| Artículo de reflexión | Reflection paper I Artigo de reflexão I

Análisis de la ciberseguridad en espacios educativos pertenecientes a la Fuerza Aeroespacial Colombiana*

Fecha de recibido: 28 de junio 2023	Fecha de aprobado: 16 de septiembre 2023
Reception date: June 28, 2023	Approval date: September 16, 2023
Data de recebimento: 28 de junho de 2023	Data de aprovação: 16 de setembro de 2023

Jaquelin Castillo García
https://orcid.org/0000-0002-4821-3991
jaquelin.castillo@epfac.edu.co

Magíster en Dirección y Gestión de la Seguridad Integral
Docente - Escuela de Posgrados de la Fuerza Aeroespacial Colombiana, Colombia
Rol del investigador: teórico y escritura
Grupo de investigación en Seguridad Integral, Inteligencia y Ciberdefensa -GISIC

Master in Integral Safety Management and Direction
Professor - Graduate School of the Colombian Aerospace Force, Colombia
Researcher's role: theorist and writer
Integrated Security, Intelligence and Cyber Defense Research Group -GISIC

Mestre em Gestão e Direção Integral de Segurança
Docente - Escola de Graduação da Força Aeroespacial Colombiana, Colômbia
Função do pesquisador: teórico e redação
Grupo de Investigação em Segurança Integrada, Inteligência e Ciberdefesa -GISIC

* Este es un artículo de reflexión derivado del proyecto titulado: "Propuesta de lineamientos en ciberseguridad para la institución educativa Gimnasio Militar de la Fuerza Aeroespacial Colombiana", el cual está enfocado desde la perspectiva institucional de la ciberseguridad al interior de dicha institución. El presente proyecto fue realizado por la autora para optar al título de magíster en Dirección y Gestión de la Seguridad Integral, con el fin de apoyar el proceso formativo de la comunidad educativa del Gimnasio Militar de la Fuerza Aeroespacial Colombiana, en Bogotá, Colombia.

Cómo citar este artículo: Castillo García, J. (2023). Análisis de la ciberseguridad en espacios educativos pertenecientes a la Fuerza Aeroespacial Colombiana. *Ciencia y Poder Aéreo*, *19*(1), 137-151. https://doi.org/10.18667/cienciaypoderaereo.803

Análisis de la ciberseguridad en espacios educativos pertenecientes a la Fuerza Aeroespacial Colombiana

Resumen: El presente artículo de reflexión está basado en la investigación que se centró en el desarrollo de una propuesta que permitió fortalecer la responsabilidad en ciberseguridad desde una perspectiva institucional, específicamente en el Gimnasio Militar de la Fuerza Aeroespacial Colombiana (GIMFA), teniendo en cuenta los lineamientos estratégicos como herramientas de apoyo y complemento al modelo educativo, cumpliendo con el objetivo de identificar y analizar las categorías que están asociadas a los riesgos y las amenazas en la comunidad educativa, que resultaron ser factores determinantes en la formación y sensibilización de la ciberseguridad en espacios como el educativo.

Palabras clave: ciberseguridad; educación; criminalidad cibernética; riesgos de ciberseguridad; amenazas de ciberseguridad; tecnologías de la información.

Cybersecurity guidelines in high education institutions of the Colombian Aerospace Force**

Summary: This reflection article is based on research that focused on the development of a proposal that could strengthen responsibility in cybersecurity from an institutional perspective, specifically in the Military Gymnasium of the Colombian Aerospace Force (GIMFA), taking into account the guidelines strategies as support tools and complements to the educational model, fulfilling the objective of identifying and analyzing the categories that are associated with risks and threats in the educational community, which turned out to be determining factors in the training and awareness of cybersecurity in spaces like educational.

Keywords: Cybersecurity; education; cybercrime; cybersecurity risks; cybersecurity threats; information technology.

Diretrizes de cibersegurança em instituições de ensino alto da Força Aeroespacial Colombiana***

Resumo: Este artigo de reflexão é baseado em pesquisas que se concentraram no desenvolvimento de uma proposta que pudesse fortalecer a responsabilidade em segurança cibernética desde uma perspectiva institucional, especificamente no Ginásio Militar da Força Aeroespacial Colombiana (GIMFA), levando em conta as estratégias de diretrizes como ferramentas de apoio e complementa o modelo educativo, cumprindo o objetivo de identificar e analisar as categorias que estão associadas a riscos e ameaças na comunidade educativa, que se revelaram determinantes na formação e sensibilização para a cibersegurança em espaços como o educativo.

Palavras-chave: cibersegurança; educação; cibercrime; riscos de cibersegurança; ameaças de cibersegurança; tecnologia da informação.

** This is an article of reflection derived from the project entitled "Cybersecurity Guidelines Proposal for the Colombian Aerospace Force Military Gymnasium Educational Institution", which is focused from the institutional perspective of cybersecurity within the Military Gymnasium of the Colombian Aerospace Force educational institution. Colombian Aerospace Force. Said project was carried out by Defense Counselor 18, to obtain the title of Master in Direction and Management of Integral Security, in order to support the training process of the educational community of the Military Gymnasium of the Colombian Aerospace Force. Bogotá, Colombia

*** Este é um artigo de reflexão derivado do projeto intitulado: "Proposta de diretrizes de segurança cibernética para a instituição educacional Gimnasio Militar de la Fuerza Aérea Colombiana", que é focado a partir da perspetiva institucional da segurança cibernética dentro da instituição. Este projeto foi realizado pelo autor para a obtenção do grau de mestre em Gestão Integral da Segurança, com o objetivo de apoiar o processo de formação da comunidade educativa do Ginásio Militar da Força Aeroespacial Colombiana, em Bogotá, Colombia.

Introducción

Los seres humanos por naturaleza son sociables, requieren de interacciones con otras personas, lo cual les permite establecer las formas en que se comunican como sociedad. Con el paso del tiempo, los procesos sociales han variado acorde a las épocas que permitieron desarrollar, evolucionar y crear nuevas tecnologías que se implementan hoy en día para relacionarse; no obstante, la globalización ha sido fundamental para acelerar las dinámicas sociales en la que están inmersos desde el nuevo milenio.

Si bien el avance tecnológico ha constituido nuevas formas de comunicación, de aprendizaje, de diversión y, al mismo tiempo, influye en el cambio de la cotidianidad y la funcionalidad de la sociedad, ocupando un lugar en el ciberespacio a partir de la creación de un usuario y su contraseña; sin embargo, la criminalidad también habita allí, dando cabida a la vulnerabilidad de los derechos humanos desde la amenaza explícita o implícita, en la que estrategias como la ciberseguridad tienen relevancia al momento de combatir los ataques cibernéticos y digitales.

