se aplica una post encuesta.

En el presente capítulo cuando se indique que se realizó la post evaluación se debe entender que el estudiante ya trabajó en la plataforma en línea y en las diferentes opciones que brinda la misma y después de conocer más sobre la seguridad informática y los riesgos digitales se procedió a llenar la encuesta.

La encuesta se aplicó sobre un total de 95 estudiantes pertenecientes al colegio universitario UTN, de tercero de bachillerato, de los cuales existe un total de 35 hombres correspondiente al 36,8 por ciento del total de encuestado y 60 mujeres que corresponde 60,20 por ciento y los estudiantes tienen una edad de entre 17 y 18 años aproximadamente. En la encuesta se explicó claramente el objetivo del estudio y se garantizó la absoluta reserva de los estudiantes, en ningún momento se pidió llenar el nombre o paralelo al que pertenecen.

En base a esta explicación a continuación se detallan los resultados obtenidos.

4.1 Pregunta No. 1. Seguridad informática

La definición de “Es un conjunto de buenas prácticas que se deben seguir en el uso de los diferentes recursos tecnológicos para que los adolescentes no se encuentren expuestos a una serie de riesgos informáticos” corresponde a:

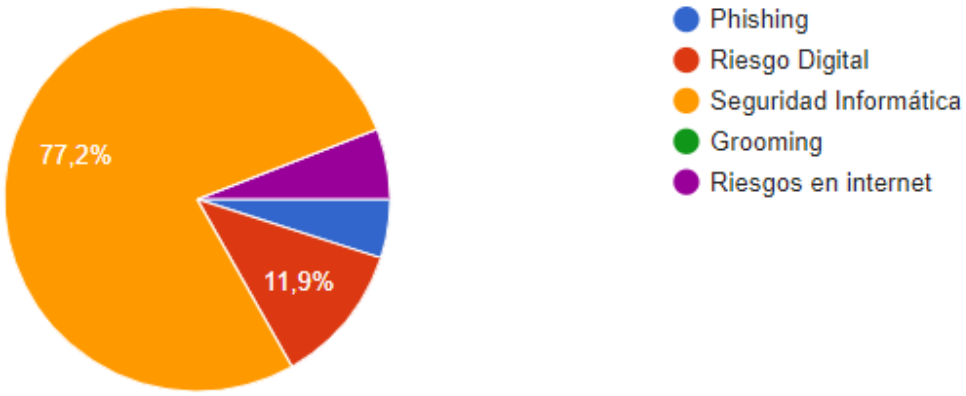

Figura 7. Encuesta. Seguridad informática

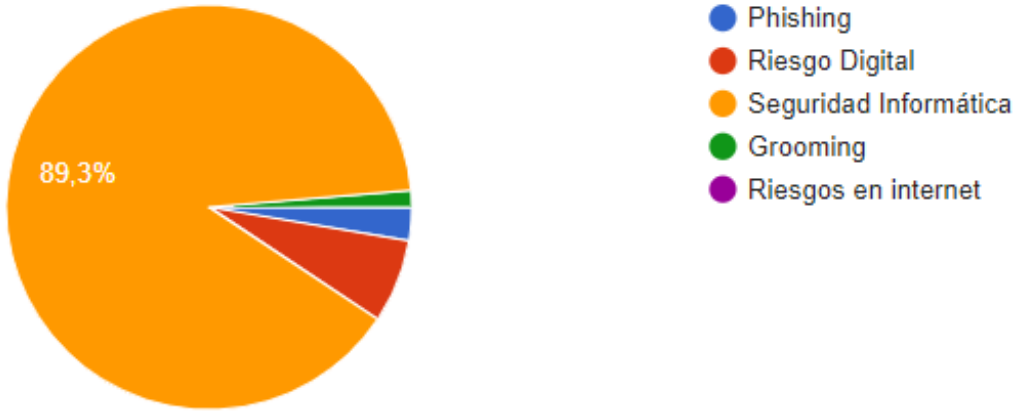

Figura 8. Post encuesta. Seguridad Informática

Análisis

La pregunta número uno está enfocada sobre el conocimiento de los estudiantes acerca de la seguridad informática, obteniéndose como resultado que un 77,2 por ciento de los alumnos encuestados responde de manera correcta a la pregunta y existe un 22,8 por ciento que lo hace de manera equivocada, dentro de esto hay un porcentaje importante que lo confunde con riesgo digital. Realizando la post evaluación que se lo hace después de que el estudiante ha trabajado en la plataforma en línea y en sus diferentes materiales didácticos se obtiene que el porcentaje de estudiantes que respondió de manera adecuada a la pregunta es el 89,3 por ciento, lo que implica que mejoró la comprensión de la definición de la seguridad informática en un 12,1 por ciento.

4.2 Pregunta 2.- Ciberbulling

La definición de: "Uso de información electrónica y medios digitales utilizados para acosar psicológicamente a una persona o a un grupo de personas de manera reiterada, agresiva y de forma intencional", corresponde a:

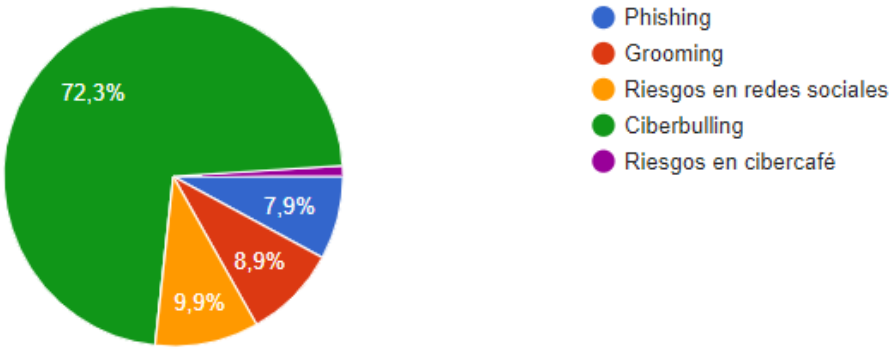

Figura 9. Encuesta. Ciberbulling

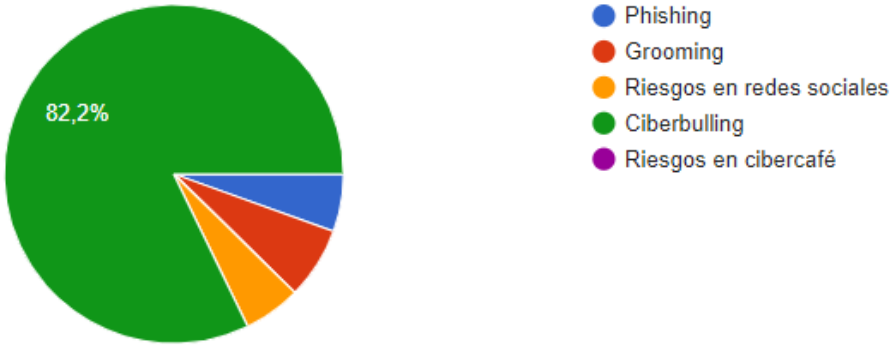

Figura 10. Post encuesta. Ciberbulling

Análisis

En la pregunta número dos se empezaba a trabajar sobre los riesgos digitales a los que se encuentran expuestos los adolescentes y el primero que se analizó fue el ciberbulling, el 72,3 por ciento de estudiantes respondió de manera correcta a la pregunta y existe un 27,7 por ciento que lo hace de manera equivocada confundiendo la definición con otros riesgos digitales. Realizando la post evaluación el porcentaje que respondió de manera adecuada a la pregunta aumentó al 82,2 por ciento. Existe un 17,8 por ciento de los estudiantes que no responde de manera adecuada a la pregunta. En base a estos datos se puede afirmar que en términos generales después de que el estudiante trabaja con la plataforma mejora la comprensión sobre la definición del riesgo digital en mención.

4.3 Pregunta 3.- Grooming

La definición de: "Es un acto de acoso progresivo, en el cual el adulto establece un vínculo de confianza y control emocional con el menor, basado en manipulaciones y engaños; uno de sus principales objetivos es obtener material de abuso contra los menores de edad", corresponde a:

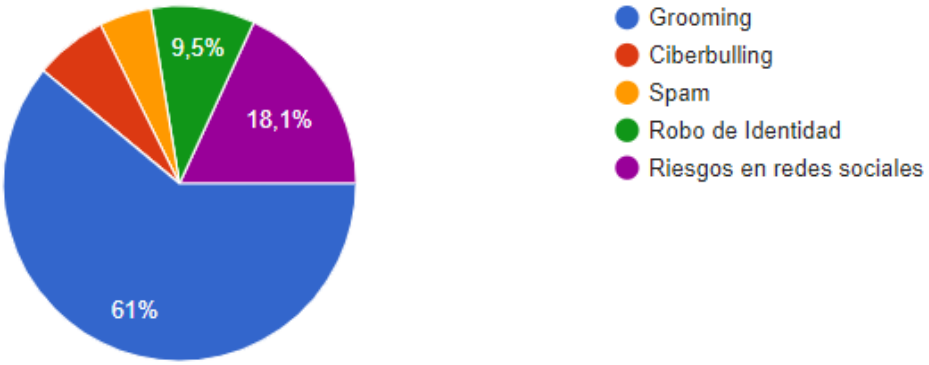

Figura 11. Encuesta Grooming

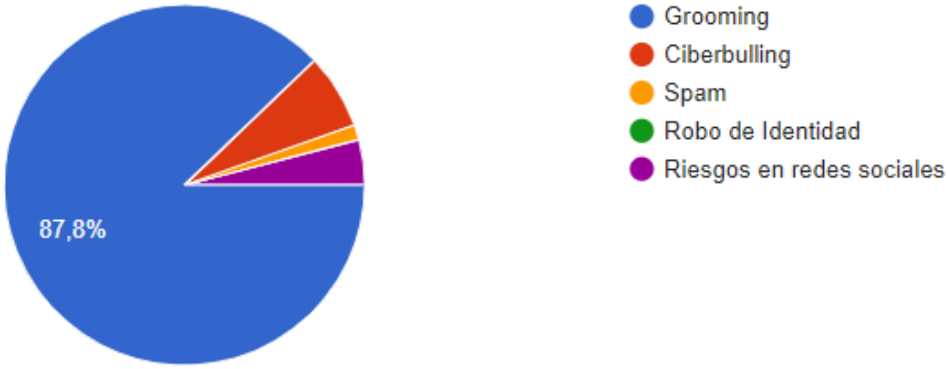

Figura 12. Post encuesta Grooming

Análisis

En la pregunta No. 3 se puede advertir que 39 por ciento de los estudiantes contesta de forma equivocada es decir de un universo de 95 estudiantes 37 contestan erróneamente y un importante 18,1 por ciento de los estudiantes confunde el grooming con riesgos en las redes sociales. En este caso al aplicar la post evaluación se nota una mejoría muy importante en la comprensión del riesgo digital Grooming, puesto que el número de estudiantes que contesta de manera equivocada baja a 11 que en porcentaje es

el 12.2 por ciento del total de estudiantes. El uso de la plataforma digital mejora de manera significativa la comprensión de los riesgos digitales, en este caso particular del grooming.

4.4 Pregunta 4.- Sexting

La definición de: "Intercambio de cualquier tipo de mensajes, fotos o videos pero con cierto contenido erótico entre adolescentes", corresponde a:

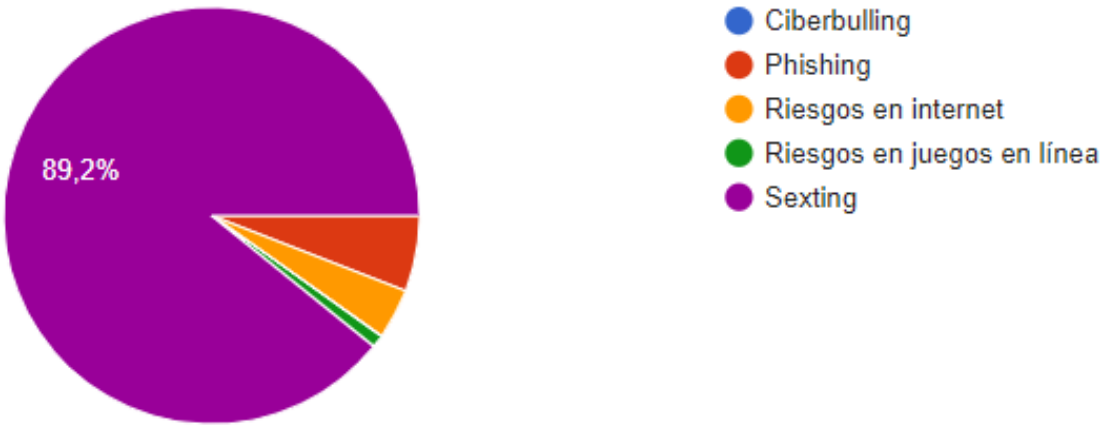

Figura 13. Encuesta sexting.

