ESTUDIO DE CIBERSEGURIDAD DE LOS ÚLTIMOS 5 AÑOS EN EL TEMA DE DELITOS INFORMATICOS DIRIGIDO A LOS NIÑOS, NIÑAS Y ADOLESCENTES EN EL DEPARTAMENTO DEL HUILA

HAMILTON ANDRADE ORTIZ

UNIVRESIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA CIENCIA BASICA, TECNOLOGIA E INGIENERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
NEIVA, HUILA
2020

ESTUDIO DE CIBER SEGURIDAD DE LOS ÚLTIMOS 5 AÑOS EN EL TEMA DE DELITOS INFORMATICOS DIRIGIDO A LOS NIÑOS, NIÑAS Y ADOLESCENTES EN EL DEPARTAMENTO DEL HUILA

HAMILTON ANDRADE ORTIZ

Trabajo de monografía, para optar el título de especialista en Seguridad en Informática

Directora/Asesora
YINA ALEXANDRA GONZALEZ SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA CIENCIA BASICA, TECNOLOGIA E INGIENERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
NEIVA, HUILA
2020

NOTA DE ACEPTACIÓN

Presidente del Jurado

Jurado

Jurado (En caso de ser solo uno, borrar este o agregar de ser necesario).

Ciudad y Fecha (Día, Mes y Año)

DEDICATORIA

El proceso académico adelantado con la UNAD ha permitido comprender como persona y profesional el componente social en las comunidades y con ello aportar conocimiento en la construcción de una sociedad mediante el ejercicio de las buenas prácticas en los diferentes sistemas de información en el internet.

Gracias a los niños, niñas y adolescentes del Huila; surge la necesidad de proteger el futuro del departamento y orientar los esfuerzos de la ciberseguridad para garantizar el bienestar y libre desarrollo de los menores de edad.

AGRADECIMIENTOS

Agradecer a DIOS por ser el promotor, guía y ayudador en mi vida; en especial al culminar con éxito la Especialización en Seguridad Informática de la UNAD. También exaltar el apoyo incondicional y el amor de mis padres Jose A. Andrade Ortiz y Migdonia Ortiz Vásquez durante, especialmente en las decisiones por forjar un futuro próspero. Por último, demostrar mi respeto y admiración a YINA ALEXANDRA GONZALEZ SANABRIA por las asesorías y concejos para formalizar la monografía y el proceso académico con la UNAD.

TABLA DE CONTENIDO

Pág.

INDICE DE TABLA

Pág.

INDICE DE FIGURA

Pág.

LISTADO DE ANEXOS

Pág.

RESUMEN

Esta monografía dará a conocer los diferentes mecanismos de la ciberseguridad utilizado por los niños, niñas y adolescentes del Huila durante los últimos 5 años, con el propósito de lograr identificar la debilidad o inadecuada práctica que ha desencadenado en los diferentes ciberdelitos según los reportes de las instituciones judiciales en el departamento.

Es importante tener en cuenta las medidas de seguridad adoptada por la población de estudio frente a la creciente demanda de las redes sociales; es importante analizar todo tipo de hecho asociado a esta herramienta para lograr identificar el proceder delictivo y los avances en cuanto a la materia para buscar conocer los retos que tendrá el departamento del Huila en el futuro para mitigar dicha situaciones que atenta contra los derechos constitucionales (VUANELLO, 2011).

Durante el desarrollo de este documento se logró comprender la situación y evolución de los ciberdelitos en el territorio del Huila; con el propósito de aportar conocimientos y recomendaciones que generen en la sociedad una postura apropiada y la implementación de controles sobre la ciberseguridad para mitigar los riesgos asociados a los ciberdelitos en los niños, niñas y adolescentes del departamento.

El estudio y análisis realizado a la información obtenida de los últimos 5 años en cuanto a los ciberdelitos de los niños, niñas y adolescentes en el departamento del Huila; permite responder a las inquietudes sobre cómo proteger a los menores de edad en el uso de la Internet y las redes sociales de forma preventiva con el propósito de mitigar el actuar delictivo y el daño irreparable que ocasiona a sus víctimas.

PALABRAS CLAVES:
CIBER SEGURIDAD, REDES SOCIALES, DELITOS INFORMÁTICOS, INTERNET, NIÑOS, ADELOECENTES, JOVENES. REOMENDACIONES, CONTROLES

[1] VUANELLO, R. La cibercriminalidad como atentado a los derechos humanos de los más jóvenes. 2011 [En línea]. Disponible en: http://www.scielo.org.co/pdf/crim/v53n1/v53n1a04.pdf

ABSTRACT

This monograph will present the different cybersecurity mechanisms used by children and adolescents in Huila during the last 5 years, in order to identify the weakness or inappropriate practice that has triggered in the different cybercrimes according to the reports of the judicial institutions in the department.

It is important to take into account the security measures adopted by the study population in the face of the growing demand for social networks; It is important to analyze all types of events associated with this tool in order to identify the criminal proceeding and the advances in the matter to seek to know the challenges that the department of Huila will have in the future to mitigate said situations that violate constitutional rights (VUANELLO, 2011).

During the development of this document, it was possible to understand the situation and evolution of cybercrimes in the territory of Huila; with the purpose of providing knowledge and recommendations that generate an appropriate posture in society and the implementation of controls on cybersecurity to mitigate the risks associated with cybercrime in children and adolescents in the department.

The study and analysis carried out on the information obtained from the last 5 years regarding cybercrimes of children and adolescents in the department of Huila; allows you to respond to questions about how to protect minors in the use of the Internet and social networks in a preventive way with the purpose of mitigating criminal acts and the irreparable damage caused to their victims.

KEYWORDS:
CYBER SECURITY, SOCIAL NETWORKS, COMPUTER CRIMES, INTERNET, CHILDREN, ADOLESCENTS, YOUNG PEOPLE. RECOMMENDATIONS, CONTROLS

1. INTRODUCCIÓN

La seguridad informática debe considerarse hoy en día como uno de los conocimientos necesarios e importantes no solo para las empresas, si no para el bienestar y protección de las personas; teniendo en cuenta que el individuo termina sufriendo las consecuencias de los ciberdelitos en especial los niños, niñas y adolescentes. Razón por la cual, es necesario investigar los aportes frente al tema en el departamento del Huila.

En Colombia se ha incrementado los ciberdelitos en un 59% por el desconocimiento de las buenas practicas por parte de los usuarios (UNOCERO, 2020). Hoy en día es un reto comprender los riesgos, las vulnerabilidades y los daños que genera un ciberdelito en los menores de edad: población objetivo para vejámenes que desencadena en daños físico y psicológico. Parte de estos sucesos se puede tipificar en delitos como: el sexting, grooming, sextorsión, morphing o ciberbulling, entre otros (UNICEF, La seguridad de los niños en línea, 2012).

El razonamiento descrito en el documento permite orientar el estudio respectivo para identificar los avances en cuanto al tema de ciberseguridad en los últimos 5 años en el departamento del Huila. Los resultados del estudio permitirán aportar información verídica frente a los ciberdelitos de los menores de edad y en el futuro permita contribuir en el desarrollo de estrategia frente al flagelo de la ciberseguridad descrita en la monografía.

El trabajo define los alcances y limitaciones de la ciberseguridad de los últimos 5 años en los niños, niñas y adolescentes del Huila. La información obtenida permite aportar conocimientos desde la UNAD a la sociedad y entidades en general mediante la identificación de los actores y responsabilidades en el proceso para continuar trabajando en la construcción de nueva soluciones que generen día a día un resultado conducente en la mitigación de los ciberdelitos.