Actualmente, los dispositivos tecnológicos, las herramientas digitales, los sitios web, las aplicaciones y las redes sociales, rompieron las barreras del conocimiento, la interactividad, el aprendizaje y la comunicación sin importar quién sea o qué quiera hacer en el ciberespacio, ya que la existencia en este espectro tecnológico y digital ha permitido indagar el propósito con el que se utiliza, pero también, permite reflexionar sobre el uso correcto de todo este mundo.

La vulnerabilidad que se tiene en el espectro tecnológico y digital da paso a los delitos que surgen con la ingeniería social, según Monsalve (2018), se refiere a:

> La técnica de fraude con el propósito de obtener información confidencial, accesos o privilegios en sistemas de información a través de la manipulación de usuarios legítimos. La ingeniería social se basa en el principio 'los usuarios son el eslabón más débil' y aprovechan la tendencia natural de la gente a confiar y a reaccionar de manera predecible ante ciertas situaciones. (p. 3)

Así mismo, Monsalve (2018) explica que, al emplearse esta técnica, la ciberdelincuencia utiliza el *phishing* que, como resultado de la manipulación a los usuarios, a partir del engaño, obtienen información confidencial de forma fraudulenta; o el *baiting*, el cual emplean al suplantar sitios web legítimos o programas que simulan ser seguros mediante un *malware* para robar la información. "Los *malwares* son *softwares* con intenciones maliciosas, contienen virus o programas que se instalan sin el consentimiento de los usuarios para robar información" (Monsalve, 2018, p. 3).

Es allí donde surgen conceptos como la ciberseguridad y la seguridad de la información, como el resultado de los vacíos de esta nueva era tecnológica que está al servicio de la sociedad como respuesta a diferentes necesidades, pero que también ha logrado tener un impacto en las transformaciones en los ámbitos que vivimos en el día a día. Según Ospina y Sanabria (2020), la tecnología es considerada señal de progreso, sin embargo, ha generado problemas de dependencia tecnológica, lo que conlleva a la vulnerabilidad de la información.

Este artículo surge de la profunda reflexión del trabajo de grado, titulado: *Propuesta de lineamientos en ciberseguridad para la institución educativa Gimnasio Militar de la Fuerza Aeroespacial Colombiana*, que tuvo como respuesta la identificación de los riesgos y las amenazas que están expuestas las instituciones educativas e integrantes de esta comunidad en el ciberespacio, a partir de la formación imperante, responsable y su sensibilización en ciberseguridad de manera integral.

El problema de la ciberseguridad

Si bien el tema de las nuevas tecnologías de la información representa un avance y también una potencial fuente de vulneración gracias a los vacíos que se presentan en el espectro tecnológico y digital, la criminalidad encuentra técnicas delictivas empleando ciberataques, teniendo un nicho detectado en la sociedad, con el fin de obtener información personal o económica que les resulta beneficioso.

Nuevamente Monsalve (2018), en su artículo *Ciberseguridad: principales amenazas en Colombia (ingeniería social, phishing y DOS),* ejemplifica la necesidad de la implementación de la seguridad de la información:

> En la actualidad existe una guerra determinada guerra cibernética, la cual se enfoca y está dirigida a los sistemas informáticos, donde la información juega un rol importante, una vez esta sea robada o se vulnere, se puede decir que los pilares de la seguridad informática como la confidencialidad, la integridad y disponibilidad de está fue alterada. El mundo de hoy en día se enfrenta a constantes ciberataques los cuales no son visibles en su acción, pero sus consecuencias son catastróficas. (Monsalve, 2018, p. 1)

Conforme a lo anterior, se deduce la urgencia de educar a los usuarios que están expuestos al momento de ser parte del mundo tecnológico. Un punto focal que resulta ser una potencial amenaza es el entorno escolar, pues desde sus prácticas cotidianas los integrantes de esta comunidad resultan ser el grupo propicio para fomentar esta sensibilización en ciberseguridad.

La ley 1273 de 2009, o mejor conocida como la ley de protección de la información y de los datos, es el soporte jurídico que se tiene en cuenta al momento de interpretar los delitos que pueden incidir en la cibercriminalidad, tales como el acceso ilegítimo, la suplantación, la interceptación, los daños y/u obstaculización a sistemas informáticos, violación de datos personales, hurto o transferencias no consentidas de activos. Por esto, se debe tener en cuenta el contexto que se vive gracias a la globalización, ciertas dinámicas sociales se vieron forzadas a transformarse a partir de este nuevo siglo, implementando las nuevas tecnologías para la transición de las prácticas cotidianas, puesto que, aspectos como la hiperconexión global y la masificación de la información, fomentaron la necesidad de la implementación de la ciberseguridad como reflexión ante la frágil protección de estos que detonan en las amenazas cibernéticas.

Caamaño y Gil (2020), plantean que, en este mundo globalizado, las organizaciones, los estados y la sociedad en general, han sido amenazadas por ciberataques, lo cual, desde el contexto económico, político y social, representa vulnerabilidades que inciden sustancialmente no solo en la toma de decisiones, sino también, en la estabilidad administrativa y económica para generar confianza ante los grupos de interés. De ahí que los problemas de ciberseguridad no deben analizarse de manera aislada, sino mediante un enfoque sistémico e integral.

Por ello, en el entorno escolar, según el D. Q. Institute (2019), los hechos delictivos que tienen mayor incidencia es la obtención de información personal con intenciones de estafar, extorsionar, secuestrar, *ciberbullying* o derivados de la explotación sexual infantil, por ello, la importancia de brindar herramientas para que cada integrante de la comunidad educativa, en especial los niños y niñas, tuviesen la responsabilidad de conocer cuáles son los riesgos cibernéticos de los que se puede ser víctima explícita o implícitamente, atendiendo a la necesidad de la ciberseguridad desde el uso de los recursos tecnológicos, la información y la comunicación.

Figura 1. Los niños y la seguridad en línea

Nota: en la figura se evidencian las estadísticas de seguridad infantil en línea, según un estudio aplicado en 30 países.

Fuente: D. Q. Institute (2019).

Los cambios que tuvo la sociedad dependiendo de las tecnologías como consecuencia a la crisis que provocó la pandemia sanitaria ocasionada por el covid-19, trasladando el escenario laboral, educativo y social a la digitalización inmediata, ya que fue un contexto coyuntural para que la seguridad de la información fuese más susceptible a la amenaza cibernética, problema que persiste en la actualidad. Por lo anterior, el Gimnasio Militar de la Fuerza Aeroespacial Colombiana fue elegido campo de investigación, basado en la seguridad que caracteriza a esta institución, ya que, al estar vinculado con la Fuerza Aeroespacial, representa una mayor vulnerabilidad frente a la criminalidad cibernética, bajo el empleo de ciberataques tanto a la institución como a las personas que hacen parte de su comunidad.

Ante esto, y desde la seguridad integral, teniendo en cuenta el entorno tecnológico y digital, para dar respuesta al interrogante sobre cómo mitigar los riesgos en ciberseguridad desde una perspectiva institucional, para ello, esta investigación tuvo el objetivo de diseñar una propuesta con lineamientos institucionales en ciberseguridad a partir de la identificación y el análisis de factores, escenarios y riesgos de protección en ciberseguridad, culminando con la elaboración de una cartilla con medidas preventivas que permitieron brindar una orientación a la comunidad para aminorar dicha vulnerabilidad institucional.