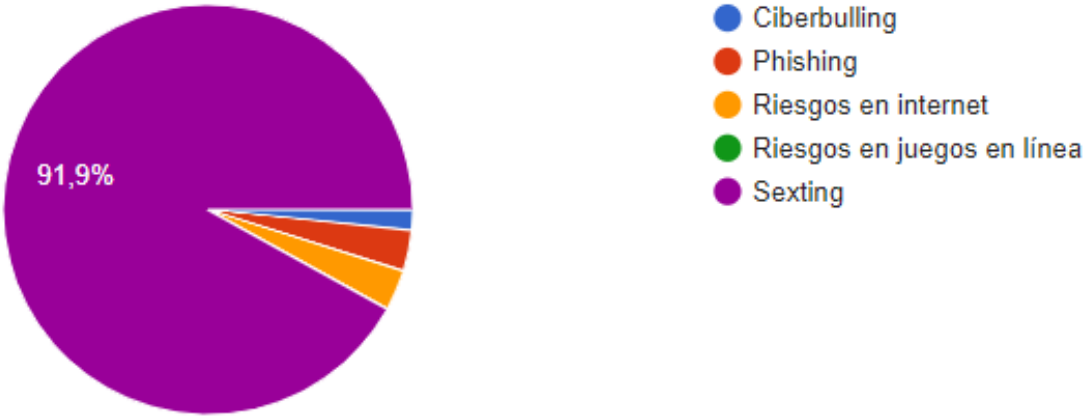

Figura 14. Post encuesta sexting

Análisis

En la pregunta No. 4 se analiza que los estudiantes tienen un importante conocimiento del riesgo digital sexting puesto que prácticamente no hay variación entre la aplicación de la encuesta con la post evaluación siendo el nivel de aciertos muy elevado ya que pasa del 89,2 por ciento en la primera encuesta a un 91,9 en la post evaluación.

Los dos porcentajes de aciertos son muy buenos, aún así con la utilización de la plataforma se mejora el nivel del conocimiento del riesgo digital en un 2,7 por ciento.

4.5 Pregunta 5.- Cibersexo

La definición de: "Es una manera de sexo virtual (no existe ningún tipo de contacto físico) donde dos o más personas se envían mensajes de carácter sexual explícito tratando de recrear un contacto sexual real. En los mensajes puede existir incluso audios, video o sonidos para hacer más real la virtualidad", corresponde a:

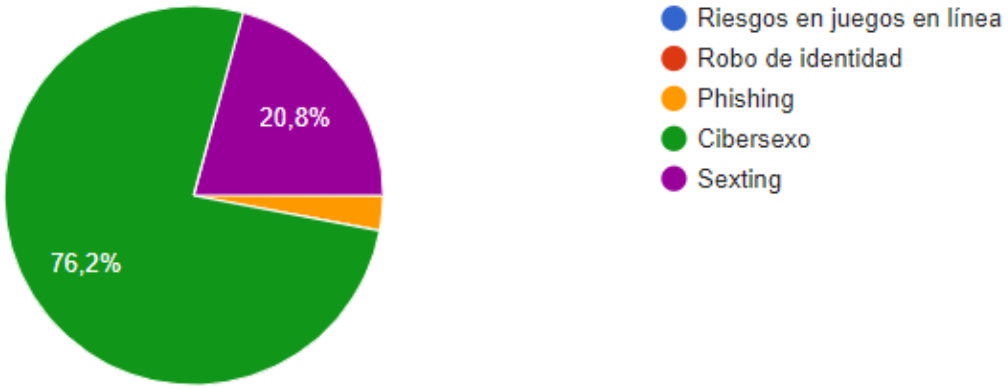

Figura 15. Encuesta cibersexo

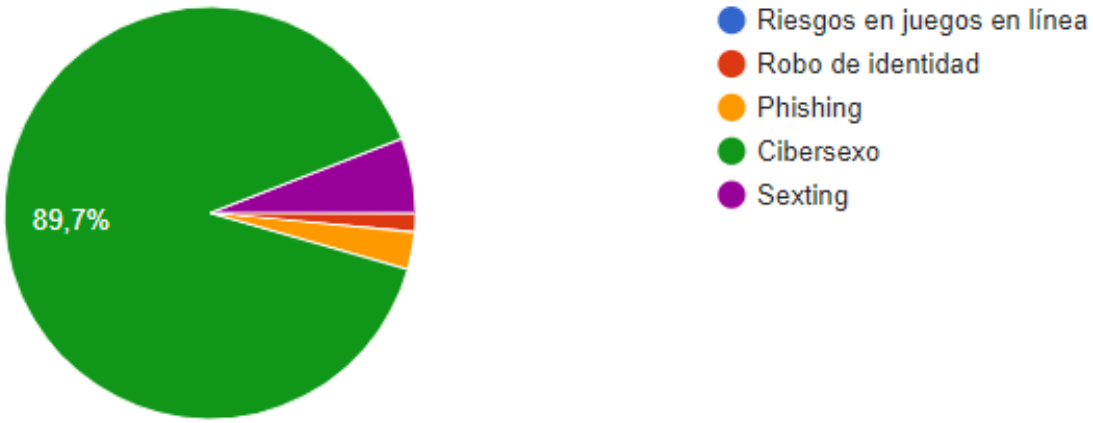

Figura 16. Post encuesta cibersexo

Análisis

En la pregunta No. 5 se pregunta por la definición de cibersexo y el 76,2 por ciento de los estudiantes encuestados responde de manera correcta, existe también un 20,8 por ciento que confunde la definición con sexting; al aplicar la post evaluación el porcentaje de alumnos que responde de forma correcta es el 89,7 por ciento lo que implica un

aumento de porcentaje significativo para esta definición después del uso de la plataforma en línea.

4.6 Pregunta 6.- Phishing

La definición de: "Es una técnica de tipo electrónico que busca adueñarse de información ajena con el fin de obtener datos personales y en última instancia un rédito económico", corresponde a:

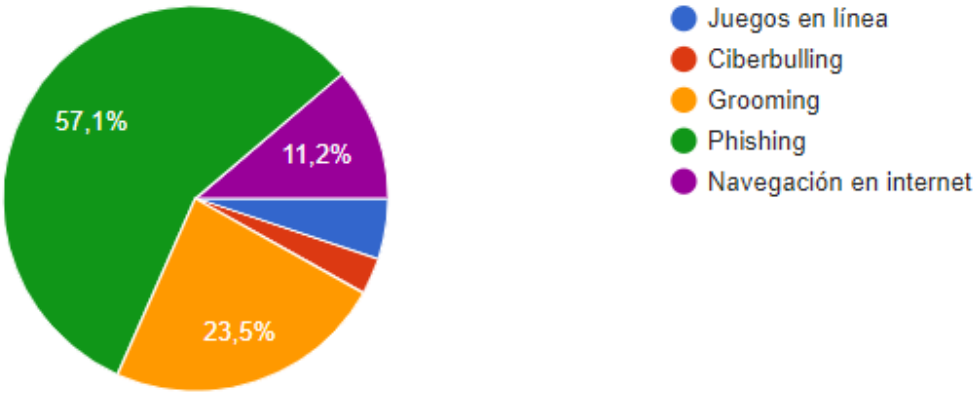

Figura 17. Encuesta Phishing

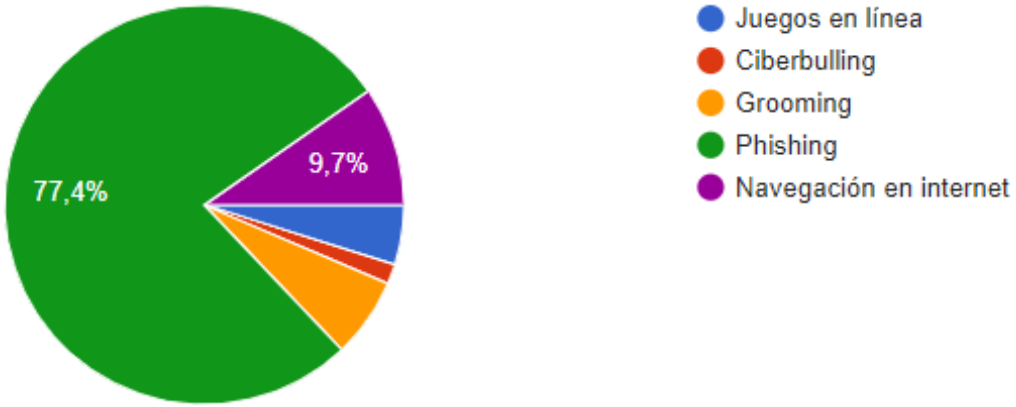

Figura 18. Post encuesta phishing

Análisis

En la pregunta No. 6 se analiza la definición de phishing, en este riesgo digital los estudiantes encuestados tuvieron problemas para acertar con la respuesta correcta puesto que solo 57,1 por ciento de los encuestados lo hizo de manera correcta, el grooming obtuvo un porcentaje importante de respuestas incorrectas con un 23,5 por ciento, en la aplicación de la post encuesta un mayor número de estudiantes contesta de manera adecuada la pregunta llegando a un 77,4 por ciento, el error sobre el grooming disminuye

de manera considerable. La definición correcta sobre el riesgo digital mejoró después de trabajar con la plataforma interactiva en 20,3 puntos porcentuales.

4.7 Pregunta 7.- Redes sociales. Ejemplo 1

Los adolescentes pueden perder de vista las relaciones y sentimientos reales, conversar con otros amigos u otras personas de diferente edad en forma presencial, la afectividad, el comportamiento porque el estar detrás de la pantalla les puede hacer perder las experiencias de la vida real. Este riesgo digital corresponde a:

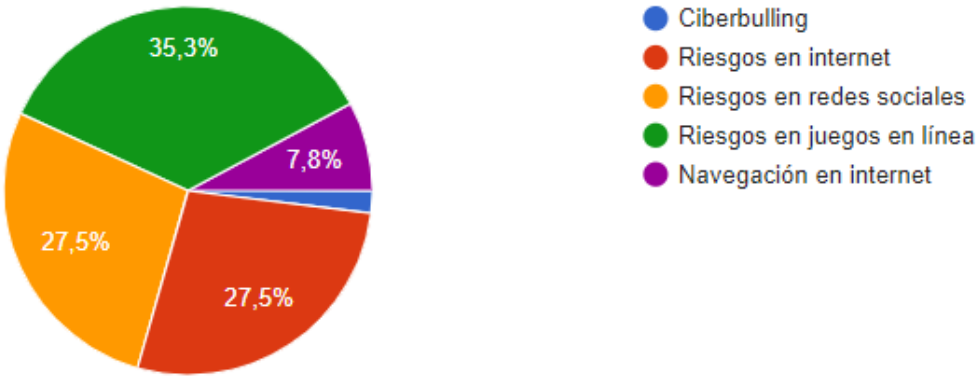

Figura 19. Encuesta redes sociales

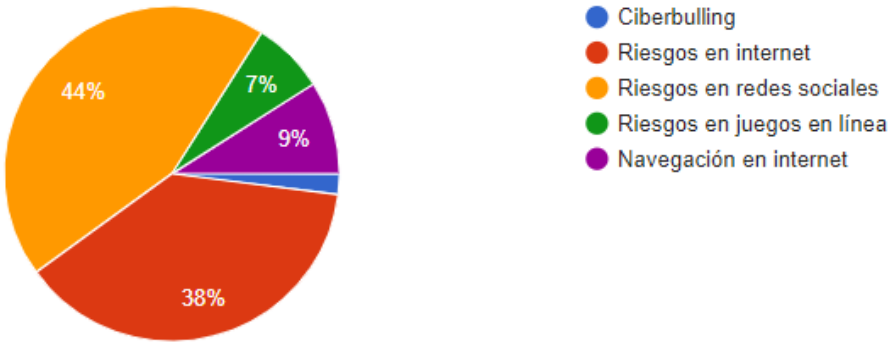

Figura 20. Post encuestas redes sociales

Análisis

A partir de la pregunta número 7, se pasa del campo de las definiciones a reconocer el tipo de riesgo digital al que se encuentran expuestos los adolescentes, la respuesta correcta para esta pregunta es riesgos en redes sociales que fue contestado por un 27,5 por ciento, un 27,5 por ciento respondió que era un riesgo en internet, 35,3 por

ciento riesgos en juegos en línea y un 7,8 por ciento navegación en internet. En esta pregunta que deja de ser una definición y es un ejemplo de riesgo digital a los que se encuentran expuestos los adolescentes se puede analizar que es más fácil saber la definición de un riesgo que determinar a qué tipo de riesgo pertenece. Con la aplicación de la post evaluación un 44 por ciento de los estudiantes responde de manera correcta, que si bien es cierto es un incremento de 16,5 puntos porcentuales, todavía sigue siendo un porcentaje muy bajo. El 38 % de los estudiantes responde que riesgos de navegación del internet. Un aspecto relevante es que la respuesta de juegos en línea cae de forma sustancial de 35,3 por ciento a 7%.

4.8 Pregunta 8.- Redes sociales. Ejemplo 2

Inadecuada configuración de las cuentas permitiendo que cualquier persona pueda acceder a información personal como son por ejemplo fecha de nacimiento, nombres, intereses, gustos, escuela o colegio donde se educan y fotos etiquetando a compañeros y familiares lo que facilita el cometimiento de otro tipo de delitos. Este riesgo digital corresponde a:

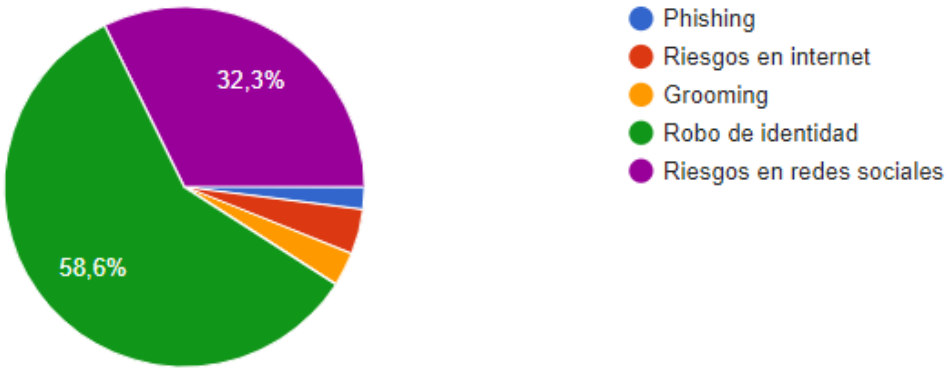

Figura 21. Encuesta redes sociales. Ejemplo 2.