[2] UNOCERO. El cibercrimen Colombia aumentó un 59%, pero en parte por culpa de los usuarios. 2020. [En línea]. Disponible en: https://www.unocero.com/noticias/cibercrimen-en-colombia-aumento-2020/

[3] UNICEF. La seguridad de los niños en línea. 2012. [En línea]. Disponible en: https://www.unicef-irc.org/publications/pdf/ict_spa.pdf

2. PLANTEAMIENTO DEL PROBLEMA

2.1 ANTECEDENTES

El trabajo es producto de la necesidad evidenciada en la región y la carencia de soluciones que aporten a la ciberdelincuencia en menores de edad del Huila. Una de las soluciones en el departamento del Huila fue la APP llamada *CyberEscudo autoría del Partido MIRA*; permitía una pedagogía a menores de edad, padres y educandos para aporta al buen uso de las tecnologías en el tema de la seguridad informática. Por otro lado, el departamento del Huila no cuenta con información fiable, completa y precisa por el cual las entidades del orden nacional e internacional pueda comunicar a la sociedad los diferentes ciberdelitos que han afectado a los Huilenses; estas situaciones están ligadas a circunstancias personales generando un desconocimiento por parte de las entidades judiciales por que la mayoría de los casos no se logra interponer la denuncia por factores que van desde el que dirán, vergüenza, etc. Estas consideraciones han marcado un antecedente y al mismo tiempo el punto de partida para generar soluciones que conlleve a implementar controles y conocimientos en la ciberseguridad con el ánimo de salvaguardar la integridad y libre desarrollo de los menos de edad en los diferentes entornos web.

En la actualidad, la sociedad en general es dependiente a los servicios TIC; sobre todo los niños(as) y adolescentes para responder con las obligaciones que trae el estudio teniendo en cuenta la pandemia, la necesidad de aprovechar los diferentes medios para entretenimiento y crear espacios sociales que permitan integrare con otras personas. La falta de conocimiento y buena práctica de los menores de edad genera la ocasión ideal para obtener información privada y esto a su vez impulsa el hecho delictivo afectando la dignidad de las personas por parte de los ciberdelincuentes.

Las medidas de control que hoy en día existen para evitar el flagelo de la ciberdelincuencia es un tema de información y práctica por pate del usuario; causa que ha originado un crecimiento en la problemática definida por la monografía a raíz de la inexperiencia de las buenas prácticas de la seguridad informática. Además, el poco interés por las instituciones educativas y empresas por capacitar, concientizar y brindar elementos a las personas en el buen uso de tecnología; ha generado una escasa participación y apoyo a incitativas que ayuden a proteger al individuo sobre los interese económicos en el ciberespacio.

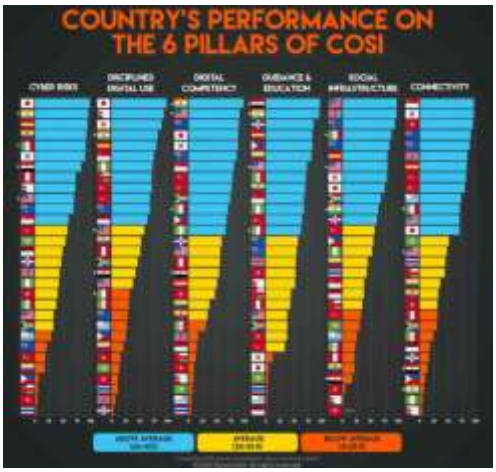
2.2 DESCRIPCIÓN

Colombia es uno de los países que cuenta con una estructura legislativa para tomar medidas preventivas y correctivas de los actos delictivos considerados por ley. Resultado de ello es la ley 1273 de 2009 correspondiente a los delitos considerado en la ciberseguridad, la ley 1581 de 2012 para la protección de los datos personales, entre otras. Aunque son normas que puede tener en el futuro una serie de modificaciones, no es un sistema eficaz que genere una respuesta contundente a los diferentes ciberdelitos identificados en la actualidad. Hoy en día se conocen una variedad de delictivos informáticos, hechos que generan una afectación propia según su aplicación en las víctimas: que para nuestro caso de estudio son los menores de edad en el departamento del Huila.

El panorama de la ciberseguridad en Colombia, no es muy alentador por los mismos avances y resultados obtenidos en la actualidad. Además, la sociedad ha demostrado un desequilibrio mental que se ve reflejado en las redes sociales y el internet por los casos reportados como ciberdelitos generando repudio en la sociedad sobre todo cuando las víctimas son menores de edad.

La ciberseguridad se debe tomar con responsabilidad y sobre todo en el momento preciso para identificar vulnerabilidades y riesgo mediante la implementación de las estrategias de control preventivo en el uso de los entornos web. Los ciberdelitos han afectado a los niños, niñas y adolescentes en el Huila y en Colombia mediante los casos reportados como el sexting, grooming, cirberacoso, sextorción, etc. El punto de partida de la monografía ha logrado identificar información incompleta sobre la situación real de los hechos en el Huila; por ende, es necesario reorientar el trabajo por medio de la aplicación de un cuestionario para obtener información directamente de los menores de edad y en el futuro los resultados de presente trabajo sirva de base para la toma de decisiones en la creación y divulgación de estrategias para la ciberseguridad en los menores de edad.

Figura 1. Posición de Colombia frente a la ciberseguridad para niños y adolescentes.



Fuente: https://www.semana.com/educacion/articulo/colombia-se-raja-en-ciberseguridad-para-ninos-y-adolescentes-informe/652523

La realidad sobre los ciberdelitos en Colombia y el Huila es impredecible; es necesario implementar mejoras en los procesos de ciberseguridad a partir de un referente o fuente de información verídica sobre el tema; para lograr avances y establecer las medidas correctas para proteger y cuidar a los menores de edad.

2.3 FORMULACIÓN DEL PROBLEMA

Basado en lo anterior surge la siguiente pregunta: ¿Cómo aportar información veraz con respeto a la ciberseguridad que permita aplicar las buenas prácticas de la seguridad informática en el Huila con el objeto de garantizar la protección y bienestar de los menores de edad según los derechos pactados en la constitución política de Colombia y las organizaciones internacionales?

3. JUSTIFICACIÓN

Los delitos cibernéticos han aumentado en un 45 %, según las cifras entregada por la Fiscalía General de la Nación (GUEVARA, s.f.); mientras en el departamento del Huila no se cuenta con una información completa y real. Las consultas realizadas directamente en las instituciones del orden departamental; ha permitido comprender que muchos de los problemas reportados hoy en día está asociado a crimines informáticos como robo de información personal, bancaria, entre otras. Son estos los resultados que evidencia la aplicación de los conceptos y técnicas definida desde la ciberseguridad a los intereses empresariales. Las razones descritas anteriormente se deben considerar con el mayor cuidado para generar un importante trabajo en la reducción en los ciberdelitos de forma general; especialmente a los niños, niñas y adolescentes del Huila.

El esfuerzo por parte de las entidades del estado en función de cada departamento, es tomar decisiones de forma preventiva y correctiva que permitan establecer medidas que aseguren la tranquilidad y seguridad de los usuarios en los diferentes medios incluyendo la Internet; para ello podemos tomar como referente la ley 1273 de 2009 y la ley 1581 de 2012. En la actualidad no hay una ley que permita responsabilizar y establecer conductas preventivas sobre la ciberseguridad en los diferentes entorno de trabajo en el territorio nacional; en la segunda plenaria del senado se presentó un proyecto: por la cual se formulaban los lineamientos de política pública para la prevención de delitos realizados a través de medios informáticos o electrónicos en contra de niñas, niños y adolescentes modificando el Código Penal y se dictan otras disposiciones (CONGRESO DE LA REPÚBLICA, 2018); la propuesta no logro ser aprobada por el Senado de Colombia y terminó en el archivo.