La importancia de la ciberseguridad en el escenario escolar

Ahora bien, se debe tener como precedente la ciberseguridad como principal respuesta a lo que representa amenazas que afectan la seguridad de la información en el espectro tecnológico y digital, pues su función radica en gestionar los riesgos que vienen del ciberespacio, relacionados con la información digital y sus sistemas interconectados, donde el ciberespacio se relaciona con internet (MinTIC, 2014 citado por Cayón, 2014).

El ciberdelito representa un reto, ataca en diferentes sectores, tanto públicos como privados que utilizan el ciberespacio y las nuevas tecnologías como herramientas para el desarrollo de las actividades cotidianas, teniendo presente el ambiente escolar como uno de los escenarios más propensos a este tipo de amenazas, sobre todo la población constituyente, pues cada actor de la comunidad educativa representa un factor de riesgo.

Cayón (2014), en su artículo: *La importancia en el componente educativo en toda estrategia de ciberseguridad*, aseveran qué, "la dependencia tecnológica ha supuesto un creciente número de retos jurídicos y sociales, muchos de los cuales aún se encuentran en vías de solución" (p. 6).

A estos efectos, la protección de los sistemas informáticos considerados críticos se ha convertido en un tema de interés nacional, ya que el daño a estos puede causar graves trastornos al funcionamiento de cualquier sociedad. Esta es una de las principales razones por las cuales la ciberseguridad es considerada un eje estratégico a nivel nacional que afecta todos los niveles de la sociedad.

Ante esto, la digitalización de la sociedad que explican Galán y Galán (2016), comprende en la exigencia de garantizar las herramientas tecnológicas que tienen la capacidad de asumir un ciberataque, que puede ser determinado por su nivel de confianza, accidentes u operaciones ilícitas o malintencionadas, que comprometan la integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas permiten acceder a los mismos.

Lo que permite analizar que, en el entorno escolar, se necesita implementar una propuesta de ciberseguridad que pueda responder a los retos que se enfrenta la institución educativa a partir de la concientización de las buenas prácticas digitales y tecnológicas, garantizando la menor vulnerabilidad en ciberseguridad.

La ciberseguridad como respuesta a la protección de la información

El significado y relevancia que se le dan a temas de trascendencia en seguridad frente a la criminalidad tecnológica y digital, en el que la vulnerabilidad e indefensión

son un punto crucial en los ciberataques en las organizaciones, instituciones y sociedad en general, por ejemplo: las instituciones educativas, a lo que Mónica Valle, en su texto titulado *Ciberseguridad: consejos para tener vidas digitales más seguras*, enfatiza en que, tanto la escuela como el sistema educativo, debe tener dentro de sus obligaciones más inmediatas el entender y darle cabida a una educación enfocada en la ciberseguridad, para que a través de dicha educación se generen puentes que permitan que estudiantes, docentes, padres de familia y comunidad académica en general, tengan certeza de los peligros existentes en las redes sociales, todo esto, gracias a una educación pertinente sobre el tema. (Valle, 2018).

Por esto, abordando la problemática de la seguridad de la información dentro del contexto académico, Morales (2019), desde un punto de vista de educación superior, afirma que "se tiene una preocupación común sobre la protección de datos en el ciberespacio, dado que varios de sus sistemas de información no cuentan con las normas de ciberseguridad necesarias" (p. 1). Esto fue el fundamento del análisis que permitió desarrollar medidas de control y estrategias de acción que aportaron a esta investigación.

En el contexto colombiano, según los resultados arrojados en el *Estudio de la evolución de la seguridad de la información en Colombia: 2000-2018,* de Cano y Rocha (2019), a partir de una encuesta aplicada durante 19 años, se logró estudiar y analizar el comportamiento de la seguridad en nuestro contexto, en la que se dedujo que este tema ha tenido tanto una evolución como nuevos retos que deben ser objeto de investigación.

De este modo, Marín *et al.* (2019) presentan un modelo ontológico de los ciberdelitos tomando como eje principal a Colombia, abordando varios aspectos como la clasificación, jurisprudencia y nivel de impacto de los ciberdelitos, con el fin de que la aplicabilidad de este modelo soporte la toma de decisiones en el ámbito de la ciberseguridad.

Para ello se requiere una formación consciente de la necesidad de la implementación de la ciberseguridad en el contexto académico, Valencia *et al.* (2020), en su texto titulado *Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico*, ejemplifican desde los resultados de su investigación de medir el impacto y difusión de publicaciones referentes al tema de la educación en ciberseguridad y la importancia que tiene la misma desde una perspectiva educativa para el entendimiento de los avances tecnológicos actuales y la protección de los nuevos procesos de innovación.

Ahora bien, abordando el tema de la ciberseguridad como una necesidad por implementarse en el ámbito escolar, el Fondo de las Naciones Unidas para la Infancia (UNICEF), presentó en el año 2019 una guía en donde los niños, niñas y adolescentes adquieren conocimientos teniendo presente las ventajas que proporciona el acceso a la información en la actualidad, pero enfatiza en que esto trae consigo riesgos, que deberán ser enfrentados con la implementación de ciertas herramientas que sean de protección.

Por consiguiente, la exposición en el mundo tecnológico y digital significan un progreso que resulta ser beneficioso, también representa la vulnerabilidad de los usuarios a la ciberdelincuencia, en especial los niños, niñas y adolescentes que son consumidores nativos de la tecnología, pues así lo ejemplifica el texto titulado *Socialización preventiva ante el ciberacoso*, desde el análisis de los resultados de la aplicación en dicho estudio, se tuvo como referencia los datos a nivel mundial, evidenciando el aumento constante y sistemático del ciberacoso en la población juvenil, el cual se desarrolla desde las plataformas digitales, lo que permite ver el origen y desenlace, así como las formas adecuadas para tratar este fenómeno y superarlo (Oliver y Santos, 2014).

Por esta razón, la identificación de las prácticas delictivas que se emplean en el mundo digital y tecnológico, así como las dinámicas sociales que son trasladas a este escenario, son la suficiente razón para la urgente implementación de un modelo preventivo que sea soporte de la ciberseguridad.

Epistemología

La investigación se fundamenta en la teoría de acción razonada, que surge en 1980 por Fishbein y Ajzen

citados en Reyes (2007, p. 2), es un modelo que pretende "buscar el origen de la conducta en las creencias que el individuo mantiene ante la intención de realizar determinada conducta", pues este factor en el espectro tecnológico y digital es determinante al analizar el uso que se tiene de la información de sí mismo y de la que reposa allí.