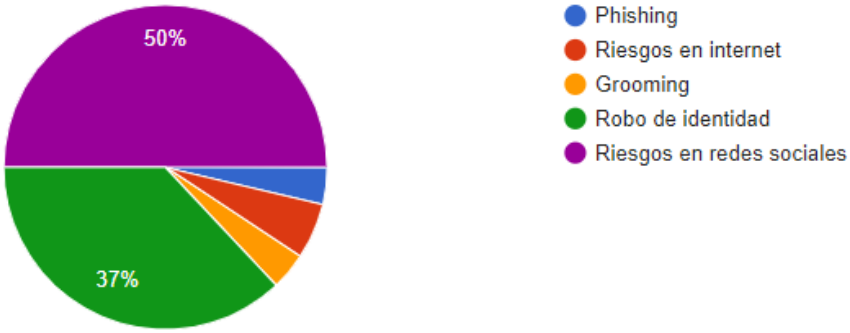

Figura 22. Post evaluación redes sociales. Ejemplo 2

Análisis

A partir de la pregunta número 8, nuevamente se pone un ejemplo de riesgo digital de una red social, sin embargo un 58,6 por ciento de los alumnos encuestados contesta de manera equivocada y escoge la respuesta robo de identidad y apenas un 32,3 por ciento riesgos en redes sociales. Se valida de forma similar que es más fácil entender la definición de un riesgo digital que reconocer un ejemplo del mismo y determinar a que tipo de riesgo pertenece. Al aplicar la post evaluación un 50 por ciento de estudiantes responde de manera correcta lo que implica un aumento de 18 puntos porcentuales y además pasa a ser la opción con mayor número de respuestas, sin embargo la opción robo de identidad se mantiene con un porcentaje alto del 37 por ciento.

4.9 Pregunta 9.- Cibercafe

Los computadores son de uso público y a través de diferentes programas pueden registrar usuarios y contraseñas y otro tipo de datos personales. Además se está expuesto a virus informáticos u otro tipo de software malicioso. Este riesgo digital corresponde a:

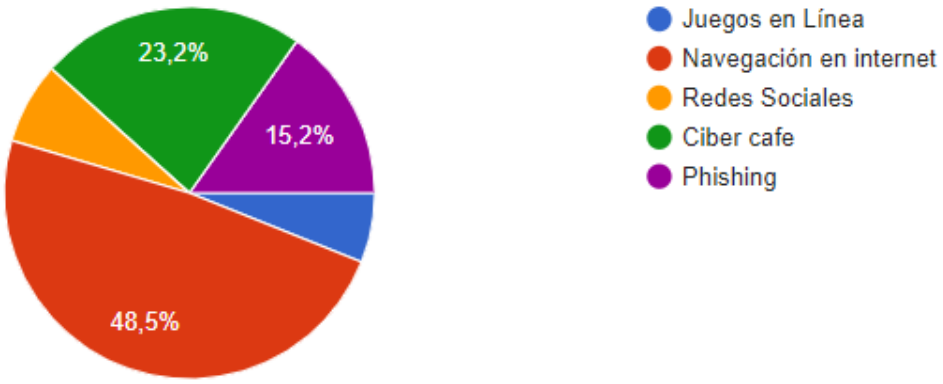

Figura 23. Encuesta Cibercafe

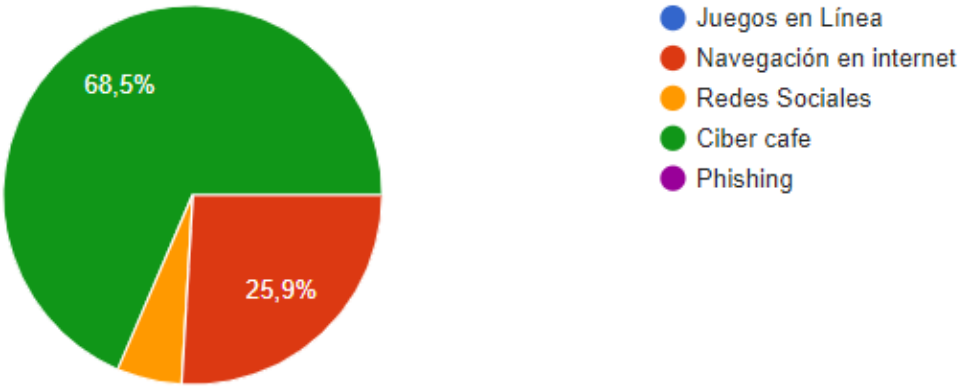

Figura 24. Post encuesta cibercafé.

Análisis

En la pregunta No. 9 se sigue analizando ejemplos de riesgos digitales, la respuesta correcta en está opción es cibercafé que es respondida de manera adecuada por el 23,2 por ciento del universo adecuado, la elección preferida por los estudiantes es navegación en internet con un 48,5 por ciento y el phishing ocupa un 15,2 por ciento. Al analizar las tres últimas preguntas en el momento de aplicar la encuesta se puede observar por los importantes porcentajes de respuesta obtenidos que los estudiantes perciben la navegación al internet como tal como un riesgo digital, sin poder determinar de manera adecuada a que corresponde el ejemplo de riesgo digital en mención. Al aplicar la post encuesta el 68,5 por ciento responde de manera adecuada a la pregunta y pasa a ser la opción de elección con mayor porcentaje con 68,5 por ciento lo que implica un aumento de 45,3 puntos porcentuales y la opción de navegación de internet baja sustancialmente a un porcentaje de 25,9 por ciento. Después de trabajar con la plataforma en línea hasta el momento es la pregunta que más puntos porcentuales subió en la elección de la opción correcta.

4.10 Pregunta 10.- Robo de identidad

A través de ingeniería social u otro tipo de software adueñarse de los datos personales con el objeto de realizar transacciones financieras. Este riesgo digital corresponde a:

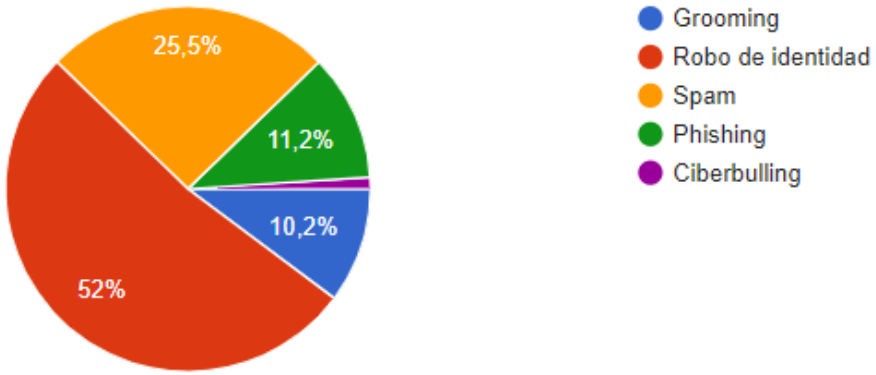

Figura 25. Encuesta robo de identidad

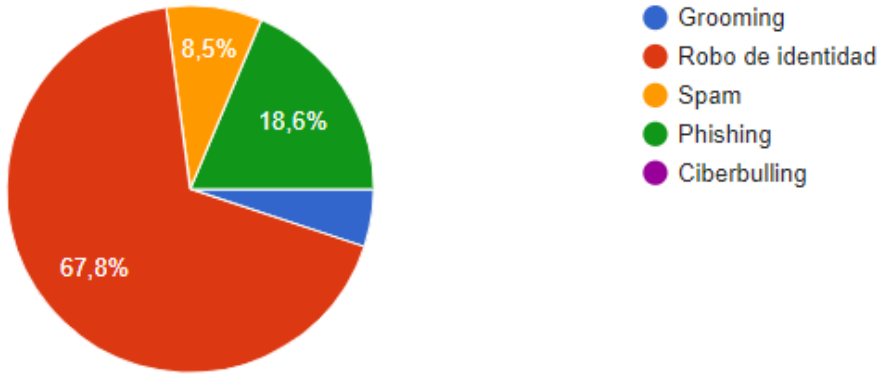

Figura 26. Post encuesta robo de identidad

Análisis

En la pregunta No. 10 la opción correcta es robo de identidad que es la opción elegida por el 52 por ciento de los estudiantes seguida por spam 25,5 por ciento, phishing 11,2 por ciento y grooming 10,2 por ciento. Al aplicar la post evaluación la opción correcta es decir robo de identidad sube a 67,8 por ciento es decir un aumento de 15,8 puntos porcentuales, la elección de spam se reduce a 8,5 por ciento y se mantiene un porcentaje importante que escoge el phishing con el 18,6 por ciento. Es importante recordar que nuestro universo encuestado es de 95 estudiantes por lo que en número de estudiantes las personas que escogen la opción correcta son 64 alumnos.

4.11 Pregunta 11.- Internet

Acceder a información equivocada o no deseada al dar un clic en un enlace no adecuado y el exceso de tiempo que pasa una persona navegando en actividades de ocio o poco productivas. Este riesgo digital corresponde a:

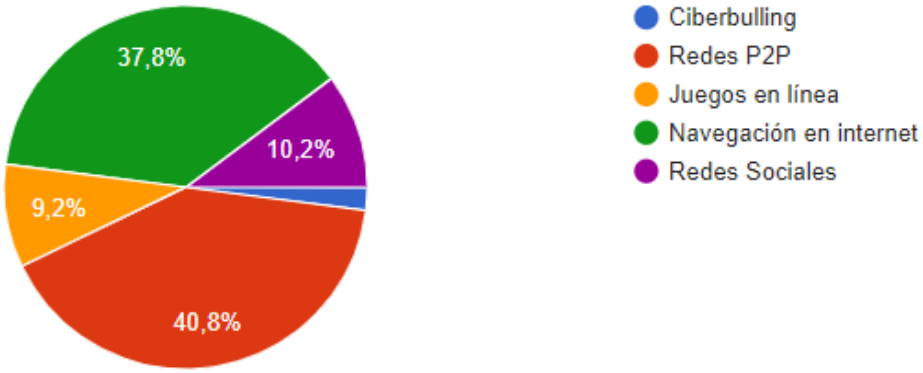

Figura 27. Encuesta navegación internet

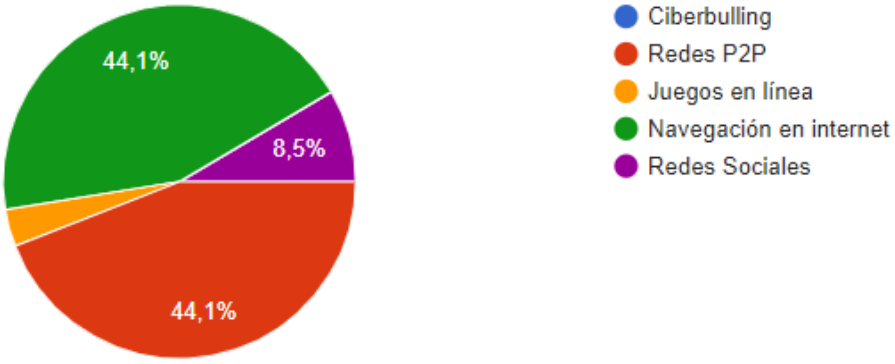

Figura 28. Post encuesta navegación en internet

Análisis

En la pregunta No. 11 un 40,8 por ciento de los estudiantes encuestados escoge la opción incorrecta redes P2P y un 37,8 por ciento la opción correcta navegación en internet, y en un porcentaje menor se escogen las demás opciones. Al aplicar la post evaluación existe un empate entre las opciones de navegación en internet y redes P2P con el 44,1 por ciento para cada opción y un 8,5 por ciento escoge redes sociales. Al hacer una análisis entre la encuesta y la post encuesta se puede verificar que los estudiantes no terminan de tener claro el ejemplo de riesgo digital o que lo tienen confundido entre redes P2P y navegación del internet, si bien es cierto sube la opción navegación en internet no

lo hace en un porcentaje significativo y tampoco es la primera opción de todas las respuestas posibles. En esta pregunta cabría la posibilidad de analizar si se debe explicar de mejor manera el ejemplo o a pesar del uso de la plataforma en línea los estudiantes no están claros entre los riesgos de navegar por internet y lo que significa los riesgos digitales de una red P2P.