---

[4] GUEVARA, C. Aprobado proyecto de Ley de MIRA que busca combatir ciberdelitos. [En Línea]. Bogotá., Disponible en https://partidomira.com/aprobado-proyecto-de-ley-de-mira-que-busca-combatir-ciberdelitos/

[5] Congreso de la Republica de Colombia. PROYECTO DE LEY ____ DE 2018 "Por la cual se formulan los lineamientos de política pública para la prevención de delitos realizados a través de medios informáticos o electrónicos, en contra de niñas, niños y adolescentes, se modifica el Código Penal y se dictan otras disposiciones". [En línea]. Bogotá. disponible en http://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2018%20-%202019/PL%20074-18%20Crimenes%20Ciberneticos.pdf

La ciberseguridad es un mecanismo necesario e importante de estudiar y aplicar en los diferentes escenarios de la informática para salvaguardar y establecer una defensa contra los ciberdelitos que tiene como propósito atentar contra la información de índole personal, bancaria, etc. Estas situaciones entre otras cosas permiten una afectación directa sobre la persona según la magnitud de la circunstancia desencadenada por el hecho delictivo.

La importancia que toma la monografía es fundamental para la ciberseguridad de los menores de edad mediante la identificación de los controles a implementar en el departamento del Huila a partir del análisis de los ciberdelitos acontecidos durante los últimos 5 años a los niños, niñas y adolescentes. Esta postura busca identificar los alcances y limitaciones logrados en el Huila frente a la lucha contra los ciberdelitos en el departamento.

Por ende, el estudio de ciberseguridad en el departamento del Huila de los últimos 5 años; permitirá lograr el objetivo de la monografía y los requerimientos que se plantearon en el trabajo. Obteniendo de ello un análisis de los resultados de forma positiva para encaminar los esfuerzos en el departamento frente a la lucha contra la ciberdelincuencia que afecta en la actualidad a los niños, niñas y adolescentes.

4 OBJETIVOS

4.1 GENERAL

- Realizar un estudio con respeto a la ciberseguridad de los últimos 5 años en el Huila, mediante la búsqueda de información para identificar los problemas de seguridad que han dado pie a los ciberdelitos dirigidos a los niños, niñas y adolescentes.

4.2 ESPECÍFICOS

- Consultar la información actual sobre la ciberseguridad para los niños, niñas y adolescentes en el departamento del Huila en los últimos 5 años.
- Establecer datos estadísticos de los ciberdelitos suscitados en el departamento del Huila en los últimos 5 años.
- Analizar los hechos o acciones que han ocurrido entorno de los ciberdelitos de los niños, niñas y adolescentes en el departamento del Huila.
- Elaborar un informé para establecer los hechos que han afectado a los niños, niñas y adolescentes del Huila y recomendaciones sobre la ciberseguridad.

5 MARCO DE REFERENCIAL

5.1 MARCO CONCEPTUAL

5.1.1 Generalidades el marco conceptual es el ítem integrador entre los temas y el enfoque del estudio, partiendo de una premisa de estudio mediante la valoración de las características que favorecen el desarrollo de un análisis a diferentes fuentes de información y literaturas existente sobre el tema de estudio a partir de teorías que pretenden explicar el problema (MARTINEZ, 2012).

Además, la monografía aborda elementos que aportar al estudio un valor importante en el desarrollo de la misma, mediante la perspectiva en la selección de los procedimientos metodológicos para explicar la temática de interés y de la forma específica en la que analiza y difunde los resultados. En otras palabras, son los antecedentes socioculturales particulares que afectan su adhesión al orden normativo de la ciencia o a la interpretación (MARTINEZ, 2012).

La ciberseguridad es uno de los pilares fundamentales en la construcción y desarrollo del estudio involucrando los elementos que permitan asegurar los entornos web a los menores de edad y por ello se debe tener en cuenta: ante la coyuntura que ha obligado a las familias a permanecer en sus hogares para detener la propagación del COVID-19 y cuidar la salud de todos. Las clases han sido suspendidas, dejando a los niños en sus hogares buscando las formas para el entretenimiento y formación académica mediante el uso de los dispositivos móviles, tabletas o PC para navegar en el internet (Kaspersky, 2020).

[6] MARTINEZ, L. Marco conceptual en el proceso de investigación. [En línea]. 2012. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-50572012000300007

[7] KASPERSKY. Cuidado con la navegación en línea de los niños ¡Ojo a estos 7 consejos!. [En línea]. 2020. Disponible en: https://huila.extra.com.co/noticias/ciencia/kaspersky-cuidado-con-la-navegacion-en-linea-de-los-ninos-oj-599771

De acuerdo a la Cámara Colombiana de Informática y Telecomunicaciones, los delitos por malware o software malicioso: crecieron un 612% entre los años 2017 y 2019 (ARGUELLO, 2020). Estas consideraciones se deben asumir con responsabilidad desde la ciberseguridad y a partir de las situaciones identificadas lograr establecer las medidas necesarias mediante la plena identificación de las vulnerabilidades y riesgos que son victima los menores de edad.

5.1.1.1 Ciberdelito son las acciones indebidas en el internet con el firme propósito de generar un daño mediante la interacción con personas desconocidas, uso de software y sitios web no seguro, entre otras consideraciones que han logrado identificar la vulnerabilidad de los dispositivos de acceso a internet. También se considera como una: actividad ilegal llevada a cabo mediante el uso de tecnología donde los responsables pueden ser personas aisladas, grupos organizados o facciones con patrocinio estatal y utilizan técnicas como el pishing, la ingeniería social y el malware de todo tipo para cumplir sus siniestros planes (AVAST, s.f.).

Entre los ciberdelitos se conocen: malware, robo de identidad, cirberacoso, cryptojacking, ciberextorsion, ciberespionaje, pornografía infantil, sextorción, sexting, grooming (AVAST, s.f.). En la actualidad estos problemas están a un paso del internet y más cuando la persona no posee conocimiento frente al tema acercando al individuo a graves problemas de índole personal y económica.

[8] ARGUELLO, D. Ciberdelitos, la actividad criminal en un mundo virtual. [En línea]. 2020. Disponible en: https://www.lanacion.com.co/792782-2/

[9] AVAST. ¿Qué es el ciberdelito y cómo puede prevenirlo?. [E línea]. Disponible en: https://www.avast.com/es-es/c-cybercrime

5.1.1.2 Análisis comparativo es el estudio de los hechos relacionados con la investigación que permiten dirigir el trabajo a partir de una guía para la realización de estudios sistemáticos sobre los fenómenos cuantificables o inferenciales de la estadística (UNED, s.f.) que describe la trayectoria de una problemática.

El trabajo investigativo debe ser orientado desde un amplio abanico de cuestiones metodológicas para la atención teórica y técnica creciente en la rama del estudio en relación con el diseño, realización y presentación de la investigación (UNED, s.f.).

5.1.1.3 Línea de tiempo es una secuencia de eventos o de hitos sobre un tema, de tal forma que se visualice con claridad la relación temporal de los hechos (EDUCATIVO, s.f.).

A partir de la información lineal en el orden cronológico se pueden obtener un resumen de los sucesos que aborda un tema específico con la definición de los elementos importantes para su interpretación.