Dicho esto, el modelo de Davis (1989) funciona a partir de la motivación, ya que esta consta de dos variables, las cuales son la utilidad percibida y la facilidad de uso partiendo del aprendizaje de la tecnología y el propósito que determina a las personas en su conducta al momento de estar inmersos en el mundo tecnológico y digital.

Entonces, se tiene presente que las transformaciones se han dado con el paso del tiempo en técnicas que son necesarias para comunicarnos o transmitir información desde la tecnología, y que, desde el uso de estas, impactan culturalmente en lo que se considera indispensable. Puesto que en los seres humanos hay un cambio evidente desde el aprendizaje, ya que las tecnologías de la información y la comunicación (TIC) tuvieron una gran acogida en la sociedad, pues Echeverría (2018), compara este hito en la historia con la revolución industrial, ya que se ha insertado en todos los ámbitos de nuestras vidas, y por esta razón surge la necesidad de conocer cómo está impactando la tecnología en la sociedad.

Tabla 1.
Modelos de la teoría de acción razonada

Modelo de aceptación tecnológica - Davis (1989)	Utiliza la metodología de los valores esperados de la teoría de acción razonada y reemplaza las creencias actitudinales que estaban definidas en esta por dos nuevos constructos: facilidad de uso y utilidad percibida, y adicionalmente, la actitud hacia el uso de la tecnología y la intención de uso.
Modelo motivacional - Davis (1989)	Relacionadas con los procesos de cambio, tanto sociales como individuales, por esta razón se han adaptado las perspectivas motivacionales extrínsecas e intrínsecas, que han sido utilizadas como predictores de la intención de la conducta de los usuarios.
Teoría del comportamiento planificado - Fishbein y Ajzen (1975)	Cuando los individuos forman una actitud positiva hacia el aprendizaje en aspectos relacionados con la tecnología, tendrán una intención más fuerte hacia la adopción y mayores inclinaciones para usarla. La acción humana la relaciona con las creencias que un individuo pueda tener acerca de las consecuencias de una conducta; las creencias que posea sobre las expectativas normativas de otra persona (presión social); y, las creencias sobre los factores que puedan influir en el desarrollo de una conducta positiva o negativa. Estos tres constructos se combinan para generar la intención conductual.
Modelo de combinación del modelo de aceptación y la teoría del comportamiento planificado	Se refiere a la evaluación que hace el usuario sobre el uso de las tecnologías; las normas subjetivas tienen que ver con las opiniones de personas o grupos de personas que pueden resultar importantes para un individuo; el control de percepción del comportamiento, está vinculado a las percepciones sobre la presencia o no de recursos u oportunidades que se consideran necesarias para llevar a cabo una conducta determinada y, finalmente, la utilidad percibida, es un concepto que se desarrolla en torno a la probabilidad subjetiva que poseen los usuarios.
Modelo de utilización del pc	Donde se plantea que la conducta de los individuos, en relación al uso de la tecnología, puede ser predicha por una combinación de la intención de uso, basándose en la actitud y motivaciones, en la norma, y en las conductas y hábitos.
Teoría de la difusión de las innovaciones	Ventaja relativa, mejora que tienen los individuos de una nueva tecnología sobre otra ya existente; compatibilidad, la innovación es percibida como consistente con las necesidades, los valores y las experiencias pasadas de los adoptantes; complejidad, grado en que una innovación es fácil o difícil de usar; observabilidad, grado en que los resultados de una innovación son observables y, la experimentación, grado en que una innovación puede ser probada por quienes desean adoptarla.
Teoría social cognitiva	No se utiliza específicamente para predecir comportamientos de aceptación, sino para proporcionar ideas adicionales en la determinación de los comportamientos relacionados con la adopción de las innovaciones como, por ejemplo, el efecto de las características de cada individuo sobre su autoeficacia y la relación que existe con sus resultados de aceptación de la tecnología.

Fuente: elaboración propia, basada en Fernández *et al.* (2015).

Ahora bien, teniendo en cuenta que el tema central de esta investigación se desarrolla en el contexto escolar, y que es importante indagar el impacto que puede tener el contacto con el ciberespacio en la niñez y la adolescencia, Jean Piaget, en su teoría del desarrollo cognitivo, aborda las etapas de crecimiento del individuo, en donde los niños aprenden mediante la estimulación, la observación y la exploración que inciden en su formación como sujetos.

Por ello, Castilla (2013) rescata que el aprendizaje se divide en periodos como el sensomotor, preoperacional, operacional concreto y operacional formal, que van marcando las etapas de la vida y su desarrollo. Entonces, pasan de la adaptación, el aprendizaje, la investigación y, finalmente, a partir de los 12 años, se completa la racionalidad, lo que le permite reflexionar desde la crítica lógica y no solo desde las emociones.

Así mismo, la teoría de Maslow permite abordar desde los cinco niveles de las necesidades de los seres humanos, partiendo de las fisiológicas, la seguridad, la afiliación, el reconocimiento y culminando con la autorrealización, que en últimas se experimenta como algo satisfactorio.

Con ello se llega a la conclusión de que los niños, niñas y adolescentes les surge la necesidad de ser reconocidos socialmente, argumentando la aceptación y validación social; McClelland (1964) ejemplifica que, las personas aprenden inconscientemente y actúan conforme a tres necesidades de influencia social: como el logro, la afiliación y el poder, que resultan ser la consecuencia de estar inmersos en estos contextos.

Adicionalmente, los cambios que se generaron con la llegada de la tecnología, incidió profundamente en la cotidianidad de la sociedad, al punto en que no se tuviese en cuenta la edad desde la que tenemos acceso a este mundo, siendo así que lo que se consideraba menester de la sociedad en el centenario pasado, se vio sumido y transformado desde las TIC en este nuevo siglo, pues desde la mirada que brinda la pirámide de Maslow, aplicada por el BBVA (2017), se evidencia que estas necesidades se modificaron y ahora se tiene como referente principal la tecnología.

Por ello, se refuerza el desafío de crear un modelo para sensibilizar desde la cultura de la ciberseguridad a todos los usuarios, para que no estén expuestos a la ciberdelincuencia, o por el contrario, si se recibe una amenaza se tengan las herramientas para enfrentarla.

Figura 2. Pirámide de Maslow
Fuente: BBVA Research Center y Maslow (1943).

Ejecución de la metodología

La investigación se desarrolla bajo la aplicación de una metodología descriptiva, la cual tiene como funcionalidad especificar las características halladas desde el método cualitativo, lo que permite identificar desde un contexto educativo desarrollado en el GIMFA, los riesgos y amenazas de vulnerabilidad a los que se está expuesto, que conforme a las categorías enfatizan en los lineamientos académicos que rigen a las instituciones y miembros de la comunidad educativa.