4.12 Pregunta 12. Redes P2P.

Bajar información no deseado conocida con el nombre de fake y con software malicioso o malware. Este riesgo digital corresponde a:

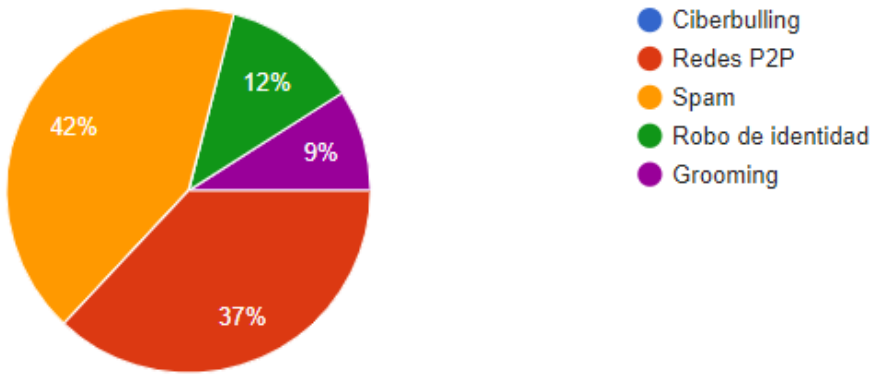

Figura 29. Encuesta Redes P2P

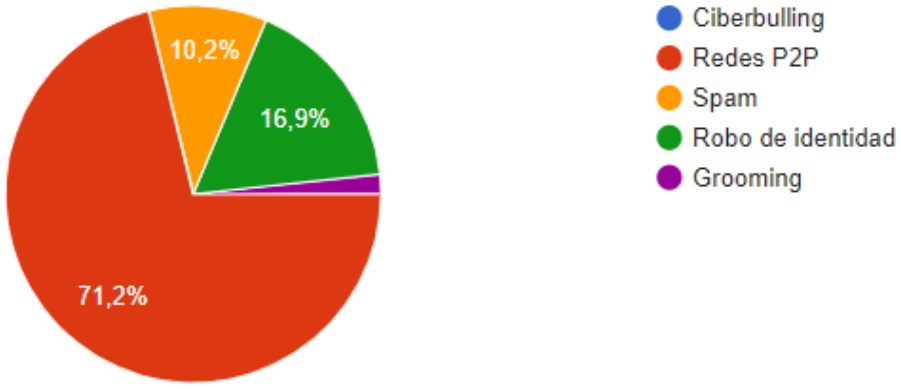

Figura 30. Post encuesta redes P2P

Análisis

En la pregunta No. 12 en la aplicación de la encuesta un 42 por ciento de los encuestados escoge la opción incorrecta spam y un 37 por ciento la opción correcta redes P2P un 12 % robo de identidad y un 9 % Grooming. Al analizar la post encuesta el 71,2

por ceinto de los encuestados escoge la opción correcta redes P2P, lo que implica un aumento 34,2 puntos porcentuales, las otras opciones escogidas son robo de identidad con 16,9 por ciento y spam con 10,2 por ciento. Al trabajar con la plataforma en línea queda claro lo que es un riesgo digital que corresponde a redes P2P.

4.13 Pregunta 13.- Usuarios de redes sociales

Según la empresa Menntinno Group la red social que más usuarios tiene en el Ecuador es:

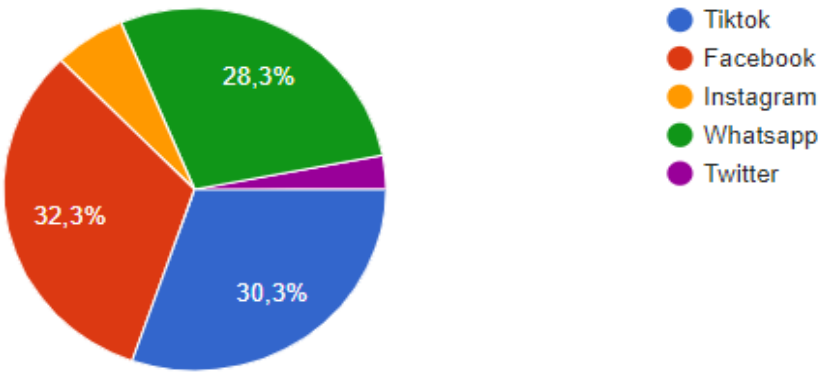

Figura 31. Encuesta usuarios redes sociales

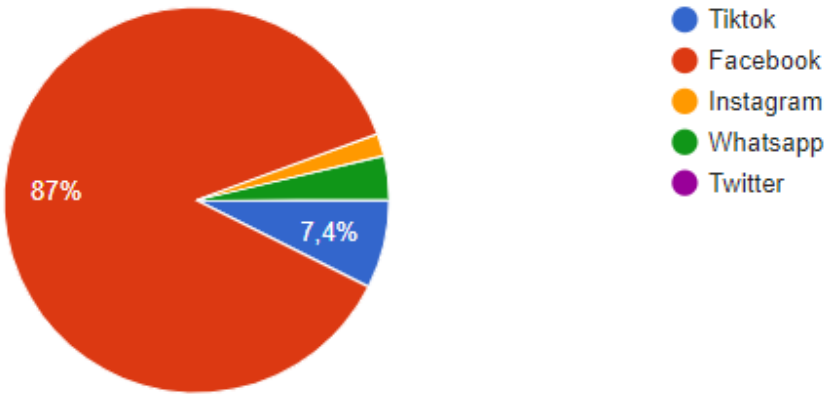

Figura 32. Post encuesta usuarios de redes sociales

Análisis

En la pregunta No. 13 es general sobre el número de usuarios que posee cada red social en Ecuador, existe en las respuestas prácticamente un empate entre Facebook, whatsapp y tiktok, cada uno con alrededor de 30 puntos porcentuales. Al realizar la post evaluación la opción Facebook que es la correcta alcanza el 87 por ciento. En está

pregunta se pueden concluir algunas cosas importantes cuando la respuesta es conceptual es decir no requiere mayor razonamiento el trabajar con una plataforma ayuda muchísimo en la recepción de los datos hacia los encuestados. En este caso la respuesta correcta pasó del 32, 3 al 87 por ciento es decir subió más de 54,7 por ciento de puntos porcentuales. Sin duda la respuesta que más puntos subió.

4.14 Pregunta 14. Actores del proceso de seguridad informática

En las estrategias para reducir los riesgos digitales a los cuales se encuentran expuestos los adolescentes deben intervenir los siguientes actores del proceso de enseñanza aprendizaje.

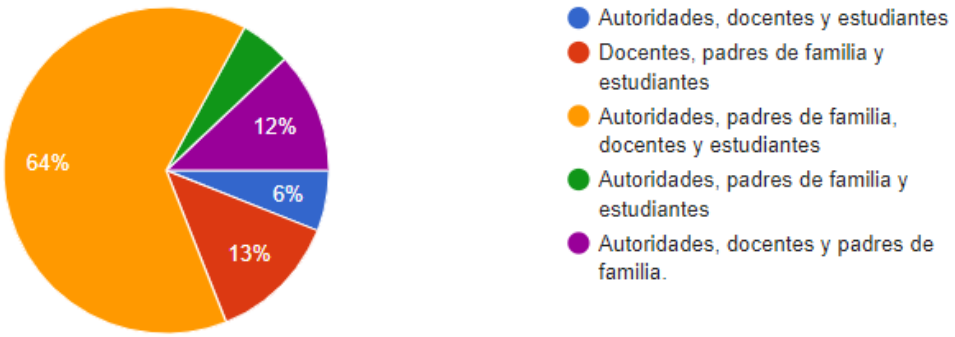

Figura 33. Actores del proceso de seguridad informática

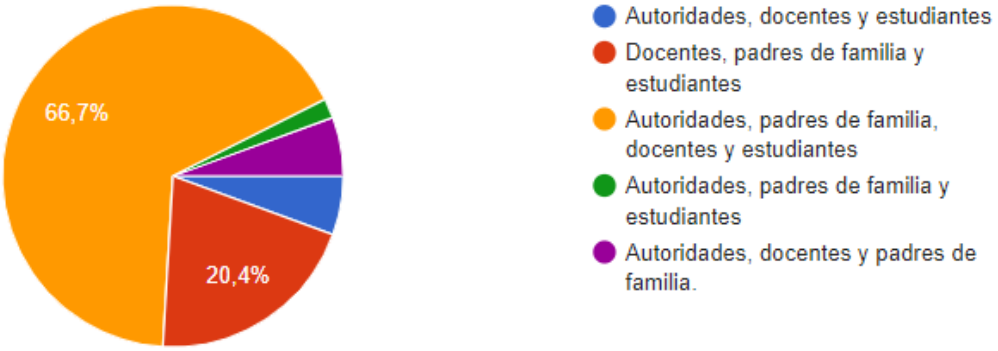

Figura 34. Post encuesta actores del proceso de seguridad informática

Análisis

En la pregunta No. 14 el 64 por ciento de los estudiantes responde de manera correcta es decir autoridades, padres de familia, docentes y estudiantes y 20,4 por ciento excluye a las autoridades, un 12 por ciento a los estudiantes. En la post evaluación responde de manera acertada el 66,7 por ciento de estudiantes, es decir un aumento

porcentual de solo un 2,7 por ciento. Si bien es cierto el porcentaje de elección correcta es alto, no es un cambio importante con la plataforma en línea como sucede con otras respuestas, pero una observación importante que hay que señalar al respecto, es que en la plataforma no existía material lúdico sobre este tema sino un documento en pdf que hay que bajarlo con estrategias de seguridad informática para adolescentes.

CAPITULO V
Propuesta

5.1 Estrategias de seguridad

La tecnología ha evolucionado en los últimos 20 años a un ritmo vertiginoso y los riesgos a los que se encuentran expuestos los adolescentes como se ha revisado en este documento son muchos, sin embargo la tecnología ofrece una serie de ventajas y oportunidades que es imposible negar su acceso o dejar de utilizarlas, lo conveniente es conocer los cuidados que se deben tener en el manejo de las aplicaciones. Es decir se debe conocer estrategias para minimizar los riesgos digitales y potencializar el uso de las tecnologías de manera que permitan desarrollar las diferentes capacidades de los adolescentes.

Los riesgos digitales afectan directamente a los adolescentes sin embargo todos los involucrados en el proceso de enseñanza aprendizaje (padres, estudiantes, docentes, autoridades), deberían conocer los mismos y en base a este conocimiento poder aplicar las recomendaciones que les corresponde.

Con un manejo adecuado del internet la principal ventaja que disponen los adolescentes es poder acceder a una cantidad innumerable de recursos didácticos de prácticamente todas las materias lo que permitirá mejorar su aprendizaje, el acceso a una cantidad importante de información en un mínimo de tiempo.

Respecto a esto cabe destacar lo que dice Pérez Tornero (2017) al plantear que “el uso adecuado de internet se garantiza cuando existe una buena convivencia online con los demás, la cual requiere altas dosis de tolerancia y respeto, que les aportará las claves para convertirse en ciudadanos digitales”.

Tabla 19.- Ventajas y desventajas en el uso de internet en la formación de valores

Ventajas con uso adecuado de internet	Desventajas con uso inadecuado de internet
Aprendizaje social	Diversidad de opiniones
Desarrollo de la empatía	Anonimato

Conciencia e implicación social	Relativización de los problemas
Trabajo colaborativo	Falta de honestidad
Influencia positiva	Influencia negativa
Código de comportamiento	Ciberacoso
Fomento de la libertad de expresión	Límites dudosos
Adquisición del concepto de autoría	Piratería
Desarrollo del respeto	Falta de respeto
Ayuda para potenciar la tolerancia	Desarrollo de Xenofobia

Fuente: Tornero(2017)

Las recomendaciones que se dan para el uso seguro de la navegación en internet y el uso de las diferentes aplicaciones han sido obtenidas de diversas fuentes y el autor ha elaborado en base a estas las siguientes recomendaciones o sugerencias que de aplicarse por todos los involucrados en el proceso de enseñanza aprendizaje sin duda alguna disminuiría de manera significativa los riesgos digitales a los que se encuentran expuestos los adolescentes.

5.1.1 Para los adolescentes

- Una contraseña de ningún tipo de aplicación en línea debe ser compartida a personas ajenas al entorno familiar y estas deben cambiarse regularmente, se recomienda hacer un registro con la aplicación y la contraseña y mantener este registro en un lugar seguro. Evita tener la misma contraseña en todas las aplicaciones y nunca guardes las misma en ningún navegador. Las contraseñas deben tener al menos 8 caracteres y mezclar letras mayúsculas con letras minúsculas, números y algún carácter especial por ejemplo Vi@L@cte@2030, es una contraseña segura.
- En las aplicaciones que requieran de usuario no se debe poner nombres que hagan referencia al nombre real y evita acompañarle del año de nacimiento o de la edad por ejemplo Carlos_1974, no es un usuario adecuado, porque se puede presumir que es un hombre de nombre Carlos que nació en el año de 1974, esto

complementado con información de otras aplicaciones puede permitir capturar mucha información de la persona.

- Revisa la información que va a estar disponible en el internet sea está fotos, videos, archivos multimedia u otro tipo de información personal, recuerda que si no se tiene el suficiente conocimiento para realizar las configuraciones de seguridad en las aplicaciones, estás van a estar disponibles para que cualquier persona pueda acceder a las mismas. No compartas imágenes, videos u otro tipo de archivos multimedia de tipo comprometedor con ninguna persona sea conocida o desconocida, no se debe olvidar que una vez que compartes una foto, un video o un archivo multimedia u otro tipo de información de carácter digital, se pierde el control de lo que pueda pasar con los mismos.
- No se debe compartir ningún tipo de foto o video con contenido sexual sea propio o de terceros con ninguna persona por mucha afinidad o afectividad que exista. La divulgación de estas imágenes por error, hurto u omisión causan un grave daño a la privacidad de las personas afectadas. La mejor estrategia es evitar este tipo de fotos y videos, ni siquiera se debe tener en el celular u otro tipo de dispositivo electrónico.
- No se debe pactar ningún tipo de cita real con personas que se conoce a través de una aplicación en línea. En este mismo sentido si se decide tener una cita virtual con un desconocido no se debe prender la cámara del dispositivo digital.
- Si por alguna aplicación se recibe algún tipo de insulto, de provocación o amenaza bloquea a la persona que lo hace e informa inmediatamente a una persona adulta de confianza, de preferencia a los padres. Si la aplicación lo permite se debe mantener las pruebas de este tipo de actos, es decir no borrar los mensajes, las grabaciones de voz, los videos, etc.
- El comportamiento en las diferentes aplicaciones que se utilicen debe ser el adecuado, es decir tratar con respeto a las personas con las que te comuniques.
- Investiga sobre las configuraciones de seguridad que brindan las diferentes aplicaciones y realiza las respectivas configuraciones. No es una buena práctica dejar ningún tipo de plataforma social como pública.
- No responder a ningún tipo de formulario o cualquier otro tipo de interface que pida datos de tipo personal por internet. Sea que estos pedidos lleguen por correo electrónico, chat, u otro tipo de plataforma tecnológica. Las encuestas u otro tipo

de documentos para realizar cualquier tipo de estudio incluso publicitario no solicitan información personal.