5.1.1.4 Retos son los compromisos o esfuerzos para lograr un objetivo en particular definiendo soluciones para una necesidad real detectada previamente (UTPL, s.f.). Tiene en cuenta el desarrollo de la investigación destacando la adquisición de conocimiento para contribuir a la sociedad y a la ciberseguridad.

---

[10] UNED. Metodología cualitativa: análisis comparativo y estudios de caso. [En línea]. Disponible en: http://portal.uned.es/portal/page?_pageid=93,53594848&_dad=portal&_schema=PORTAL&idAsignatura=29901088

[11] PORTAL EDUCATIVO. ¿Qué es una línea de tiempo y cómo se organizan?. [En línea]. Disponible en: https://www.portaleducativo.net/quinto-basico/507/Que-es-una-linea-de-tiempo-como-se-organizan

[12] UTPL. ¿Qué es un reto?. [En línea]. Disponible en: https://retos.utpl.edu.ec/?q=es/que_es_un_reto

Para este enfoque se debe comprender los elementos obtenido en la investigación para proyectar la solución y lograr los resultados esperados con respeto a la ciberseguridad de los niños, niñas y adolescentes del Huila.

5.1.1.5 Redes sociales es un servicio establecido para los usuarios con el propósito de interactuar con otras personas e intercambiar información en diferente índole. Los propósitos de estos nuevos servicios se configuran como poderosos canales de comunicación e interacción para crear grupos de seguidores en la forma de generar una fuente de información para entretenimiento, comunicación, empleo, etc. (UNILIBRE, 2016).

Todos los usuarios registrados en las redes como Facebook, Twitter, Instagram, etc. Implica publicar información de índole personal de modo voluntario, pero no siempre estas consciente de ello (UNILIBRE, 2016) razón que lleva a materializar un riesgo para los usuarios por la facilidad en la consulta de información privada de las personas en los diferentes medios de la internet.

5.1.1.6 Buena práctica son todas aquellas actividades con bases sólida en el conocimiento para evitar un mal uso de los recursos y conservar la integridad de la información en los diferentes entornos web.

Las buenas prácticas tiene como objeto dar a conocer cómo tratar los riesgos que suponen una amenaza que está asociada a la forma de gestionar los datos, por el cual se especifican un conjunto de prácticas aportando a la seguridad de las operaciones y la gestión de incidentes (INCIBE, Buenas prácticas en el área de informática, s.f.)**.**

[13] UNILIBRE. Redes sociales: El uso y el abuso. [En línea]. 2016. http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/2349-redes-sociales-el-us-y-el-abuso

[14] INCIBE. Buenas prácticas en el área de informática**.** [En línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/buenas-practicas-area-informatica

5.1.1.7 Desconocimiento está relacionado con la falta de conocimiento o experticia en el uso de una herramienta web donde es posible gestionar cualquier tipo de información de una persona. Esta situación aumenta el grado de vulnerabilidad en la seguridad de la información por errores humanos que conlleva a materializar un ciberdelito.

Si aún no cree que adquirir conocimientos y habilidades relacionados con las herramientas tecnológicas sea un tema por el cual preocuparse, creemos que es momento de que empieces a considerarlo (MANAGER, s.f.).

El conocimiento permite un acercamiento al éxito y al mismo tiempo genera la confianza de las operaciones que realiza en cualquier herramienta con acceso al ciberespacio para proteger los datos y la integridad de una persona ante un ciberdelito.

5.1.1.8 Cultura informática son los hábitos o costumbre en la forma repetida y controlada de proceder ante la agestión de la información en los medios tecnológicos.

También se considera las habilidades básicas en la utilización de la informática como apoyo a la actividad del individuo y se considera útil en cualquier área de aplicación utilizando como apoyo la búsqueda, procesamiento y presentación eficiente de la información mediante las herramientas, técnicas y conocimiento del estado actual de los datos (ECURED, s.f.).

[15] TIME MANAGER. Riesgos del desconocimiento de las herramientas tecnológicas de uso diario, una cuestión de ética. [En línea]. Disponible en: https://www.timemanagerweb.com/riesgos-del-desconocimiento-de-las-herramientas-tecnologicas/

[16] EcuRed. Cultura informática. [En línea}. Disponible en: https://www.ecured.cu/Cultura_inform%C3%A1tica

5.1.1.9 Ley 1273 de 2009 determina toda aquella procedencia para impartir un juicio en el mal usos de la infraestructura tecnológica de una empresa u organización para socavar la información o afectar un sistema de forma indebida.

La ley estable los actos inapropiados sobre un sistema de información mediante el accesos abusivos, obstaculización legítima, interceptación de datos, daño informático, uso de software malicioso, violación de datos personales y suplantación de sitios web (SENADO, 209).

Todo daño en los sistemas de información es la evidencia para generar una pena punitiva de índole carcelaria y económica teniendo al ciberdelincuente teniendo en cuenta la magnitud del daño.

5.1.1.10 La ley 1581 de 2012 mecanismo para la protección de los datos personales y con ello refrenar los actos delictivos a nombre de personas incautas en el tratamiento de estos sin la debida autorización.

La ley pretende generar principios sobre la protección de los datos en todos los motores de almacenamiento con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal (SENADO S. , 2012).

El tratamiento de los datos debe considerar el consentimiento del usuario y no podrá beneficiar con ello a terceros ni mucho menos para hacer un daño directo o indirecto a una persona a través de los medios tecnológicos.

[17] SECRETARIA SENADO. Ley 1273 de 2009. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[18] SECRETARIA SENADO. Ley 1581 de 2012. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

5.1.1.11 Ciberseguridad es el procedimiento o guía de la seguridad informática para asegurar la información y establecer las buenas prácticas en el uso del internet, redes sociales u otras plataformas.

Las ciberamenazas mundiales siguen desarrollándose a un ritmo acelerado, con una cantidad cada vez mayor a la filtración de datos en cada año. En el informe por RiskBased Security, reveló la siguiente cifra que de hecho es alarmante: 7900 millones de registros han sido expuestos por filtraciones de datos solo en los primeros nueve meses del 2019. Esta cifra es más del doble (112 %) de la cantidad de registros expuestos en el mismo período durante el 2018 (Kaspersky, ¿Qué es la ciberseguridad?, s.f.). El panorama para Colombia no es muy alentador en el años 2019 con 28.000 casos reportados (DATA, s.f.).

Ante la creciente ola de amenazas en el internet, es necesario fortalecer los procedimientos que permiten mitigar los riesgos y vulnerabilidades en el uso de los elementos tecnológicos y servicios por medio de la aplicación correcta de la ciberseguridad y las buenas prácticas en una cultura determinante y retroalimentada día a día.

5.1.1.12 Informática es el proceso para automatización de la información mediante gestión de los datos que permita obtener un menor tiempo de respuesta y rendimiento de la información de forma veraz y completa.

[19] KASPERSKY. ¿Qué es la ciberseguridad?. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[20] PROTE DATA. Ciberseguridad – En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. [En línea]. Disponible en: https://protecdatalatam.com/ciberseguridad-en-2019-se-reportaron-mas-de-28-000-casos-de-ciberataques-en-colombia/#:~:text=Convenios-,Ciberseguridad%20%E2%80%93%20En%202019%20se%20reportaron%20m%C3%A1s%20de,casos%20de%20ciberataques%20en%20Colombia&text=Adem%C3%A1s%2C%20de%20los%2028.827%20casos,los%20delitos%20inform%C3%A1ticos%20en%20Colombia.

El concepto está muy relacionado al orden de los datos, ya que un conjunto de datos empleados sin ningún orden nos daría una información diferente de la deseada o incluso podría no aportar ninguna información (UNNE, s.f.).