Tabla 2.
Desarrollo metodológico

Objetivos	Metodología
Realizar un diagnóstico para diseñar un recurso digital con los lineamientos institucionales en ciberseguridad. en el Gimnasio Militar de la Fuerza Aeroespacial Colombiana.	Se realizó una valoración de riesgos para cumplir con el objetivo general de la investigación.
Identificar las categorías de análisis asociadas a factores de riesgo y protección de ciberseguridad en Instituciones educativas.	Revisión documental para categorizar los factores de riesgo, así: riesgos de conducta, de contenido y de contacto.
Reconocer factores de riesgo y protección frente a la ciberseguridad en los niños de los grados cuarto y quinto del GIMFA.	Por medio de entrevistas y encuestas para reconocer los riesgos de valoración más alta.
Análisis de la información mediantetécnicas de análisis de riesgo de la ISO 31010.	Elaborar un informe de estos riesgos donde se pudo analizar la causa, consecuencia, plan de acción y control de los riesgos.
Elaborar una cartilla digital, con medidas preventivas para mitigar los riesgos en ciberseguridad.	Se entrega una cartilla, con recomendaciones, juego interactivo para los niños, padres, docentes del Gimnasio Militar de la Fuerza Aeroespacial Colombiana.

Fuente: elaboración propia (2022).

Para efectos de la empleabilidad de la metodología escogida, se inicia por la revisión documental, teniendo presente que la ciberseguridad en Colombia comenzó a tener importancia desde el 2001, bajo una aplicabilidad tanto en el entorno privado, como en el público, en esencia en la sociedad en general, pues la necesidad imperante de salvaguardar la información personal, fue lo que influyó en el sistema judicial al promulgar leyes y normatividades de lineamientos de delitos y derechos del usuario, entablando discusiones abordadas desde el escenario educativo, ya que en el contexto académico, la comunidad accede a este tipo de sensibilización y lo replican en otros contextos que se sientan o tengan conocimiento de un riesgo de vulnerabilidad.

Continúa con el desarrollo de entrevistas con expertos en la seguridad de la información, que tengan relevancia en la institución educativa, así como con la aplicación de encuestas a los miembros de la comunidad educativa, en la que se obtuvo la ejecución de la triangulación de estos, como la explica Albert (2007), "esta es una técnica estructurada, que permite la recogida rápida y abundante de información mediante una serie de preguntas orales o escritas que debe responder un entrevistado con respecto a una o más variables a medir" (p.115).

Es entonces que se planea el diseño de una herramienta disponible en digital que desde el análisis de la identificación de los riesgos y amenazas, entable la necesidad de implementar y/o fortalecer la protección tecnológica y digital, aplicando la técnica de investigación proyectiva, la cual Passos (2015), explica que permite crear una propuesta que dé solución al problema de manera práctica, abordando un área particular del conocimiento, desde el diagnóstico de las necesidades apuntando a las tendencias futuras.

Al ser una metodología cualitativa, la subjetividad juega un papel importante, Sneiderman (2006), le da valor a la toma de decisiones desde la comprensión y el análisis de un fenómeno en específico, el cual puede tener carácter real o simbólico y evidenciarse en un aspecto manifiesto y/o latente.

Para efectos de esa investigación, se tuvo presente la revisión documental, desde la selección de muestra, la cual tuvo de base el muestreo no probabilístico, que Otzen y Manterola (2017), dicen que trata de "una técnica en que la selección de los sujetos de estudio dependerá de ciertas características y criterios que el investigador considere para el estudio" (p.2). Por lo tanto, para desarrollar el estudio, seleccionaron parte de la población de la comunidad educativa como muestreo compuesto por estudiantes de cuarto y quinto de primaria, docentes, padres de familia y personal directivo de la institución.

Teniendo presente que allí se encuentran los estudiantes que tienen mayor incidencia en ser vulnerables

en el ciberespacio, ya que inician su inmersión en las redes sociales, el uso de la tecnología y las plataformas digitales, empezando a ser un tema más arraigado para el cómo desarrollan su cotidianidad desde lo personal, pero también desde lo educativo, pues el GIMFA, aparte de enriquecer a sus estudiantes en conocimientos y competencias cumpliendo los estándares de alta calidad, también emplea herramientas tecnológicas para el desarrollo académico.

Entonces, para la recolección de datos como requisito solicitaron el consentimiento informado para emplear el estudio en los menores de edad, también se utilizaron dos instrumentos: la entrevista estructurada y la encuesta descriptiva, ambos se diseñaron con la intención de acopiar información de cada grupo focal, desde la observación y el análisis de los objetivos de la investigación; pues para la identificación de riesgos, se basa en la norma IEC-ISO 31010, la cual se aplica para evaluar en diferentes contextos los riesgos que se presentan en los cambios tecnológicos y digitales, así como el análisis de corbatín que según la norma mencionada anteriormente, permite evidenciar la trayectoria de un evento desde sus causas hasta sus consecuencias (ICONTEC, 2019).

Por esto, el objetivo de la investigación radicó en diseñar una propuesta que aborde normatividades, orientaciones y conocimientos que permitan a la comunidad educativa hacer un correcto uso de las herramientas tecnológicas y digitales desde la forma segura que proporciona la ciberseguridad.

Análisis de resultados

Como resultado de la ejecución de la metodología en la que se emplearon instrumentos de recolección de información pertinente en este estudio investigativo, que posteriormente se realizó la triangulación de los datos obtenidos, gracias a las respuestas del objeto de estudio, el cual estuvo compuesto por 10 estudiantes entre los 9 y 12 años de cuarto y quinto del GIMFA, 10 padres de familia entre los 36 y 47 años de edad, y 10 docentes orientadores de estos cursos, cuyo rango de edad está entre los 40 a 55 años, en que a partir del muestreo se construye un mapa de riesgos a los que se encontraba expuesta la institución educativa, es importante tener presente las amenazas, los riesgos, la comunicación y las políticas-ciber, pues estas categorías son determinantes en el análisis de la ciberseguridad en los colegios.

Con base en los resultados obtenidos de las 30 encuestas y entrevistas de los actores seleccionados de la institución educativa, se ejecutaron los análisis de riesgos aplicando la técnica de corbatín, la cual por medio de diagramas expone los riesgos, consecuencias y medidas de recuperación que sean adecuadas a cada riesgo, también se aplicó la técnica de escenarios, que permitió identificar las posibles circunstancias en el futuro que sean incidencia en el riesgo, con el objetivo de definir estos escenarios, haciendo alusión a la necesidad de implementar herramientas que permitan mitigar estos posibles resultados.

A partir de la categorización y el análisis relacionados a la investigación de ciberseguridad en instituciones educativas, se halló que las amenazas más elevadas fueron el *ciberbullying*, el *phishing* y actividades de ingeniería social, y que los riesgos más comunes se situaban en el robo de la información y la suplantación. El mapeo de incidentes dejó en evidencia las amenazas y los riesgos a los que está expuesta la comunidad educativa, teniendo el precedente de los hechos y los posibles incidentes que se presenten con el objeto de evitar su materialización.