- Evita dar clic en enlaces que se utilicen para descargar archivos a menos que se tenga la certeza que no es un software malicioso.
- En el caso de las plataformas sociales no aceptes invitaciones de amistad de personas desconocidas, detrás de una bonita foto se esconde el anonimato, recuerda que si no conoces a la persona de manera real, no tienes idea de con quien realmente estás tratando.
- Investigar sobre los diferentes tipos de licencia que existen para las diferentes aplicaciones, respeta el uso de las licencias de software y la propiedad intelectual. Una buena práctica es leer la política de privacidad de las diferentes aplicaciones.
- En cualquier aplicación que utilices cámara web debes tener cuidado, recuerda que se puede estar grabando de manera remota la conversación y lógicamente el video de la cámara web. Se debe usar la cámara web cuando estás con personas conocidas y debes tener el mismo cuidado de si estuvieses en público, es decir frente a una cámara no debes hacer nada de lo que no harías de manera pública.
- Las aplicaciones en internet son múltiples incluida la propia navegación se debe dar un buen uso a las mismas que sirvan para mejorar y aumentar conocimientos, habilidades y capacidades acorde a la edad de cada persona.
- El uso del internet para divertirse, jugar o realizar otro tipo de actividades de distracción es totalmente válido, pero se debe tener en cuenta las recomendaciones emitidas para realizar las actividades con seguridad.

5.1.2 Para los padres

- Los padres deben acompañar en el uso de la tecnología a sus hijos desde pequeños, establecer control, reglas y horarios para el uso de dispositivos electrónicos sea estos computadores, teléfonos celulares, tablets u otro tipo de dispositivos electrónicos; de esta forma cuando el niño sea adolescente estará acostumbrado a un manejo vigilado de la tecnología por parte de sus progenitores.
- Los computadores así como otros dispositivos digitales deben estar en un lugar visible y de común acceso para todos los miembros de la familia, se debe evitar colocar los dispositivos digitales en los dormitorios.

- Establecer normas para el manejo de los dispositivos electrónicos, dentro de estás un aspecto muy importante es el tema de los horarios, se debe tratar en la medida de los posibles que la navegación y uso de los equipos sea hasta las 18:00. Evitar la navegación en la noche y limitar el tiempo de uso de la tecnología.
- Dialogar con los hijos para concienciar en ellos las ventajas del uso de la tecnologías, pero también los riesgos que existen en las diferentes aplicaciones.
- Investigar sobre los contactos, amistades de los hijos en el mundo virtual en las diferentes plataformas, tratar de conocer cuales son amigos de tecnología y a cuales contactos conoce realmente, al hacer esto se debe evitar invadir la privacidad de los hijos.
- Involucrarse con los hijos en el manejo de la tecnología, jugar con ellos, navegar en temas que les interese, adentrarse en el mundo de la tecnología junto a sus hijos. Hable con ellos sobre el temas tecnológicos tal cual lo hace sobre temas de la vida real. Los hijos deben estar claro que los padres mantendrán la supervisión de las actividades en línea que realicen.
- Conversar con los hijos sobre los riesgos de compartir fotos, videos, archivos multimedia o datos personales sean individuales o del entorno familiar.
- Tener un comportamiento respetuoso, responsable y ético en el uso de las tecnologías para que pueda transmitir con el ejemplo estos principios a sus hijos.
- Hablar con los hijos acerca de los enlaces no deseados en internet, sobre la posibilidad de abrir enlaces pornográficos u otro tipo de enlaces sobre temas no apropiados para la edad de ellos y la manera de afrontar este tipo de situaciones desagradables.
- Una buena práctica de ser posible es destinar en el hogar lugares libres de dispositivos electrónicos por ejemplo se puede consensuar durante las comidas no utilizar los dispositivos y mantenerlos en silencio en otros lugares de la casa.
- Es recomendable apagar el wi fi en la noche después de una determinada hora.
- Instalar un programa de control parental se explicará con detalle el tema más adelante, pero en ningún caso esto reemplazará a la supervisión de los padres.

5.1.3 Para los docentes

- Evitar ingresar contraseñas en las aplicaciones delante de los estudiantes o en computadores de uso grupal, puesto que pueden tener instalados software de lectura de contraseñas. En la medida de lo posible se debe utilizar un computador personal o si el computador es de la institución se debe revisar que este se encuentre actualizado el sistema operativo y con al menos un antivirus actualizado.
- No compartir las contraseñas con ninguna persona sea docente o estudiante y mantener un registro de las contraseñas en un lugar seguro.
- No se debe utilizar dispositivos digitales de la institución para utilización de aplicaciones o plataformas sociales de carácter personal.
- Si se requiere utilizar plataformas sociales para el proceso de enseñanza aprendizaje es recomendable manejar dos cuentas la primera servirá para interactuar con los estudiantes en las diferentes actividades y la segunda debe ser de carácter personal.
- Las instituciones educativas deben utilizar filtrado de contenidos o control parental con el fin de mantener el registro sobre los diferentes sitios en los que navegan los alumnos. En caso de no tenerlo se debe recomendar el uso de dicho software de control.
- Los estudiantes acorde a la edad de cada uno tiene diferentes tipos de gustos en la navegación así como en el uso de las aplicaciones en internet. El docente debe estar informado de las tendencias de los estudiantes en el manejo en línea acorde a las edades.
- Concienciar a los estudiantes sobre el manejo y uso de las diferentes licencias de software. Es una forma de enseñarles a respetar la propiedad intelectual.
- Emitir normas claras sobre el uso y manejo de los dispositivos digitales en clases y en los laboratorios y supervisar para que las mismas se cumplan.
- Informar a los padres sobre las normas emitidas para el control de los dispositivos en las aulas.
- Respeta la privacidad de los estudiantes en sus diferentes aplicaciones y plataformas sociales, supervisa que las normas emitidas se cumplan pero sin afectar la privacidad de los mismos.
- Investigar sobre las aplicaciones de la web, las diferentes plataformas sociales, y las nuevas tecnologías y el aparecimiento de nuevas aplicaciones dentro del

proceso de enseñanza aprendizaje. Es muy útil tener un manejo adecuado de las TICs.

5.1.4 Para las autoridades

- Disponer que se realice un inventario de equipos informáticos que incluya computadores de escritorio, computadores portátiles, impresoras y otro tipo de equipos y dispositivos informáticos, tanto los que ocupa el personal administrativo en sus diferentes actividades, cuanto aquellos equipos que son de uso de los estudiantes y que se encuentran en el laboratorio. Especificar el estado en el que se encuentran los equipos informáticos. Si la institución educativa es grande incluir en el inventario de equipos servidores. En el inventario se debe tener como información mínima el registro y las características de los componentes internos del CPU (Disco duro, memoria, procesador y otros), la ubicación en la que se encuentra el equipo y cuál es el responsable del mismo.
- Registrar todos los componentes activos que conforman la red de la institución es decir switch, router, dispositivos alámbricos e inalámbricos, racks y/o armarios de comunicaciones y otro tipo de accesorios de ser el caso. Los dispositivos tienen que estar claramente identificados así como los lugares en los que se encuentran ubicados para mantener un adecuado control y facilitar el mantenimiento de los mismos en caso de ser necesario.
- Todos los computadores de la institución deberán tener claves de acceso, tanto del personal administrativo, como de los laboratorios y de ser el caso aquello equipos que se utilizan para diferentes tipos de presentación dentro de las aulas. Se debe crear reglas para la creación de contraseñas seguras.
- La institución debe contar con un especialista en TI con el conocimiento suficiente para realizar las actividades antes mencionadas.
- Organizar charlas, talleres o conferencias sobre temas de seguridad informática para el personal docente y administrativo de la institución así como para los estudiantes y padres de familia. Para impartir este tipo de charlas se debe partir bajo la hipótesis que existe un nulo conocimiento del tema, Si la institución educativa es pequeña y no cuenta con recursos económicos para contratar capacitadores sobre el tema se pueden realizar gestiones ante diferente tipo de autoridades sobre todo universitarias con el fin de tener panelistas con

conocimientos sobre la seguridad informática. Otra fuente importante de investigación son los diferentes recursos en línea disponible de manera gratuita en internet. Este tipo de charlas deben ser periódicas de modo tal que se vaya creando conciencia en todos los actores que conforman una institución educativa sobre la importancia de la ciberseguridad en general y de la seguridad informática en particular. En las capacitaciones se debe incluir al especialista en TI.

- Las autoridades deberían impulsar la creación de un plan de seguridad informática para la institución, pero por las características de las diferentes instituciones educativas se deber contar al menos con un documento de medidas de seguridad para garantizar la seguridad de la información, el cual debe ser conocido y cumplido por todos los actores dentro de la institución.
- Apoyar las denuncias sobre posibles amenazas a la seguridad de la información. Es indispensable que el personal conozca que cualquier amenaza va a ser investigada, puesto que todos estamos expuestos a un ataque a la seguridad de la información. La idea principal de una investigación es evitar los ataques informáticos y concienciar al personal docente, administrativo, estudiantes y padres que todos estamos expuestos a ser atacados por ciber delincuentes a través de mecanismos sencillos como la ingeniería social.
- Es imprescindible capacitar en temas de seguridad informática a los padres, puesto que ellos son los principales actores de la educación de sus hijos y por ende desde casa deben guiar el manejo correcto del uso de la tecnología lo que facilitará cualquier actividad que sobre el tema se realice en la institución educativa.
- Elegir el software adecuado para la institución considerando las diferentes opciones de licenciamiento y las disposiciones legales.
- Apoyar de manera decidida cualquier actividad dentro de la institución para mejorar la seguridad de la información.

En las recomendaciones de seguridad emitidas para los diferentes actores del proceso de enseñanza aprendizaje se debe considerar lo que dice Echebúrua y De Corral (2010) respecto a este tema “El uso de las TIC y de las redes sociales impone a los adolescentes y adultos una responsabilidad de doble dirección: los jóvenes pueden adiestrar a los padres en el uso de las nuevas tecnologías, de su

lenguaje y sus posibilidades; los padres, a su vez, deben enseñar a los jóvenes a usarlas en su justa medida.

5.2 Control Parental

El Control parental es cualquier tipo de herramienta, tecnológica o no que permita a los padres vigilar, supervisar a los hijos la manera en la que navegan en el internet, las aplicaciones y las plataformas sociales que usan y para que lo usan. En este contexto el control parental automático son programas desarrollados para ayudar a los padres en las actividades mencionadas.

El código de la niñez y adolescencia publicado en el registro oficial el 3 de Julio del 2003 en sus artículos 45, 46 y 47 en cuanto se refiere a acceso a la información y sus controles en la parte concerniente textualmente dice:

"Art. 45.- Derecho a la información. Los niños, niñas y adolescentes tiene derecho a buscar y escoger información: y a utilizar los diferentes medios y fuentes de comunicación con las limitaciones establecidas en la ley y aquellas que se derivan del ejercicio de la patria potestad.

Es deber del Estado, la sociedad y la familia, asegurar que la niñez y adolescencia reciban una información adecuada, veraz y pluralista: y proporcionarles orientación y una educación crítica que les permita ejercitar apropiadamente los derechos señalados en el inciso anterior".

"**Art. 46.- Prohibiciones relativas al derecho a la información**. Se prohíbe:

1. La circulación de publicaciones, videos y grabaciones dirigidos y destinados a la niñez y adolescencia que contengan imágenes, textos o mensajes inadecuados para su desarrollo: y cualquier forma de acceso de niños, niñas y adolescentes a estos medios....."

Estas prohibiciones se aplican a los medios, sistemas de comunicación, empresas de publicidad y programas"

El internet es una red de redes que permite el uso de diferentes aplicaciones como ya se ha mencionado, los adolescentes lo utilizan para muchas actividades, ocio, recreación, diversión, comunicación, entretenimiento y también es una herramienta para la educación. El número de horas diarias en la que un menor pasa frente a dispositivos digitales es cada vez mayor por ende la posibilidad de encontrarse con contenido no adecuados para su edad aumenta cada día, como se ha mencionado ya en el Código de la niñez y adolescencia es "Deber del estado, la sociedad y la familia" el control que el acceso a la información sea el adecuado, además del acompañamiento permanente de los padres en el uso de la tecnología una herramienta adecuada para lograr esto es el control parental.

En cuanto se refiere al control parental automático es decir a través de software existen dos maneras de operar la seguridad: La prevención y el control.
Es recomendable recordar que ningún programa automático de control parental es cien por ciento seguro, este siempre debe estar complementado con el control de los padres de manera presencial a través de la educación y la concienciación. Es decir las herramientas de control parental coadyuvan en un mejor uso del internet y sus aplicaciones en los adolescentes pero nada reemplazará al diálogo permanente que debe existir entre padres e hijos en temas tecnológicos.