Para ello, el sistema de información debe gestionar los datos para obtener information integra y veraz a través de las consultas. Es aquí donde juega un papel fundamental la ciberseguridad y con ello determinante para el alcance de la información que podrá ser consultada mediante la identificación de los usuarios y los privilegios que tendrán en el sistema con el interés de evitar un inadecuado procedimiento en las bases de datos.

5.1.1.13 Datos es un conjunto de caracteres agrupados para definir los datos y con ello lograr ser almacenado y procesado en las base de datos. Es el punto de partida en la organización y definición de la información en las diferentes plataformas web.

Un dato es una representación simbólica (numérica, alfabética, etc.) de un atributo o característica de una entidad. El dato no tiene valor semántico (sentido) en sí mismo, pero convenientemente tratado (procesado) se puede utilizar en la realización de cálculos o toma de decisiones (UCLA, s.f.).

5.1.1.14 Información es un conjunto de datos que permita obtener en detalle una información que puede guardar en relación de un tema específico. Este activo constituye un valor fundamental e importante en los sistemas de información.

La información tiene una aplicabilidad coherente y específica en la gestión de las plataformas computacionales para lograr:

[21] UNNE. Informática. Conceptos fundamentales. [En línea]. Disponible en. http://exa.unne.edu.ar/ingenieria/computacion/Tema1.pdf

[22] UCLA. Guía de Estudio No. 1. Datos e Información. [En línea]. Disponible: http://www.ucla.edu.ve/dac/departamentos/informatica%20I/sesion%20no.%201.pdf

- Aumentar/mejorar el conocimiento del usuario, o dicho de otra manera reducir la incertidumbre existente sobre un conjunto de alternativas lógicamente posibles.
- Proporcionar a quien toma decisiones la materia prima fundamental para el desarrollo de soluciones y la elección.
- Proporcionar una serie de regla de evaluación y regla de decisión para fines de control (EcuRed, s.f.).

5.1.1.15 Investigación actividad que permite explorar un escenario o conocimiento con el propósito de adquirir nueva información del cual pueda ser aplicado en otros contextos para generar soluciones a partir de un conocimiento adquirido por la investigación.

El estudio se basa en recabar información sobre un tema determinado, además de tratar de conocer algo a partir de la examinación de ciertos detalles. Ahora bien, la investigación puede definir el proceso metódico, sistematizado, objetivo y ordenado, que tiene como finalidad responder ciertas preguntas, teorías, suposiciones, conjeturas y/o hipótesis que se presentan en un momento dado sobre un tema específico. La investigación además permite la adquisición de conocimientos e información sobre un tema o asunto que se desconoce (ISBL, 2018).

5.1.1.16 Estudio es el desarrollo de una investigación junto a la aplicación de una metodología para obtener resultados conducentes en la construcción y definición de la información mediante una necesidad especifica.

El resultado de un estudio frente a un análisis de datos conlleva a generar valor a la información frente a las investigaciones para aportar conocimiento y modelación de la realidad con el propósito de establecer estrategia y elementos en la solución de una necesidad.

[23] EcuRed. Información. [En línea]. Disponible en: https://www.ecured.cu/Informaci%C3%B3n

[24] ISBL. ¿Qué se entiende por investigación? [En línea]. 2018. Disponible en: https://isbl.eu/que-se-entiende-por-investigacion/

5.1.1.17 Niño (a) es el estado inicial de una persona donde aprende lo que ve e interactúa con otras personas. Esta etapa se puede explorar el mundo que les rodea y al mismo tiempo desarrollar habilidades para su crecimiento cognoscitivo y emocional.

Es una época valiosa en la que los niños y las niñas deben vivir sin miedo, seguros frente a la violencia, protegidos contra los malos tratos y la explotación (UNICEF, s.f.) incluyendo el escenario tecnológico.

5.1.1.18 Adolescente es el estado maduro del niño, permite tomar decisiones y comprender ciertas situaciones de la vida de forma consiente y seguro de los deseaos para sí mismo.

En la adolescencia se puede desarrollar una forma diferente de ver el mundo, el pensamiento abstracto, que permite un gran distanciamiento de la realidad inmediata para juzgarla a partir de lo que podría ser, imaginar otras posibilidades además de las que existen, pensar sobre los propios procesos psicológicos, sobre lo que se piensa o lo que se siente, tratar de explicar lo que sucede a través de múltiples hipótesis, o analizar todas las posibilidades y valorar la realidad como una de dichas posibilidades (INJUVE, s.f.)

5.1.1.19 Internet es un servicio mundial para intercambiar información y comunicar a los individuos sin importar las distancias. Esta tecnología permite acceder a todo tipo de información y servicios donde se debe tener en cuenta la seguridad por parte del usuario en los sistemas de información para evitar algún tipo de riesgo o problema que pueda estar comprometido un usuario incauto.

[25] UNICEF. Definición de infancia. [En línea]. Disponible en: https://www.unicef.org/spanish/sowc05/childhooddefined.html

[26] INJUVE. EL SIGNIFICADO DE LA ADOLESCENCIA. [En línea]. Disponible en: http://www.injuve.es/sites/default/files/027-036-Violencia3_2.pdf

[27] INTERNET SOCIETY. Breve historia de Internet. [En línea]. Disponible en: https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/

Internet es una herramienta con propósito múltiple a nivel mundial, mecanismo desarrollado para intercambiar información, medio para el trabajo colaborativo, interacción social mediante un dispositivo para establecer la conexión a los servicios de la red global (SOCIETY, s.f.).

5.1.1.20 Vulnerabilidad son errores o situaciones que puede comprometer un sistema de información por medio de una amenaza o debilidad que puede ser identificada para ingresar de forma ilegítima para cometer un ciberdelito.

El análisis de este tipo; tienen en cuenta todos y cada uno de los aspectos que puedan representar un riesgo que comprometer la información de la empresa o personal. Es necesario la seguridad perimetral y la sensibilización a las personas para generar un escenario adecuado y seguro en l software (ACCENSIT, s.f.).

El tema debe ser abordado con una sutil delicadeza y trato para salvaguardar la triada en cuanto a la seguridad de la información y evitar la exposición de datos personas al público.

5.1.1.21 Amenaza es la exposición que compromete la información o activos que se encuentra clasificado o protegido desde la ciberseguridad**.**

La amenaza es aprovechada por el ciberdelincuente para identificar y atenta contra la seguridad de un sistema de información. Es decir, que podría tener un potencial negativo sobre algún elemento de nuestros sistemas.

[28] ACCENSIT. Análisis de vulnerabilidad informática: ¿En qué consiste?. [En línea]. Disponible en: https://www.accensit.com/blog/analisis-vulnerabilidad-informatica-en-que-consiste/

[29] INCIBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?. 2017. [En línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Las amenazas pueden proceder en ataque informáticos (fraude, robo, virus), sucesos del ambiente (incendios, inundaciones, etc.), decisiones institucionales equivocadas (mal manejo de contraseñas, no usar cifrado) (INCIBE, Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?, 2017).

5.1.1.22 Riesgo es la exposición de un sistema de información ante un ciberdelito y con ello acarrea graves consecuencias por la falta de políticas y controles en la ciberseguridad.

La protección de datos y sistemas valiosos en el espacio digital se ha vuelto sumamente importante; asegurar los sistemas y las diferentes tecnologías informáticas (TI) es un reto en la actualidad mediante la capacitación y sensibilización (ATALAIT, 2017).

5.1.1.23 Software programas informáticos con unas funciones propias para gestionar la información, agilizar y mejorar las tareas en los proceso de las áreas específicas.