Desde las prácticas cotidianas, se muestra que ejercicios simples como usar internet no genera una diferencia marcada correspondiendo a la edad. Esto evidenció que en el espectro tecnológico y digital la comunidad educativa se encuentra expuesta a múltiples amenazas, desde la incomodidad que invade al sujeto cuando se enfrenta a situaciones como la interacción con desconocidos, el *ciberbullying*, la ingeniería social o el *phishing*, que incurren en delitos como el robo de datos, la suplantación de identidad, la estafa, encuentros con pedófilos, la pornografía, las amenazas o el acoso.

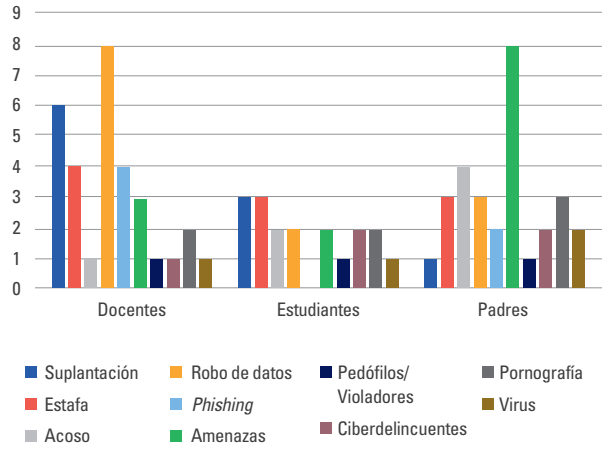

Figura 3. Resultados para la categoría amenazas y riesgos asociado a las amenazas y riesgos identificados que se encuentran en Internet
Fuente: elaboración propia (2022).

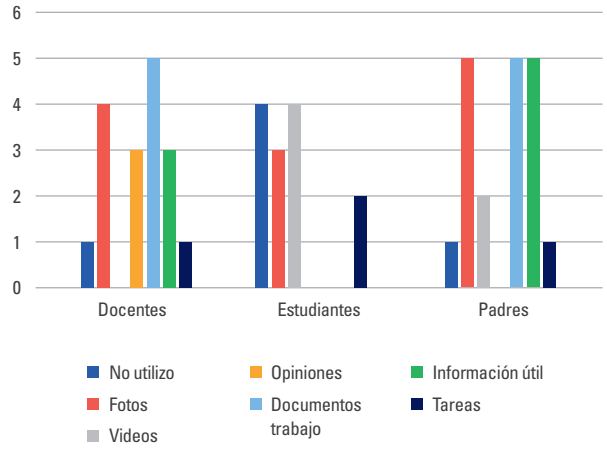

Figura 4. Resultados para la categoría comunicación sobre tipo de información que suben a plataformas o redes sociales
Fuente: elaboración propia (2022).

Así mismo, en esta misma categoría se obtuvo como resultado, en primer lugar, los riesgos de contacto, seguidos de los riesgos de conducta, finalizando con los riesgos de contenido. No obstante, tanto los docentes como los padres de familia tienen conocimientos que les permitió reconocer estos riesgos, mientras que los niños no reconocen ninguno de estos, presentando la primera necesidad de fortalecer esta sensibilización frente a la ciberseguridad.

En cuanto a la categoría de la comunicación, que aborda el uso de las plataformas, redes sociales, correos electrónicos, entre otras herramientas digitales que median a los integrantes de la comunidad educativa en su comunicación habitual.

Así se analizó que el tipo de información que se transmite está anclado al ejercicio del día a día de cada persona de ese estudio, pues mientras los docentes envían documentación laboral, información útil, se abren a espacios de opinión e incluso suben fotos, lo cual no varía en cuanto a los padres de familia, pero sí se revisa el caso de los estudiantes, porque ellos prefieren subir fotografías o compartir videos, aunque no contemplan que en el mundo de las redes sociales WhatsApp y TikTok son parte de ellas.

En cuanto a la esfera políticas-ciber, se suscribe a los conocimientos previos y las precauciones que debe implementar la comunidad educativa con el objetivo de mitigar los riesgos y las amenazas en ciberseguridad, es por esto que, al evaluar los resultados obtenidos se encuentra que los adultos comprenden el concepto de la ciberseguridad, que aplican normas en cuanto el uso del internet tanto en el hogar como en la institución educativa, no obstante, los estudiantes representaron mayoritariamente el desconocimiento frente a la ciberseguridad.

Pese a que la vulnerabilidad cibernética es enseñada en el colegio y en la casa, con el objeto de que los estudiantes reconozcan estos peligros, no se abordan en igualdad, puesto que los riesgos como el *phishing*, el *bullying*, la divulgación de fotografías y videos son temas poco discutidos en cada espacio, sin embargo, no sucede lo mismo con las amenazas, ya que se reconocen la suplantación de identidad, la explotación sexual, las estafas, los virus o *hackers*, lo que conlleva a que los niños recuerden más las tres últimas.

Aunque existan reglas que son implementadas por los padres de familia, como no compartir claves o información personal, también existe un control de tiempo y uso del internet, y la delimitación de los espacios en que se está permitido el uso de equipos tecnológicos, como el celular, así como normas de bloquear descargas y el acceso a páginas no seguras, no obstante, y aunque la institución educativa implemente varias de estas reglas y normas, no existe una retroalimentación de conocimientos en ciberseguridad en estos dos actores, más allá de las sanciones que se establecen en

el manual de convivencia, no hay evidencia de normatividad o reglamento preventivo referente a la gestión de la ciberseguridad, por ello se obtiene el desconocimiento de este tema en los estudiantes, quienes se limitaron al uso del celular en clase.

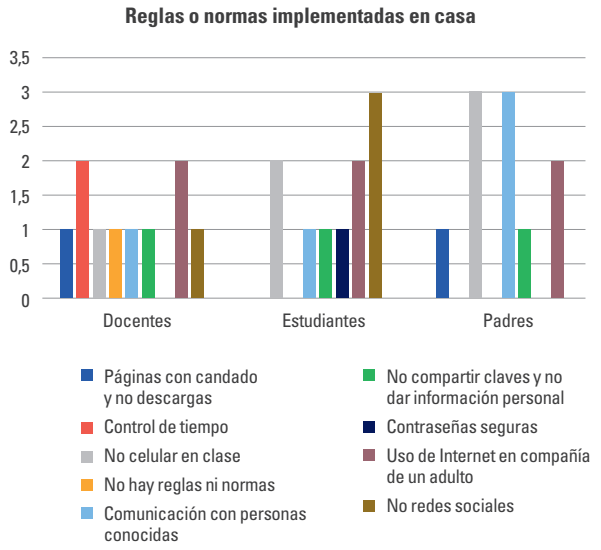

Figura 5. Resultados de políticas ciberamenazas en cuanto a reglas y normas implementadas en la casa
Fuente: elaboración propia (2022).

Como resultado, este desconocimiento en los niños y niñas, los docentes y padres de familia, quienes manifiestan que, aunque existan políticas de ciberseguridad en la Fuerza Aeroespacial Colombiana, no las conocen o no se implementan de la misma manera en el GIMFA.