Todos los programas de control parental tienen la misma lógica de funcionamiento es decir que realizan con pequeñas diferencias las mismas tareas, entonces analizaremos en términos generales cómo funcionan los programas de control parental.

- Permiten controlar la navegación a través de determinar a qué páginas web se puede ingresar y a cuales son páginas no permitidas. Para esto se ha creado un estándar en la industria que les suele llamar lista blanca y lista negra. En la lista blanca se encuentran las páginas a las que el menor se encuentra permitido acceder y en la lista negra aquellas que están bloqueadas.
- La cantidad de páginas web creadas hasta el momento puede superar las mil millones y cada día aumentas, entonces el bloqueo por listas es útil pero no siempre puede resultar efectivo, entonces otra de las características es el permitir bloquear el acceso por contenidos dependiendo de la existencia de ciertas palabras. Por ejemplo se puede bloquear contenidos que tengan palabras como

drogas, pornografía, sexo, violencia, muerte entre otras, es decir en este caso se puede bloquear los contenidos según las palabras que contenga un determinado artículo.

- Bloquean aplicaciones o plataformas sociales según nuestros requerimientos, en este caso podríamos determinar que aplicaciones y plataformas sociales puede usar el menor de edad.
- Determinar horarios, es decir se puede autorizar el uso de los dispositivos digitales con restricciones de horario, en el programa de control parental se puede decir desde que hora hasta que hora pueden utilizar las aplicaciones e incluso se puede modificar los horarios para que el fin de semana ampliar o reducir el número de horas de uso de tecnología.
- Bloquear la información que sale desde la computadora u otro tipo de dispositivo digital esto impedirá la difusión de datos personales u otro tipo de datos. Es muy útil desde cualquier aplicación como el correo electrónico, chat, llenado de formularios, la navegación misma u otros.
- Una característica adicional de las herramientas de control parental es el monitoreo, el cual permite saber en todo momento que páginas web se han visitado, en algunos casos incluso el tiempo que estuvieron en esas páginas, con esto se puede determinar los hábitos de los niños y adolescentes en el uso de aplicaciones y plataformas sociales. Para el uso de esta opción siempre es necesario recordar la privacidad del menor de edad, sin embargo puede ser un muy buen recurso para controlar la navegación de los hijos en los diferentes tipos de dispositivos tecnológicos.

Sobre este tema Roldan (2018) indica “es importante controlar de forma adecuada a los hijos/as en el uso de Internet, ellos pasan mucho tiempo conectados con libre acceso a webs de todo tipo y suelen tener un buen manejo de las nuevas tecnologías casi de forma innata, puede que ellos sepan más que los padres sobre Internet, así que no hay que quedarse atrás, se debe aprender sobre el uso de Internet y de las nuevas tecnologías para el control del mismo”

Como todo lo que se refiere a las aplicaciones en internet existen una gama de productos de software para control parental, se presenta algunos de los programas más utilizados en la siguiente tabla:

Tabla 20. Software de control parental

Software	**Tipo de Software**	**Costo en dólares**	**Página Web**
Qustodio	Propietario	Desde 54,95 al año	https://www.qustodio.com/es/
Google Family Link	Libre	Sin costo	https://families.google/intl/es_ALL/familylink/
Eset Parental Control	Propietario	Desde 49,99 al año	https://co.tienda.eset-la.com/eset-parental-control
Eyezy	Propietario	199,88 al año	https://www.eyezy.com/es/
Kurupira web filter	Libre	Sin costo	https://www.kurupira.net/
Segure Kids	Propietario	Desde 29,95	https://securekids.es/
Norton Family	Propietario	39,99 al año	https://lam.norton.com/products/norton-family

Fuente: Propia

Dentro del control parental una recomendación importante para la seguridad es la utilización de los navegadores para niños recomendados hasta los 14 años, estos tienen la misma lógica que un navegador normal para adulto como es Google Chrome, Opera,

Mozilla Firefox entre otros es decir que pueden acceder a la búsqueda de información a través de los hipervínculos, la diferencia entre un navegador para adultos y otro para niños, es que esté ultimo bloquea links a enlaces no adecuados para la edad del menor de edad, es decir en el navegador viene con sus propios filtros para bloquear contenido no adecuado. Como todo lo que funciona a través del internet existen una variedad de opciones, solamente hay que indagar cual es la que se adapta mejor a nuestras necesidades. Algunos de los navegadores conocidos para menores de edad son: KidRex, Kids Search, Bunnis, Kiddle, Safe Search Kids.

Anthony Lake, Director Ejecutivo de UNICEF, en el año 2017 en en su disertación sobre Crecer en el mundo digital: Cómo internet afecta al bienestar y la seguridad de los niños dijo: “En un mundo digital, nuestro reto es doble: cómo mitigar los daños y a la vez maximizar los beneficios de internet para todos los niños”.

“Internet fue diseñado para adultos, pero los niños y los jóvenes lo utilizan cada vez más, y la tecnología digital afecta cada vez más sus vidas y su futuro. Por ello, las políticas, las prácticas y los productos digitales deberían reflejar mejor las necesidades, las perspectivas y las opiniones de los niños”.

5.3 Plataforma interactiva

El autor del presente trabajo además ha desarrollado una plataforma interactiva en línea con el fin de ayudar al conocimiento de la seguridad informática y los riesgos digitales a los que se encuentran expuestos los adolescentes, recordemos que mientras más se conozca sobre el tema nos encontraremos menos expuestos.

La plataforma interactiva en línea se encuentra en la dirección https://seguridadinformaticarcn.com/rcn/web20/web/web.htm, se puede acceder a través de cualquier navegador o incluso por un teléfono inteligente, pero para aprovechar de mejor manera todos sus juegos y material didáctico se recomienda hacerlo a través de un computador y se debe tener acceso a internet.

La pantalla principal de la plataforma en línea consta de un libro digital y un Menú, navegando por el libro digital se puede aprender de manera divertida sobre los

diferentes riesgos digitales a los que se encuentran expuestos los adolescentes. Además en las diferentes páginas de libro encontrarás gráficos, videos y acceso a diferentes enlaces sobre estudios hechos por organizaciones a nivel mundial sobre el tema en mención. Sin duda la plataforma interactiva es una forma interesante de aprender sobre la seguridad informática para adolescentes. En la ilustración que se muestra a continuación se puede ver la página principal de la aplicación.

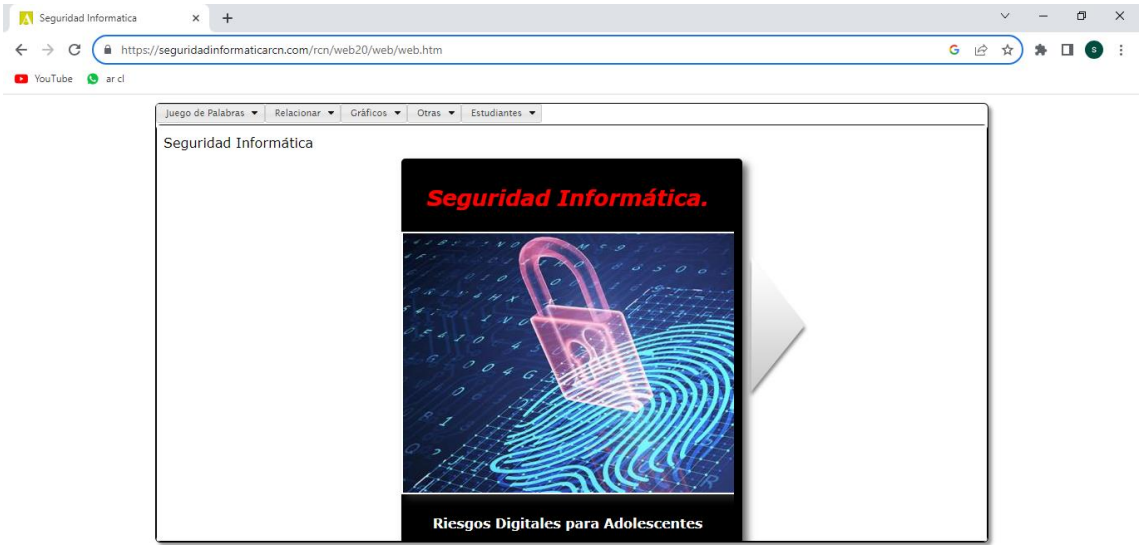

Figura 35. Pantalla principal de la aplicación interactiva en línea

Además del libro digital en la plataforma encontrarás un Menú que se encuentra agrupado por diferentes tipos de material didáctico donde podrás jugar, disfrutar y aprender sobre los riesgos digitales. El material didáctico se encuentra agrupado de la siguiente manera:

- Juego de Palabras.- donde podrás jugar diferentes opciones como son el ahorcado, sopa de letras y construye palabras.
- Relacionar.- donde podrás realizar actividades como juego de memoria, asociar una imagen con una palabra, juntar diferentes términos con sus definiciones a través de gráficas y completar definiciones sobre riesgos con las palabras adecuadas.
- Gráficos.- donde tendrás la opción de armar un rompecabezas sobre un riesgo digital y de asociar las fotos de diferentes riesgos digitales a través de las palabras.

- Otras.- tenemos una pizarra colaborativa que te permite jugar con definiciones, gráficos, texto, aumentar el tamaño de cada uno, cambiar de colores, trabajar de manera colaborativa con otros compañeros mientras aprendes sobre la seguridad informática y también la opción de resolver un test con veinte preguntas sobre seguridad informática y riesgos digitales.
- Estudiantes.- Está es la parte documental de la plataforma, podrás descargarte un archivo en formato pdf con estrategias de seguridad para todos los involucrados en el proceso de enseñanza aprendizaje (padres, estudiantes, docentes y autoridades), sin duda si sigues estás recomendaciones podrás disfrutar de todos los beneficios que brinda la tecnología con mayor seguridad. Otra opción importante es el formulario donde puede llenar una encuesta para evaluar todos tus conocimientos sobre el tema. Y finalmente la última opción es el control de estudiantes que está dedicado para el docente, al cual no podrás acceder sin el usuario o clave respectiva y es una ayuda para el docente para revisar el avance en los diferentes tema de la plataforma en línea.

Al ingresar a los diferentes opciones de material didáctico dispones de una explicación clara de como funciona cada uno de ellos, esto con el fin de que puedas disfrutar de la plataforma de la manera más sencilla posible. En la siguiente ilustración se puede observar un ejemplo de lo anotado en el presente párrafo:

Figura 36. Captura de pantalla del Juego de Memoria

Como se puede observar en la ilustración en el encabezado del material lúdico se explica como jugarlo, cual es el objetivo y el tiempo que se dispone para la actividad. Es la lógica aplicada a las diferentes actividades.

La plataforma interactiva en línea está disponible para todas las personas que requieran aprender sobre el tema, tiene su propio dominio seguridadinformaticarcn.com, se espera que sea un aporte dentro del proceso de enseñanza aprendizaje para todos los involucrados en el tema, porque como ya se ha mencionado antes en este documento, mientras mas conozcamos acerca de la seguridad informática podremos disfrutar de mejora manera de las bondades que nos brinda la tecnología minimizando los riesgos digitales.

CAPITULO VI
CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Para implementar una plataforma digital en línea es necesario seguir una metodología que en nuestro caso implico desarrollar la teoría en base al marco teórico, definir el material didáctico que se va a desarrollar en base a los temas a tratar, escoger un entorno de desarrollo integrado (IDE) para la plataforma, diseñar y desarrollar la plataforma, obtener un dominio (seguridadinformaticarcn.com) y un webhosting para subir la plataforma en línea, es decir no se trata solamente de elaborar un software, existe un soporte importante pre software que ayudan con el éxito de cualquier plataforma tecnológica.
- Toda plataforma tecnológica requiere de un proceso de capacitación para permitir un uso adecuado de la misma.
- Para implementar la plataforma tecnológica en línea, se requirió la aprobación de las autoridades de la institución y un adecuado proceso de inducción con el responsable de las TICS, para que sea aceptado de mejor manera por los estudiantes, además para el correcto uso de la misma se necesita de una conexión estable a internet.
- El estudio fue realizado en los estudiantes de tercero de bachillerato del colegio UTN, sin embargo la plataforma se encuentra disponible en línea para cualquier persona que quiera aprender más sobre seguridad informática y los riesgos digitales que corren los adolescentes. Para acceder a la plataforma se lo puede hacer con cualquier digitando la dirección https://seguridadinformaticarcn.com/rcn/web20/web/web.htm
- En cada una de las preguntas aplicadas en el estudio, el porcentaje de respuestas correctas aumentó en la post evaluación es decir a partir de que el estudiante trabajó en la plataforma en línea.
- En los estudiantes encuestados se observa que entienden de mejor manera cuando las preguntas se tratan de definiciones puesto que los porcentajes de respuesta correcta siempre superaron el 50 por ciento en cualquier pregunta referente a lo

que significa un riesgo digital, con el uso de la plataforma los porcentajes subieron sobre el 75 por ciento llegando en algunos casos incluso a superar el 90 por ciento.