Soporte lógico de un sistema informático; es decir, es la parte no física que hace referencia a un programa o conjunto de programas de cómputo que incluye datos, reglas e instrucciones para poder comunicar con el ordenador y responder ante requerimientos por un usuario (CISET, s.f.)**.**

El software permite que un usuario común pueda tener acceso a mediante el alcance de los servicios establecidos para la administración de la información mediante la identificación de usuarios y las actividades autorizadas en la plataforma web.

[30] ATALAIT. Riesgos informáticos en una empresa. 2017. [En línea]. Disponible en: https://www.atalait.com/blog/riesgos-informaticos-en-una-empresa

[31] CISET. Software - Concepto y tipos de software. [En línea]. Disponible en: https://www.ciset.es/glosario/480-software

5.1.1.24 Sexting es la trasmisión de información que contiene elementos sexuales sin la debida autorización por parte de la víctima con el interés de publicar ese contenido en las redes sociales e internet violando la privacidad y haciendo publico la información privada y personal.

Teniendo claro el concepto, se puede inferir lo siguiente: el menor de edad no es consciente de la amenaza que puede atentar contra su bienestar, ni las implicaciones desde el punto de vista de la seguridad: la exposición de los datos personales, privados e íntimos a través de las nuevas tecnologías de la comunicación para ser difundido en el mundo entero. Esta situación determina el grado alto sobre el riesgo que está expuesto un menor edad por que la información privada será consumida como los contenidos para adultos (CAIB., s.f.).

5.1.1.25 Grooming es el medio utilizado en internet para establecer una comunicación con una persona desconocida para buscar elementos privados y con ello generar un daño a la víctima.

Conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza de un menor de edad a través de la Internet, con el fin de obtener contenidos de índole sexual. El grooming puede estar íntimamente relacionada con la sextorsión; para obtener un benéfico de ello. El propósito de los contenidos es lograr su comercialización en el ramo de la pornografía. Los menores de edad son obligados y seducidos ante una serie de amenaza y finaliza con la destrucción de las emociones y psicológica de una persona (CAIB., s.f.).

5.1.1.26 Cirberacoso actos temerarios para ridiculizar a otras personas por medio de la Internet y generar una conducta inapropiadas en el ser humano por sometimiento.

[32] CAIB. Qué es el sexting?. [En línea]. Disponible en: http://www.caib.es/sites/ciberconviu/es/que_es_el_sexting-68265/

El hostigamiento de un menor de edad a otro en forma de insultos, vejámenes, amenazas, chantaje, etc. Son trasmitidos por medio de un canal tecnológico. El propósito del ciberdelito es la forma para ejercer la humillación pública, ciberbullying, en caso de que compañeros del menor utilicen cualquier elemento para burlarse, hacer comentarios públicos, etc. Las burlas pueden ser puntuales o prolongarse a lo largo del tiempo v(CAIB., s.f.).

5.1.1.27 Sextorción aprovechando los contenidos íntimos, exige una indemnización a cambio de no publicar información íntima del individuo obtenida de forma indebida.

El adolescente, temeroso ante la posibilidad de que su sextorsionador pueda dar difusión a imágenes sensibles que le comprometerían públicamente, puede tomar la decisión de acceder a su chantaje, que normalmente consiste en seguir enviándole fotografías o vídeos de carácter sexual y en casos extremos realizar concesiones de tipo sexual con contacto físico. De esta manera, el adolescente puede entrar en una espiral cuya salida pasa por no acceder a las pretensiones del hostigador, y comunicar la situación a un adulto (CAIB., s.f.).

5.1.1.28 Pornografía infantil es la publicación de fotos y videos intimitos pasando por alto la ley de un país y vulnerando los derechos fundamentales de una persona. A demás, este problema: deja cifras tan alarmantes como: cada siete minutos se muestra en Internet a un menor siendo objeto de abusos sexuales (MORA, 2019).

Los organismos que vela para que los contenidos que circulan en la red deben considerar propios y pertinente para la población que accede a estos; el año pasado se eliminó 78.589 páginas web de todo el mundo que ofrecían este tipo de imágenes (MORA, 2019).

[32] CAIB. Qué es el sexting?. [En línea]. Disponible en: http://www.caib.es/sites/ciberconviu/es/que_es_el_sexting-68265/

[31]. MORA, A. Pornografía infantil: la cara oscura de Internet. 2019. [En línea]. Disponible: https://elpais.com/elpais/2018/11/15/planeta_futuro/1542292342_375507.html

Desde 1996, IWF ha borrado más de 250.000 páginas con contenido pedófilo. “En cada fotografía, en cada vídeo, hay una agresión sexual, una violencia ejercida y una violación de los derechos de los niños y las niñas. Además, Del contenido analizado y eliminado por IWF en 2017, se desprende que el 43% de las víctimas tiene entre 11 y 15 años y que el 55% tiene 10 años o menos. También deja ver que en el 33% de los casos hubo violación o tortura (MORA, 2019).

5.1.1.29 Perjuicio es un hecho que genera un mal de índole físico o moral producto de un sufrimiento o la pérdida de algo muy importante para un individuo ocasionado un sufrimiento.

Un juicio u opinión, generalmente negativo, que se forma sin motivo y sin el conocimiento necesario. Supone tener una actitud negativa y hostil hacia una persona que identificamos como perteneciente a un grupo, por el simple hecho de pertenecer a ese grupo (LEIOA, s.f.).

5.1.1.30 ONU es el organismo internacional que vela por el cumplimiento de la ley para asegura los derechos fundamentales de las personas definidos por los estados que los conforman a nivel internacional.

Los temas principales en la agenda de trabajo son: la paz, derechos humanos, asuntos humanitarios, desarrollo y derecho internacional. Teniendo en cuenta el estudio de ciberseguridad; busca enfatizar la seguridad y cuidado de los menores de edad según la ley y los medos para promover y velar por el debido cumplimiento de los derechos internacionales. Entendiendo como entidad que permite la promoción y protección de los derechos fundamentales y principios que son los elementos rectores de la Organización (ONU, s.f.).

[33] MORA, A. Pornografía infantil: la cara oscura de Internet. 2019. [En línea]. Disponible: https://elpais.com/elpais/2018/11/15/planeta_futuro/1542292342_375507.html

[34] LEIOA. Prejuicios y estereotipos y cómo influyen en la convivencia. [En línea]. Disponible en: http://www.leioa.net/vive_doc/prejuicios-y-estereotipos-es.pdf

[35] ONU. Que hacemos. [En línea]. Disponible en: https://www.un.org/es/sections/what-we-do/index.html

5.1.1.31 UNICEF organización que trabaja con el apoyo de 190 países y territorios para salvar las vidas de los niños y para defender sus derechos. Busca alternativa y mecanismo para alcanzar su máximo potencial desde los enfoques de: protección de la infancia e inclusión, supervivencia infantil, educación, política social, en situaciones de emergencias, genero, innovación en benéficos de los niños, suministro y logística, investigación y análisis (UNICEF, Que hacemos, s.f.).

5.1.1.32 Instituciones públicas son aquellas que tiene como actividad específica el orden nacional, departamental y municipal para velar por el debido cumplimiento de la ley y asegurar los derechos fundamentales de una persona. Las instituciones que hacen parte del estado en el tema de seguridad y bienestar de los menores de edad son identificadas como: la Defensoría del Pueblo, Gobernación, ICBF, Policía Nacional, Fiscalía, Dijín, etc.

Estas entidades deben aseguran la integridad y amparo de las personas para evitar que los ciberdelitos puedan afectar el libre desarrollo y crecimiento de la sociedad que hoy conocemos en los diferentes espacio en su interacción social.