Ahora bien, se tiene presente que tanto la tecnología como la digitalización han contribuido y transformado la cotidianidad de la sociedad, y que estas tienen un impacto diferente en los niños, niñas y adolescentes, puesto que su forma de aprendizaje cambia constantemente, también impacta en cómo la influencia de presiones sociales, culturales, políticas y económicas detona en el qué y el cómo funcionan las instituciones educativas, pues estos espacios ahora son mediados por dichas herramientas, las cuales han contribuido a mejorar los resultados educacionales, lo que demanda al sector educativo emplear procesos de innovación desde el sentido de la escolaridad, el currículo, la pedagogía, la evaluación, la administración, la organización e incluso el desarrollo profesional de docentes y directivas de las instituciones educativas.

Por ende, el análisis que se obtuvo de la matriz de riesgos aplicada al GIMFA, evidenció que el uso de la tecnología y digitalización favorece la educación, aunque también existe un interrogante al que se le debe dar respuesta con respecto a la seguridad cibernética y su imperante necesidad de implementarse, pues a partir de los resultados que se clasificaron en la matriz de riesgo, se identifica que el *cyberbullying*, el *phishing*, la ingeniería social y la intrusión a clases son índices de vulnerabilidad en el espectro tecnológico y digital, demostrando una vez más que la ciberseguridad permite abordar los procesos mediados por la tecnología de manera efectiva en la comunidad educativa.

Tabla 3.
Matriz de riesgos en los procesos de formación

Código	Categoría	Evento del riesgo	Responsables	Categoría
R1	Conducta/ Riesgo	*Cyberbullying*	Estudiantes, padres de familia, docentes, psicólogos y coordinación de convivencia.	ALTO
R2	Contacto/ Amenaza	*Phishing*	Estudiantes, padres de familia, institución académica.	ALTO
R3	Contacto/ Amenaza	Ingeniería social	Estudiantes, padres de familia.	MODERADO
R4	Contenido/ Amenaza	Intrusión a clases virtuales	Estudiantes, padres de familia, director de la institución educativa, policía nacional.	MODERADO

Fuente: elaboración propia (2022).

Identificación del riesgo/plan de acción

Acorde a los resultados evidenciados en la matriz de riesgo se identificaron cuatro riesgos potencialmente peligrosos, como el *cyberbullying*, y aunque en estos

casos existan medidas de protección en el uso de las TIC, como solicitar intervención e informar quiénes tienen el control sobre estas situaciones desde los mismos estudiantes, los padres de familia, docentes, psicólogos hasta la coordinación de convivencia, pues el nivel de riesgo es alto, lo que requiere implementar acciones como la instalación de antivirus licenciados y *software* en los dispositivos tecnológicos, también concientizar a los estudiantes sobre el acoso y el ciberacoso, instruirlos en la cultura tecnológica y tener conocimiento de los lugares que habitan y sus compañías, sus prácticas en el ciberespacio a partir de una comunicación asertiva y constante con los estudiantes.

Lo mismo ocurre con el *phishing*, por ello es necesario tener presente que si se presenta sospecha de enlaces o *software* de dudosa procedencia, se debe educar a los estudiantes en instancias de responsabilidad civil, penal y administrativas que se imputan cuando se vulneran derechos propios o de terceros, pues todos los actores de la comunidad educativa son responsables de ejercer este control, ya que el nivel de riesgo es alto, por lo tanto, se requiere implementar contraseñas seguras, verificando las políticas de privacidad y avisos legales, confirmando el requerimiento de enviar información personal y comprobando la legalidad de las páginas web.

En cuanto a la ingeniería social, su funcionamiento está ligado a la información personal que se comparte en espacios como las redes sociales, allí la ciberdelincuencia actúa con el solo hecho de dar acceso al perfil propio, permitiendo evaluar la vulnerabilidad que se tiene a partir de determinadas circunstancias que resultan ser beneficiosas para su actuar delictivo, pese a que está en un nivel de riesgo moderado, requiere implementar medidas de seguridad como la creación de un avatar en vez de una fotografía para el perfil, utilizar contraseñas seguras y cambiarlas constantemente, obtener las aplicaciones, información y demás necesidades en sitios oficiales.

Finalmente, respecto a la intrusión en las clases virtuales, se da principalmente por conectarse a clases desde espacios no seguros o públicos, compartir el enlace con personas ajenas a la institución o aceptar su participación, aunque a veces puede darse el ingreso sin autorización, lo que violenta los accesos de seguridad, aprovechando estos espacios para sabotear, compartir pornografía o insultar a quienes hacen parte de la clase, siendo importante fomentar la conciencia de la responsabilidad que cada actor de la comunidad académica tiene en la protección de sí mismo y de los demás.

Aunque su nivel de riesgo sea moderado, no es sinónimo de bajar los niveles de seguridad existentes, como el control de la pantalla compartida, las credenciales de seguridad y los antivirus, también se puede fomentar la cultura de la tecnología, el bloqueo del aula virtual para que solo se tenga acceso los autorizados o la creación de enlaces diferentes para cada sesión de clase.

Conclusiones

El estudio de investigación que se abordó permitió determinar que la sociedad está inmersa en la evolución de la tecnología y la digitalización de la cotidianidad, pues con el paso del tiempo y las eras que fueron significativas en los cambios que hoy en día se emplean para aprender, comunicarnos, divertirnos, por esto, en el sector educativo, se presenta el acceso a esta como un avance en los procesos de aprendizaje, con el objeto de transformarlos y mejorarlos, lo que influye en la necesidad de las instituciones académicas por implementar métodos innovadores para converger la pedagogía con la tecnología, haciendo partícipes a toda la comunidad educativa.

También, se debe tener presente que al ser tan etérea la tecnología y los cambios abruptos que se presentan con la invención de una nueva versión, no se puede predecir de qué manera tendrá un impacto en los procesos educativos más que las actuales y funcionales a la fecha, la cual cumple un rol en la posesión del conocimiento, de enriquecerlo, de permitir tener nuevas formas de enseñanza, de aprender y de gestionar la escolaridad.

La ciberseguridad no solo cumple con el rol de proteger desde el ciberespacio al usuario, también influye en el impacto que podría tener un ataque en sus inmediaciones, pero que resulta desastroso en el plano físico, por esto es necesaria la acción oportuna y desde la cultura de la prevención, para minimizar los riesgos que podrían desembocar en daños a miembros de la comunidad académica, a la reputación, o incluso inconvenientes legales.

A partir de ejercicios como el análisis del riesgo, se tuvo otra perspectiva de cómo la tecnología podría beneficiar al sector educativo, sin desconocer las amenazas persistentes en estos escenarios, esto permite desarrollar un trabajo colaborativo, que influya en la manera en que se abordan, controlan y se da tratamiento a los riesgos de manera efectiva, con el objetivo de garantizar la calidad, seguridad y potenciar los procesos educativos desde las nuevas tecnologías.