- A los estudiantes objeto del estudio realizado les cuesta mucho más entender a qué riesgo digital corresponde un determinado caso, cuando las preguntas se trataban sobre este tema en promedio las respuestas correctas estaban en el 35 por ciento y con el uso de la plataforma en línea el porcentaje de respuestas correctas en estos casos subió al 65 por ciento. En todos los caso sin embargo como ya se mencionó el uso de la plataforma mejoró ostensiblemente el porcentaje de respuestas correctas.
- En la encuesta aplicada había una pregunta referente a los actores del proceso de seguridad informática en el proceso de enseñanza aprendizaje, este caso era especial porque no tenía material lúdico para aprender dentro de la plataforma, lo que había es un documento en formato pdf que había que leerlo para obtener la respuesta correcta, en el entorno encuestado esta pregunta tuvo un comportamiento diferente puesto que el porcentaje de respuestas correcta prácticamente fue el mismo en la pre y post evaluación, lo que nos lleva a concluir que el estudiante al menos en el universo en mención prefiere aprender jugando, no gusta mucho o evita cuando tiene una plataforma tecnológica la lectura de documentos.
- Los estudiantes son receptivos para aprender sobre nuevos temas a través de la tecnología.

6.2 Recomendaciones

- Para que una institución pueda implementar soluciones tecnológicas dentro del proceso de enseñanza aprendizaje debe existir la decisión de las autoridades quienes deberán liderar este tipo de procesos, no pueden ser soluciones aisladas dentro de una aula de clases, debe ser una visión estratégica que permita cambiar la forma de enseñanza dentro de una institución.
- En la plataforma en línea existe un tipo de reporte para los estudiantes con usuario y contraseña para determinar el avance del estudiante en el manejo del material didáctico, este control se lo hace a través de archivos planos, se puede plantear un nuevo proyecto que permita cambiar está parte de la plataforma en línea con manejo de base de datos que brinda muchas otras posibilidades de control. Esto es posible porque la plataforma pertenece a la Universidad Técnica del Norte.
- Antes de desarrollar cualquier solución tecnológica es necesario realizar un estudio de factibilidad para determinar si la misma va a poder ser implementada dentro de la institución, es decir si cuenta con los recursos de hardware, software y económicos para el correcto funcionamiento.
- En la actualidad existe una serie de entorno de desarrollo integrado (IDE) para docentes para elaboración de material lúdico, estos brindan la facilidad de que no se requiere saber de programación para crear cierto tipo de plataforma tecnológica, pienso que en base a todo esto se debería analizar la posibilidad de un nuevo tipo de docente con una capacitación más enfocada a la tecnología, acorde a los nuevos tiempos pues como dijo Ian Jukes profesor, administrador, escritor, consultor, instructor universitario y director de InfoSavvy21 “Tenemos que preparar a nuestros estudiantes para su futuro, no para nuestro pasado”

ANEXOS

Metodología utilizada para el desarrollo de la plataforma

Para el desarrollo de la plataforma tecnológica se utilizará la metodología de Kendall y Kendall explicada en su libro Análisis y Diseño de Sistemas del año 2005.

La plataforma tecnológica en línea a desarrollar no es propiamente la construcción de un sistema transaccional, sin embargo adaptaremos la metodología para el desarrollo de la plataforma.

La metodología consta de las siguientes fases:

- Análisis.- Incluye la detección de las necesidades en base a los objetivos planteados y los requerimientos para llevar a cabo la construcción de la plataforma.
- Diseño.- De las diferentes pantallas con las opciones que tendrá la plataforma, el tipo de menú y los materiales didácticos a desarrollar, en esta fase se tendrá una idea bastante clara de la plataforma en cuanto al funcionamiento. Es el sistema en planos.
- Desarrollo.- Construcción de la plataforma en un software adecuado para la misma.
- Pruebas.- Previo a sacar la plataforma en línea se realizarán las pruebas necesarias para comprobar el correcto funcionamiento de la plataforma.
- Implementación.- Plataforma en línea, a la cual se puede acceder desde una dirección URL.

Análisis

Introducción

Para el desarrollo del presente trabajo debemos recordar los tres objetivos planteados en nuestra investigación.

Objetivo No. 1: Recopilar bases teóricas y conceptuales, definiciones, trabajos acerca de la problemática de la seguridad informática con especial énfasis en la educación.

Objetivo No. 2: Desarrollar estrategias didácticas en una plataforma tecnológica interactivasobre seguridad informática dirigido a estudiantes de tercero de bachillerato

Objetivo No. 3 : Evaluar el impacto de la implementación de la herramienta tecnológica.

El objetivo No.1 está cubierto en el Capítulo II del presente trabajo donde se realizó la búsqueda de la información en base a consultas en libros, artículos científicos, revistas de investigación, entre otras. En este capítulo se desarrolló una introducción al tema de la seguridad informática a través de las diferentes aplicaciones que se pueden utilizar con internet, luego se realizó una explicación de lo que es el internet como tal para adentrarnos en el mundo de los riesgos digitales a los que se encuentran expuestos los menores de edad en general y los adolescentes en particular, una vez analizado este tema se procedió a realizar recomendaciones para trabajar de una manera segura en el internet y aprender a disfrutar de las bondades que nos brinda esta herramienta y finalmente se explicó el control parental que es una de las estrategias para mejorar la navegación del internet minimizando los riesgos. Otro aspecto que se explico es el marco legal, pero este acápite no forma parte de la construcción de la plataforma.

En esta etapa otro punto importante que se debe considerar es la elección del entorno de desarrollo donde se va a llevar a cabo la construcción de la plataforma tecnológica, para lo cual se analizará tres entornos de desarrollo que permitan implementar soluciones didácticas.

Herramientas didácticas

Wordwall.- Es una herramienta que permite crear recursos didácticos para clases a través de plantillas preestablecidas. Tiene 18 plantillas a las que se puede acceder sin costo para realizar actividades como crucigramas, juego de parejas, puzzle, ordenamiento, sopa de letras entre otras. Se puede acceder a los 18 recursos pero en la versión gratuita solo se pueden desarrollar 5.

Para utilizar WordWall se requiere realizar un registro para lo cual es necesario disponer

de un correo electrónico y para poder utilizar todas las características se requiere realizar un pago. Todos los recursos son preestablecidos, no existen opciones importantes de modificación de los recursos. Estos recursos es posible incrustarlos en un sitio web aunque no disponen los drivers para un servidor web propiamente dicho.

Ardora.- Es un software español que al igual que Wordwall permite la creación de recursos didácticos. En la página oficial de Ardora textualmente dice "El programa Ardora es totalmente gratuito, siempre y cuando sea usado de forma personal, sin carácter lucrativo y con fines estrictamente educativos". El software ardora está bajo licencia Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Ardora mantiene documentación abundante para desarrollar los diferentes tipos de materiales didácticos y con el mismo se pueden crear diferentes recursos desde los más simples como crucigramas, puzzle, juego de parejas, ordenamiento hasta más complejos como páginas multimedia y páginas en el servidor. Todo lo desarrollado se puede montar en un servidor web con los drivers y configuraciones apropiadas. En total se pueden desarrollar más de 40 actividades de diferente índole agrupadas en diferentes categorías como son juego de palabras, actividades con gráficos, ordenar, completar, seleccionar, cálculo, páginas multimedia, páginas web entre otras.

Además está desarrollado en lenguaje de programación Java, y las librerías están disponibles lo que permite personalizar cada una de las aplicaciones y aumentar algunos recursos didáctico si el caso lo amerita.

JCLIC.-Es una aplicación desarrollada en JAVA, es un proyecto de código abierto que funciona en diferentes sistemas operativos. En la aplicación se puede desarrollar diferentes recursos didácticos como son rompecabezas, asociaciones, palabras cruzadas entre otras. Está formado por cuatro componentes Applet, player, autor y reports.

- JClic Applet.- permite insertar actividades en una página web.
- JClic Player.- permite realizar actividades desde el computador, sin estar conectado en línea.
- JClic Author.- permite crear, editar y publicar de una manera atractiva mejorando su interfaz visual.
- JClic Report.- informes de las actividades desarrolladas por los estudiantes.

Funciona bajo licencia pública general de GNU (GPL).

La principal desventaja de este software es que si bien posee documentación abundante

no es en sí de la aplicación sino de proyectos desarrollados en la aplicación, motivo por el cual es más complicado el desarrollo de los recursos didácticos. Por el tipo de licencias tiene muchas fuentes de información y muchas herramientas para desarrollar recursos que se han adaptado a la herramienta principal, pero su estudio y análisis se hace mas complejo. Se requiere muchos conocimientos de la herramientas JAVA.

Evaluación del software

El objetivo del trabajo de investigación es elaborar los recursos didácticos para aprender sobre los riesgos digitales en los adolescentes, por este motivo nos hemos centrado en tres entornos de desarrollo que son Wordwall, Ardora y Jclic, si bien existen un sinfín de herramientas que nos permiten desarrollar recursos didácticos hemos considerado estás tres para someterles a un criterio de evaluación y poder decidir con que herramienta vamos a realizar la plataforma en línea.

La evaluación lo haremos tomando como referencia la metodología explicada por Cabero y Duarte (1999), en cuanto se refiere al punto de evaluación Características y potencialidades tecnológicas.

Característica	Wordwall	Ardora	Jclic
Plataforma para funcionar en línea	X	X	X
Permite generar código para montar sobre un servidor web con dominio propio		X	X
Multiplataforma		X	X
Tipo de licencia Detallar los tipos de licencia	Privativo	CC BY-NC-ND 4.0	GNU
Documentación de desarrollo		X	X
Requiere conocimientos básicos de programación para realizar cambios en las plantillas		X	X
Requiere conocimientos avanzados de programación para realizar cambios en las plantillas			X
Permite la creación de proyectos a partir de plantillas	X	X	X
Impresión de reportes	X	X	X

Diseño

En base a la información recopilada en la parte documental con el marco teórico se

desarrollará diferentes tipos de riesgos informáticos a los que se encuentran expuestos los adolescentes en general.

En esta etapa se considerará la interfaz de usuario como parte del diseño lógico de la aplicación, la interfaz conecta al usuario con la aplicación por lo tanto es un paso sumamente importante.

En el diseño también se determinará que estrategias didácticas se utilizarán en la aplicación en línea, por ejemplo se puede determinar si se utilizará libros digitales, crucigramas, videos, sopa de letras, entre otros y como se conectarán en interactuarán con el usuario las diferentes estrategias didácticas, se determinará si la aplicación en línea será de libre acceso o se requerirá de usuario y contraseña.

Otro de los aspectos que se analizará en esta fase son diferentes tipos de herramientas open source en las que se pueda desarrollar diferentes tipos de material didáctico que disponga de espacios webs, repositorios multimedia, gestión de usuarios, escritorios virtuales para permitir dos tipos de acceso el público y el privador (Con usuario y contraseña) y que se permita montar en un servidor web para que la aplicación este en línea.

Dentro del material propiamente a desarrollar deberá permitir el desarrollo de libros digitales, juegos de palabras, relaciones, cálculos, actividades con gráficos, páginas multimedia y otro tipo de actividades.

Una vez escogida la herramienta para desarrollar la aplicación interactiva en línea, se empezará con el proceso de desarrollo de los diferentes materiales a utilizar para aprender de una manera interactiva los riesgos informáticos existentes dentro de un proceso de enseñanza aprendizaje.

Se hará un diseño de la plataforma y la construcción de un prototipo para pasar a las siguientes etapas del ciclo de desarrollo de sistemas y finalmente desarrollar la aplicación final.

Desarrollo

La siguiente fase del ciclo de vida de los sistemas de información es el desarrollo el cual consiste en base a todos los requerimientos recopilados en las fases anteriores realizar la aplicación propiamente dicha en el IDE escogido para tal efecto.

Un aspecto a considerar es la obtención de un dominio web, y la aplicación se montará dentro de un servidor web para que la misma se encuentre en línea con una disponibilidad de 99.6 %.

Pruebas

Antes de colocar la aplicación para el usuario final se deben realizar diferentes pruebas con el fin de probar el correcto funcionamiento de la aplicación. Para esto se debe manejar un adecuado banco de datos y simular las diferentes probabilidades que puede tener el usuario al trabajar con la aplicación y que errores se presentan para proceder a corregirlos.

El banco de datos debe ser adecuado para evitar que se produzcan errores cuando la aplicación ya se encuentre implementada.

Implementación y evaluación

Después de haber cumplido todas las fases del ciclo de vida del desarrollo de sistemas estamos en condiciones de implementar la plataforma tecnológica interactiva la misma estará disponible en línea permitiendo dos tipos de acceso uno público sin ningún tipo de restricciones para cualquier usuario en la web que esté interesado en el tema y un privadoa través de usuario y contraseña para un número reducido de usuarios de tercero de bachillerato. Con estos usuarios se determinará preevaluación para saber cuanto saben sobre seguridad informática y sus riesgos digitales y luego una post evaluación después de haber trabajado sobre la plataforma digital, el tipo de contenido responde a los requerimientos de los usuarios entre los aspectos más importantes. Para proceder a realizar la evaluación se utilizará como herramienta la encuesta con los estudiantes previamente seleccionados.

A los estudiantes participantes en la evaluación de la plataforma, se les informará de forma oral, los aspectos más relevantes de la investigación: objetivos, procedimientos, la importancia de su participación, tiempo de duración aproximada de la encuesta, leyes, códigos y normas que lo amparan, el carácter voluntario en la

participación y beneficios. Así mismo se tramitarán todos los permisos respectivos para tener acceso a la comunidad educativa y se respetará el anonimato de los involucrados.

La metodología propuesta en el presente documento para llegar a la implementación de la plataforma tecnológica es la de Kenneth Kendall y Julie Kendall en su libro Análisis y Diseño de sistemas, sexta edición.

Referencias

Aguirre Giraldo, C. A., & Rojas Riascos, K. J. (2021). *El Cibersexo en mujeres universitarias del distrito de buenaventura.*

Alcántara, M. (2019). *Palabras invasoras, el español de las nuevas tecnologías.* UAM Ediciones. España. https://bit.ly/2BTZAYQ

Alonso Mezarina, N., & Orcon Abregu, X. M. (2022). *Sexting y autoestima en estudiantes de una universidad privada de Lima Norte*.