[36] UNICEF. Que Hacemos. [En línea]. Disponible en: https://www.unicef.org/es/que-hacemos

5.2 MARCO TEÓRICO

5.2.1 Defensa activa e inteligencia: de la teoría a la práctica Es un conocimiento vital que genera una importancia para visionar aquellos sucesos que han de ocurrir, pensado como un atacante para detectar vulnerabilidades y con ello definir una respuesta casi que inmediata por medio de adaptaciones de seguridad en los diferentes elementos de trabajo continuo para alcanzar el objetivo de calidad y aseguramiento. La evolución y sofisticación de los ataques es algo más que evidente, pero también los mecanismos de defensa que han evolucionado (INCIBE, Defensa activa e inteligencia: de la teoría a la práctica, 2018) para generar un baluarte de la seguridad informática.

5.2.2 Colombia se 'raja' en ciberseguridad para niños y adolescentes: informe El acceso seguro a la Internet es uno de los temas que más inquieta a muchas familias, docentes y expertos en educación (REVISTA SEMANA, Colombia se 'raja' en ciberseguridad para niños y adolescentes: informe, 2020) razón por el cual, hace que el tema genere una preocupación para la seguridad de los niños, niñas y adolescentes por las cifras infladas sobre de los ciberdelitos que son ejecutados en todo momento en los sitios web; donde la despreocupación pasa un factura costosa al considerar las recomendaciones de la seguridad informática como innecesaria; al tiempo que el desconocimiento de las buenas prácticas impulsa a la población la oportunidad perfecta para ser víctima de un ciberdelito.

5.2.3 Los niños como sujetos sociales. Notas sobre la antropología de la infancia Los niños y niñas, son considerados como actores importantes en una sociedad y pilar del futuro para construir sociedad. Razón, que lleva afirmar la importancia en incluir la seguridad informática en los acostumbrados entornos web para mitigar los riesgos que pueden ser expuestos los menores de edad en los entornos web.

---

[37] INCIBE CERT. Defensa activa e inteligencia: de la teoría a la práctica. [En línea]. 2018. Disponible en: https://www.incibe-cert.es/blog/defensa-activa-e-inteligencia-teoria-practica

[38] Revista Semana. Colombia se 'raja' en ciberseguridad para niños y adolescentes: informe. [En línea]. 2020. Disponible en: https://www.semana.com/educacion/articulo/colombia-se-raja-en-ciberseguridad-para-ninos-y-adolescentes-informe/652523

El deber de las entidades del gobierno es garantizar una sociedad que logre mitigar los peligros y amenazas que se ven enfrentados en pleno siglo XXI; La información tiene una aplicabilidad coherente y específica en las plataformas web para lograr la aplicabilidad coherente y específica al desarrollo de las plataformas computacionales para lograr que los niños les pueda ofrecer confianza, protección y oportunidad que están contemplados en derechos constitucionales (CALDERON CARRILLO , 2015).

5.2.4 Los niños frente a Internet: seguridad, educación y tecnología La vulnerabilidad que se ve expuesto un menor de edad, hace pensar en crear espacios y herramientas para protegerlos de un entorno virtual inseguro en la internet; aquella puerta que permite una opción ilimitada a un mundo desconocido con miles de peligros que se convierte en problemas y sucesos que puede desencadenar en líos a los niños, adolescentes y familia. Para las generaciones que han crecido paralelamente al desarrollo tecnológico, el espacio virtual representa una realidad complementaria de la fáctica, que les otorga identidad (VAUNELLO GLADYS , 2015).

5.2.5 Internet, un sitio sin bondad para los jóvenes esta premisa parte de la inseguridad que trae el Internet; un espacio abierto, sin cesura y la libertad de expresar o compartir contenidos sin el más mínimo cuidado a las persona. Razón que ha llevado a la ONU a considerar que el cirberacoso es un problema en crecimiento que afecta a 1 de cada 10 niños en el mundo y sus víctimas tienen una probabilidad mayor de sufrir baja autoestima, problemas de salud, y adicciones según la UNICEF (ONU, Internet, un sitio sin bondad para los jóvenes, 2019). Adema, la ONU visualiza la violencia en línea y el acoso digital representan un gran peligro para los niños y jóvenes que tienen acceso a internet a nivel mundial y es necesario tomar medidas (ONU, Internet, un sitio sin bondad para los jóvenes, 2019).

---

[39] CALDERÓN, D. Los niños como sujetos sociales. Notas sobre la antropología de la infancia. [En línea]. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-06362015000100007

[40] VUANELLO, G. Los niños frente a Internet: seguridad, educación y tecnología. [En línea]. 2015. Disponible en: https://www.redalyc.org/articulo.oa?id=60741185005

[41] ONU. Internet, un sitio sin bondad para los jóvenes. 2019. [En línea]. Disponible en: https://news.un.org/es/story/2019/02/1450561

.

Los adolescentes y jóvenes en países desarrollados el 94% se conecta a internet y en subdesarrollo el 65%; por último y grave el Internet se ha convertido en un elemento esencial de la vida de los jóvenes independientemente al nivel de ingresos (ONU, Internet, un sitio sin bondad para los jóvenes, 2019).

5.3 MARCO ESTADO DEL ARTE

A continuación se presentan algunos proyectos orientados a la ciberseguridad de los niños, niñas, y adolescentes; esta información genera un antecedente y punto de partida para el estudio. La siguiente tabla describe los avances del tema teniendo en cuenta los siguientes proyectos:

Tabla 1. Estado del arte

AUTORES	**TÍTULO**	**AÑO**	**PAÍS**	**RESUMEN**
CAROLINA MONTES AGUDELO Y VIVIANA ROCIO VARGAS FORERO	PROBLEMAS DE INGENIERÍA SOCIAL Y SU IMPACTO EN LA ADOLESCENCIA COLOMBIANA	2018	COLOMBIA	Monografía presenta un análisis de los problemas a los que se ven abocados los adolescentes a causa de la ingeniería social, en el contexto de las actuales costumbres del manejo de las redes (MONTES AGUDELO & VARGAS FORERO, 2018)
PATRICIA ALONSO RUIDO	EVALUACIÓN DEL FENÓMENO DEL SEXTING Y DE LOS RIESGOS EMERGENTES DE LA RED EN ADOLESCENTES DE LA PROVINCIA DE OURENSE	2017	ESPAÑA	El estudio del fenómeno del Sexting y de los riesgos emergentes vinculados al uso de las tecnologías y espacios virtuales, aunque todavía escasamente conocidos, representan una línea de investigación que está acaparando una creciente atención en España derivada de las negativas consecuencias que tienen asociadas (ej. Sextorsión, Grooming, Ciberbullying o Teen Dating Violence) (ALONSO RUIDO, 2017).
LILIANA MARÍA POSADA GIL	RIESGOS EN EL USO DE INTERNET EN LOS ESTUDIANTES DE LA INSTITUCIÓN EDUCATIVA JOAQUÍN CÁRDENAS GÓMEZ DEL MUNICIPIO SAN CARLOS (ANT), PARA EL AÑO ESCOLAR 2015.	2015	COLOMBIA	Esta investigación exploró los riesgos a los que están expuestos los estudiantes del grado sexto hasta el grado once de dicha institución al hacer uso de Internet y las actividades rutinarias que ellos realizan (POSADA GIL, 2015).
CAMILO ALFONSO GUZMAN FLOREZ Y CRISTIAN ANDRES	PROTOCOLOS PARA LA MITIGACION DE CIBERATAQUES EN EL HOGAR. CASO DE ESTUDIO: ESTRATOS 3 Y 4 DE LA CIUDAD DE BOGOTÁ	2017	COLOMBIA	Por estas vulnerabilidades se propuso un documento que contenga protocolos permitiendo preparar a una persona del común para mitigar la probabilidad de un ciberataque en su hogar identificando herramientas y brindando conocimientos para su

ANGARITA PINZON				protección (Angarita Pinzón & Guzmán Flórez, 2017).
MARIA JULISSA ZAMBRANO MACÍAS	CIBERSEGURIDAD: RIESGO Y AMENAZAS DE LOS JOVENES EN LAS REDES SOCIALES CASO: COELEGIO FISCAL MIXTO CAMILO PONCE	2018	ECUADOR	El uso de la tecnología de manera constante por los jóvenes permite generar uno riesgo que pueden fracturar a ciberseguridad de los entes de formación (ZAMBRANO MACIAS , 2018).