Cada miembro de la sociedad, de las organizaciones, instituciones o donde se pertenezca tiene una importante responsabilidad en hacer buen uso de la tecnología y los espacios de la virtualidad y la digitalización. Está en nuestro poder detener las cadenas de la criminalidad cibernética, fomentando la sensibilización de la importancia de implementar la ciberseguridad en cada espacio que se habite, para tener el conocimiento de las indicaciones a seguir en caso de ser vulnerado o aprender a identificar este tipo de incidentes.

Esta investigación permitió realizar el diagnóstico que se basó en la identificación de las categorías de análisis de factores de riesgo como la conducta, el contenido y el contacto, que determinaron los niveles con mayor incidencia como el *ciberbullying*, el *phishing*, la ingeniería social y la intrusión en las clases virtuales, como resultado de la aplicación de técnicas de análisis de riesgo abordando la causa, la consecuencia, el plan de acción y la contención de los riesgos, todo esto fue fundamental para diseñar el recurso digital con los lineamientos institucionales aplicando la ciberseguridad en el Gimnasio Militar de la Fuerza Aeroespacial Colombiana, el cual se materializó y permitió evidenciar la importancia de implementar un manual en ciberseguridad, que esté al alcance de toda la comunidad educativa.

Referencias bibliográficas

Albert, M. J. (2007). La investigación educativa: claves teóricas. McGraw Hill. Pp. 1 – 266. https://www.academia.edu/27287685/La_Investigaci%C3%B3n_Educativa_Claves_Te%C3%B3ricas_Albert_G

Banco Bilbao Vizcaya Argentaria - BBVA. (2017). *La importancia de las TIC en las necesidades de la sociedad: una aproximación a través de la óptica de Maslow*. https://www.bbvaresearch.com/wp-content/uploads/2017/09/maslow_piramide.pdf

Caamaño, E. & Gil, R. (2020). Cybersecurity risk prevention from forensic auditing: combining organizational human talent. *Novum, Revista de Ciencias Sociales Aplicadas*, *1*(10), 61-80. https://www.redalyc.org/journal/5713/571361695004/html/

Cano, J. J. y Rocha, A. (2019). Ciberseguridad y ciberdefensa: retos y perspectivas en un mundo digital. *Risti*, (32). https://doi.org/10.17013/risti.32.0.

Castilla, M. F. (2013). *La teoría del desarrollo cognitivo de Piaget aplicada en la clase de primaria.* https://uvadoc.uva.es/bitstream/handle/10324/5844/TFGB.531.pdf;jsessionid=3DE54FF07F73E8720E2F8E86068BE10D?sequence=1

Cayón, J. G. (2014). La importancia del componente educativo en toda estrategia de ciberseguridad. Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacionales. *Esdegue Revista científica*, *9*(18). https://esdeguerevistacientifica.edu.co/index.php/estudios/article/view/9/4

Davis, F. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly, 13*(3), pp. 319-340.

D. Q. Institute. (2019). *DQ Global Standards Report 2019.* https://www.dqinstitute.org/wp-content/uploads/2019/11/DQGlobalStandardsReport2019.pdf

Echeverría, J. (2018). *La revolución tecnocientífica.* http://naturalezacienciaysociedad.org/wp-content/uploads/sites/3/2018/01/Echeverria-Revoluci%C3%B3nTecnocient%C3%ADfica.pdf

Fernández, K., Casarín, A. y McAnally, L. (2015). Apropiación tecnológica: una visión desde los modelos y las teorías que la explican. *Perspectiva Educacional, Formación de Profesores, 54*(2), 109-125. https://www.redalyc.org/pdf/3333/333339872008.pdf

Fondo de las Naciones Unidas para la Infancia – UNICEF. (2019). *Niños, niñas y adolescentes en línea. Riesgos de las redes y herramientas para protegerse.* http://www.codajic.org/node/4215

Galán, C. M. y Galán-Cordero, C. (2016). La ciberseguridad pública como garantía del ejercicio de derechos. *Derecho & Sociedad*, (47), 293-306. https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/18892

ICONTEC. (2019). *Norma IEC-ISO 31010: el uso de técnicas para la evaluación del riesgo*. https://campus.icontecvirtual.edu.co/uploads/posts/Z95h9fsvPvDsUZNjwKxr.pdf

Ley 1273. (2009). *Ley de protección de datos.* Secretaría del Senado. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Marín, J., Nieto, Y., Huertas, F. y Montenegro, C. (2019). Modelo ontológico de los ciberdelitos: caso de estudio Colombia. *Risti*, (17), 244-257. https://www.proquest.com/openview/ef48269d2b309b4657581d7bc7b8172a/1?pq-origsite=gscholar&cbl=1006393#:~:text=Al%20realizar%20el%20modelo%20ontol%C3%B3gico,realiza%20la%20conducta%20y%20su

McClelland, D. (1964). The Achieving Society. *JSTOR.* 3(3), 371-381. https://doi.org/10.2307/2504238

Monsalve, J. (2018). *Ciberseguridad: principales amenazas en Colombia (ingeniería social, phishing y DOS).* Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/4663

Morales, J. A. (2019). *Ciberseguridad y su aplicación en las instituciones de educación superior.* Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

Oliver, E. y Santos, T. (2014). Socialización preventiva ante el ciberacoso. *C&SC – Communication & Social Change*, *2*(1), 87-106. https://doi.org/10.4471/csc.2014.09

Ospina, M. y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad, 62*(2). http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199

Otzen, T. y Manterola, C. (2017). Técnicas de muestreo en una población sobre una población de estudio. *Int. J. Morphol*., *35*(1), 227-232. http://dx.doi.org/10.4067/S0717-95022017000100037

Passos, E. (2015). *Metodología de la presentación de trabajos de investigación. Una manera práctica de aprender a investigar, investigando.* Editorial Institución Tecnológica Colegio Mayor de Bolívar.

Reyes, L. (2007). La teoría de la acción razonada: implicaciones para el estudio de las actitudes. *Investigación Educativa Duranguense,* (7), 66-77. https://www.researchgate.net/publication/28175060_La_Teoria_de_la_Accion_Razonada_Implicaciones_para_el_estudio_de_las_actitudes

Sneiderman, S. (2006). Las técnicas proyectivas como método de investigación y diagnóstico. Actualización en técnicas verbales: el cuestionario desiderativo. *Subjetividad y Procesos Cognitivos,* (8), 296-331. https://www.redalyc.org/pdf/3396/339630247014.pdf

Valencia, A. Bermeo, M., Acevedo, Y., Garcés, L., Quiroz, J., Benjumea, M. y Vanegas, J. (2020). Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico. *Risti*, (29), 225-239.

Valle, M. (2018). Ciberseguridad. Consejos para tener vidas digitales más seguras. *Educatio Siglo XXI, 36*(3), 519-522.