Álvaro Cabrera, E. (2022). *Bullying y Ciberbullying en adolescentes de Educación Secundaria Obligatoria: incidencia y variables sociales asociadas.*

Alvites-Huamaní, C. G. (2019). *Adolescencia, ciberbullying y depresión, riesgos en un mundo globalizado.* Etic@ net: Revista científica electrónica de Educación y Comunicación en la Sociedad del Conocimiento, 19(1), 210-234.

Arab, L. E., & Díaz, G. A. (2015). *Impacto de las redes sociales e internet en la adolescencia: aspectos positivos y negativos.* Revista Médica Clínica Las Condes, 26(1), 7-13.

Arango Gomez, O. D. (2023). *El ABC de la seguridad informática: guía práctica para entender la seguridad digital.* https://www. autoreseditores. com/libro/22997/oscar-dario-arango-gomez/el-abc-de-la-seguridad-informatica-guia-practica-para-entender.

Arias, V. (2019). *Sexting: Nuevas prácticas de exhibición sexual en medios digitales.* ECOS-Estudos Contemporâneos da Subjetividade, 9(1), 4-16.

Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019). *Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad.* Revista Electrónica Educare, 23(3), 339-362.

Barreiro Herrera, D. A.(2020). *Detección de phishing en etapa de detección temprana utilizando características relacionadas a la marca afectada*. (Doctoral dissertation, Universidad Nacional de Colombia).

Barroso Beltri, V. (2021). *Análisis y Simulación de un Ataque de Phishing* (Bachelor's thesis, Universitat Politècnica de Catalunya).

Basante, M. A. C. (2020). *Riesgos digitales*. Revista Universitaria de Informática RUNIN, 7(10), 64-69.

Bastidas Jácome, C. D., & Paredes Sevillano, F. E. (2022). *Prototipo de un sistema anti-phishing basado en herramientas open source o de bajo costo para la Empresa Intercommerce SA* (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones).

Bojorquez Huanca, J. S. (2022). *Ciberseguridad.*

Cabero Almenara, J., & Duarte Hueros, A. M. (1999). *Evaluación de medios y materiales de enseñanza en soporte multimedia.* Pixel-Bit.

Calvete, E., Orue, I., & Gámez-Guadi, M. (2022). *Una intervención preventiva para reducir el riesgo de grooming online entre los adolescentes.* Psychosocial Intervention, 31(3), 177-184.

Calvo, J. C., Arnal, R. B., Llario, M. D. G., Mengual, V. M., & Sanchez, P. S. (2014). *Internet, cibersexo y consumo de alcohol: estudio preliminar en adolescentes.* International Journal of Developmental and Educational Psychology, 1(1), 507-515.

Cano Vázquez, P. (2020). *Aplicación P2P de comunicación y organización de grupos con compartición de ficheros.*

Cantos Agudo, J. C. (2020). *Red P2P centralizada para el streaming de vídeo almacenado*. (Doctoral dissertation, Universitat Politécnica de Valencia)

Castaño Duque, M. R. (2020). *Impacto del esquema del mercado P2P en el mercado eléctrico colombiano.*

Cardozo, G., Dubini, P., & Lorenzino, L. (2017). *Bullying y ciberbullying: un estudio comparativo con adolescentes escolarizados*. Revista Mexicana de Psicología, 34(2), 101-109.

Choi, HJ, Mori, C., Van Ouytsel, J., Madigan, S. y Temple, JR (2019). *Participación de adolescentes en sexting durante 4 años y asociaciones con la actividad sexual.* Diario de Salud Adolescente, 65 *(6), 738 - 744. https://doi.org/10.1016/j.jadohealth.2019.04.026*

Código de la niñez y adolescencia (Julio 2003)

Contreras, C. T. M., & Herrera, A. D. R. C. (2017). *Sexting practicado por adolescentes: su morfología en Facebook.* International Journal of Developmental and Educational Psychology, 2(1), 197-209.

Coronel Rojas, C. I. (2018). *Seguridad en los niños mediante herramientas de control parental que permita a los padres supervisar el uso de internet.* (Doctoral dissertation).

Corral, E. M. (2011). *El videojuego y las nuevas tendencias que presentan al mercado de la comunicación*. Anuario electrónico de estudios en Comunicación Social" Disertaciones", 4(2), 36-54.

Demartini, M. V. N., & Ríos, M. J. (2019). *El impacto generado por la seguridad informática en las PYMES de Mendoza.* (Doctoral dissertation, Universidad Nacional de Cuyo. Facultad de Ciencias Económicas).

Echeburúa, E. y De Corral, P. (2010). *Adicción a las nuevas tecnologías y a las redes sociales en jóvenes: Un nuevo reto.* Adicciones, 22*(2), 91-96. doi: 10.20882/adicciones.196*

Echeburua, E., Corral, P. y Amor, P.J. (2005). *El reto de las nuevas adicciones: objetivos terapeuticos y vias de intervencion.* Psicología Conductual, 13, 511-525.

Espinoza Guamán, E. E., Cruz Yaguachi, L. N., & Espinoza Freire, E. E. (2018). *Las redes sociales y rendimiento académico*. Revista Metropolitana de Ciencias Aplicadas, 1(3), 38-44. Recuperado de http://remca.umet.edu.ec/index.php/REMCA

Estiarte, C. V. (2017). *Predadores sexuales online y menores: grooming y sexting en adolescentes. e-Eguzkilore, (2).*

Farber, B. A., Shafron G., Hamadani J., Wald E., y Nitzburg G. (2012). *Children, Technology, Problems, and Preferences. Wiley Periodicals,* Inc., Journal of Clinical Psychology: In Session, 68 (11), 1225–1229. http://dx.doi.org/10.1002/jclp.21922

Garay, R., Ochoa, G., Cantero, F., & Ramos, N. (2012). *Violencia, Victimización y Cyberbullying en adolescentes escolarizados/as: una perspectiva desde el Trabajo Social.*

García-Barba, M., Nebot-Garcia, J. E., & Giménez-García, C. (2019). *Conductas sexuales de riesgo y uso del cibersexo. Comparación entre diferentes perfiles de uso del cibersexo.*

García-Piña, C. A. (2008). *Riesgos del uso de internet por niños y adolescentes. Estrategias de seguridad.* Acta pediátrica de México, 29(5), 272-278.

Guaña-Moya, J., Chiluisa-Chiluisa, M. A., del Carmen Jaramillo-Flores, P., Naranjo-Villota, D., Mora-Zambrano, E. R., & Larrea-Torres, L. G. (2022). *Ataques de phishing y cómo prevenirlos Phishing attacks and how to prevent them.* In *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE.

Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., Jaramillo-Flores, P., & Pillajo-Rea, C. (2022). *Ataques informáticos más comunes en el mundo digitalizado.* Revista Ibérica de Sistemas y Tecnologías de Información, (E54), Pag. 87-100.

González Londoño, J. (2020*). Estudio del estado actual de la seguridad informática en las organizaciones de Colombia.*

Hernández, G. M., & Castro, P. Á. (2014). *Influencia de las redes sociales de internet en el rendimiento académico del área de informática en los estudiantes de los grados 8° y 9° del instituto promoción social del norte de Bucaramanga.* (Trabajo de grado para optar el título de Magister en Educación). Ibagué: Universidad de Tolima.

IBM, K. (2022). Ciberseguridad concepto, tipos, amenazas y estrategias.

Kendall, K. E., & Kendall, J. E. (2005). *Análisis y diseño de sistemas*. Pearson educación.

Lachaise, S. M., & Massa, A. (2022). *Hablemos sobre grooming.* Perspectivas, (6)

Lardies, F., & Potes, M. V. (2022). *Redes sociales e identidad:¿desafío adolescente?* Avances en Psicología, 30(1), e2528-e2528.

Lizarraga, J. R. P., Hernández, J. A. L., Garay, M. A. B., Navarro, A. F., & Espinoza, D. E. F. (2019). *Protocolo para la prevención de ataques de phishing*. Revista Digital de Tecnologías Informáticas y Sistemas, 3(3).

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (1999). *Una breve historia de Internet.* Primera y segunda parte, en: http://www. ati. es/DOCS/internet/histint/histint1. html.

Lira Oscar M. (2019). *Ciberdelitos perspectiva para su persecución.* (Primera ed, Vol. 0). Tirant lo Blanch.

López Pérez, E. (2022). *Redes P2P y ciberdelincuencia.*

Masaquiza Sailema, L. V. (2021). *El phishing como delito informático en la legislación Ecuatoriana*. (Bachelor's thesis).

Melamud, A., Otero, P., Nasanovsky, J., Stechina, D., Goldfarb, G., Svetliza, J., ... & Ringuelet, L. (2007). *Los niños, sus padres, Internet y los pediatras*. Archivos Argentinos de Pediatría, 105(4), 368-371.

Mercado Contreras, C. T., Pedraza Cabrera, F. J., & Martínez Martínez, K. I. (2016). *Sexting: su definición, factores de riesgo y consecuencias*. Revista sobre la infancia y la adolescencia, (10), 1-18.

Miguel Asensio, P. A. (2022). *Derecho privado de Internet*. ARANZADI/CIVITAS.

Ministerio de Sani Guilford Press. dad, Consumo y Bienestar Social. (2017 Adicciones.2024). *Estrategia Nacional sobre adicciones*.

Montalvo, J.; Peñalva, A. y Itziar, I.(2015) *Hábitos de uso y conductas de riesgo en Internet en la preadolescencia*. Comunicar, 22: 44 (2015): 113-120.

Montiel-Bueno, G. (2022). *Programa de prevención de la adicción a juegos virtuales en adolescentes.*

Murillo Agudelo, A. I. (2022). *Influencia de las redes sociales en el autoconcepto físico en adolescentes.*

Oficina de las Naciones Unidas contra la droga y el delito

Ospina, M. (2022). *Sistemas distribuidos, escalabilidad y distribución de los datos.*

Pérez Tornero, J. M. (2017). *Aprender valores con internet. Cómo potenciar la ética, el respeto, la tolerancia y la cooperación en internet*. Octaedro

Prensky, M. (2001). *Digital natives, digital immigrants part 2: Do they really think differently?. On the horizon*.

Revista Latinoamericana de Estudios de Seguridad No. 20 (Junio del 2017)

Rivera Arteaga, E., & Torres Cosío, V. (2018). *Videojuegos y habilidades del pensamiento.* Ride. Revista Iberoamericana para la investigación y el desarrollo educativo, 8(16), 267-288.

Romero Castro M, Figueroa Morán G. Vera Navarrete D. Álava Cruzatty J. Parrales Anzúles G. Álava Mero C. Murillo Quimiz A. Castillo Merino M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*

Romo, B. A. (2018). *Ventajas y Desventajas de las Redes Sociales en 2018.* NeoAttack. Recuperado de https://neoattack.com/ventajas-y-desventajas-de-las-redes-sociales/

Rosas Murcia, A. G. (2021). *Percepción del cibersexo desde un contexto sociocultural.*

Ruiz, M. S. (2022) *Maltrato de la población adolescente a través de las TICS (grooming, sexting, ciberbullying).*.

Salinas, M. G. T. (2019). *Internet como servicio público. INGENIO*, *1*(2), 15-30.

Sánchez-Teruel, D., & Robles-Bello, M. A. (2016). *Riesgos y potencialidades de la era digital para la infancia y la adolescencia.* Educación y Humanismo, 18(31), 186-204.

Santisteban, P. y Gámez, M. (2017*). Online Grooming y Explotación Sexual de Menores a Través de Internet.* Revista de Victimología num 6 (2017): 81-100.

Sisti, M. A., & Majowka, P. D. (2019). *Seguridad Informática: La Protección de la Información en una Empresa Vitivinícola de Mendoza, 2019.*

Solórzano Alcívar, N., Moscoso Poveda, S., & Elizalde Ríos, E. (2019). *Evolución de Videojuegos y su Línea Gráfica _ un enfoque entre la Estética y la Tecnología*. Ñawi: arte diseño comunicación, 3(2), 125-145.

Subijana Zunzunegui, Ignacio José. (2008) *El ciberterrorismo: Una perspectiva legal y judicial*. Eguzkilore, 22 (2008): 169-187. http://www.ehu.eus/documents/1736829 /2176658/08+Subijana.indd.pdf.

Tamayo, D. L. O., & Otero, K. L. M. (2020). *Adolescentes en Internet: la mediación entre riesgos y oportunidades.* Revista Colombiana de Ciencias Sociales, 11(1), 153-180.

Trucco, D. (2014). *Educación y desigualdad en América Latina.*

UNICEF(2017) *Crecer en el mundo digital: Cómo internet afecta al bienestar y la seguridad de los niños.*

Valle Matute, J. C. (2013). *El delito informático de Phishing* (Master's thesis).

Villota García, S. C., Zamora López, G. G., & Llanga Vargas, E. F. (2019). *Uso del internet como base para el aprendizaje.* Atlante Cuadernos de Educación y Desarrollo, (mayo).

Villacís B., Carrillo D. (2012) *País atrevido: la nueva cara sociodemográfica del Ecuador*. Edicón especial revista Analitika. Instituto Nacional de Estadística y Censos (INEC).

Zambrano, W. R., García, V. H. M., & García, A. V. M. (2010). *Nuevo rol del profesor y del estudiante en la educación virtual.* Dialéctica: Revista de investigación, (26), 51-62.