Fuente:

- AGUDELO, Carolina y VARGAS, Viviana. PROBLEMAS DE INGENIERÍA SOCIAL Y SU IMPACTO EN LA ADOLESCENCIA COLOMBIANA. [En línea]. 2018. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/22583/41946700.pdf?sequence=1&isAllowed=y
- ALONSO, Patricia. Evaluación del fenómeno del Sexting y de los Riesgos emergentes de la Red en adolescentes de la Provincia de Ourense. [En línea]. 2017. Disponible en: http://www.investigo.biblioteca.uvigo.es/xmlui/bitstream/handle/11093/786/Evaluaci%C3%B3n_del_fen%C3%B3meno_del_sexting.pdf?sequence=1
- POSADA, Liliana. RIESGOS EN EL USO DE INTERNET EN LOS ESTUDIANTES DE LA INSTITUCIÓN EDUCATIVA JOAQUÍN CÁRDENAS GÓMEZ DEL MUNICIPIO SAN CARLOS (ANTIOQUIA), PARA EL AÑO ESCOLAR 2015. [En línea]. 2015. Disponible en: https://repository.upb.edu.co/bitstream/handle/20.500.11912/2853/INFORME_FINAL_LILIANAPOSADAGIL.pdf?sequence=1
- ANGARITA, Cristian y Guzmán, Camilo. CIBERSEGURIDAD HOGAR CIBERSEGURIDAD VULNERABILIDADES RIESGOS PROTOCOLOS. [En línea]. 2017. Disponible en: https://repository.ucatolica.edu.co/handle/10983/15321
- ZAMBRANO, María. Ciberseguridad: riesgo y amenazas de los jóvenes en las redes sociales caso: Colegio fiscal Mixto Camilo Ponce. [En línea]. 2018. Disponible en: https://repositorio.uleam.edu.ec/bitstream/123456789/1756/1/ULEAM-PER-0031.pdf

5.4 MARCO HISTÓRICO

5.4.1 INCIBE acerca de la ciberseguridad a niños de 5 a 8 años mediante un nuevo recurso

método educativo orientado a niños y niñas de 5 a 8 años para fomentar el uso correcto de internet e identificar elementos que genere el ambiente correcto que les permita garantizar su integridad y libre desarrollo.

La ciberseguridad se debe tratar como ejemplo educativo el desarrollo de una guía didáctica ‘Comenzamos con ciberseguridad’: iniciativa que pretende que los más pequeños tomen un primer contacto con la seguridad de la información, aprendan a utilizar las tecnologías de forma segura, positiva y eviten riesgos (INCIBE, INCIBE acerca la ciberseguridad a niños de 5 a 8 años mediante un nuevo recurso, 2019).

5.4.2 Problemas de ingeniería social y su impacto en la adolescencia Colombiana Estudio realizado por estudiante en la modalidad de grado para aportar elementos y conocimientos a los adolescentes de Colombia en la búsqueda de mitigar el problema de ingeniería social; permitiendo concluir: la falta de conocimiento en seguridad informática refleja la exposición las amenazas y riesgos en el ciberespacio (UNAD, 2018).

La información que un adolescente sube a las redes sociales divulga información personal acerca de: (Donde vive - Cuáles son sus traslados frecuentes - Cuáles son sus lugares favoritos - Donde estudia - Cuáles pueden ser sus contraseñas de redes sociales - Publicación de fotografías que pueden ser utilizadas para dañar o vulnerar su integridad) Uno de tantos fenómenos que se ven en la actualidad con respecto al uso de las redes sociales (UNAD, 2018).

5.4.3 Cirberacoso de niños, niñas y adolescentes en las redes sociales: un estudio sobre los sistemas de protección y prevención judicial Propuesta de grado enfocado en comprender situaciones agresivas contra la los menores de edad; impulsando el desarrollo de herramientas correspondientes para la vigilancia y promoción de espacios seguros que mitigue los ciberdelitos.

La responsabilidad del estado a través de las instituciones del orden nacional, departamental y municipal es garantizar el cumplimento de los derechos constitucionales a los menores de edad; aún más, cuando se trata de situaciones en las que se ven totalmente vulnerados como es el caso de la pornografía infantil y el cirberacoso; resaltando la necesidad de implementar las medidas de la ciberseguridad contundentes por parte de toda la comunidad (Rojas D., 2015)

[42] INCIBE. Acerca la ciberseguridad a niños de 5 a 8 años mediante un nuevo recurso. 2019. [En línea]. Disponible en: https://www.incibe.es/sala-prensa/notas-prensa/incibe-acerca-ciberseguridad-ninos-5-8-anos-mediante-nuevo-recurso

[43] UNAD. Problemas de ingeniería social y su impacto en la adolescencia colombiana. 2018. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/22583

[44] Rojas D, Caycedo O. Cirberacoso de niños, niñas y adolescentes en las redes sociales: un estudio sobre los sistemas de protección y prevención judicial. 2015. [En línea]. Disponible en: https://repository.ucatolica.edu.co/handle/10983/2564

5.4.4 Delitos de abuso y explotación sexual infantil problemática mundial y sin escrúpulos en la búsqueda de beneficio económico pasando por alto la ley internacional según la UNICEF: invitan a la ciudadanía a proteger a niñas, niños y adolescentes del abuso y explotación sexual (UNICEF, Delitos de abuso y explotación sexual infantil, 2018).

La problemática no solo se basa en la publicación de contenidos, sino también en la explotación y turismo sexual magnificando el problema que afecta a Colombia y el Huila. Todas estas situaciones son impulsadas por negocios ilegales mediante redes ocultas bajo la modalidad de los negocios corruptos que ofrece un lucrativo beneficio por medio de la Internet.

5.5 MARCO LEGAL

5.5.1 Ley 1928 del 2018 Convenio Internacional con el gobierno nacional para sumar fuerza contra la lucha de la ciberdelincuencia celebrado en Budapest. Las consideraciones son similares a la Ley 1273 de 2019 con algunas aplicaciones específicas; permitiendo unificar criterios entre los gobiernos internacionales que permita reducir los índices y judicializar a los delincuentes con mayor agilidad.

La ley tiene como objeto garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio de Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, defender sus opiniones, libertad de expresión mediante la consulta y publicación de información, respeto de la intimidad, derecho a la protección de los datos personales fortaleciendo la lucha contra la ciberdelincuencia, incluidas las medidas adoptadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8 (SENADO S. , LEY 1928 DE 2018, 2018).

[45] UNICEF. Delitos de abuso y explotación sexual infantil. 2018. [En línea]. Disponible en: https://www.unicef.org/colombia/comunicados-prensa/delitos-de-abuso-y-explotacion-sexual-infantil

[46] Secretaria del Senado. Ley 1928 DE 2018. 2018. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

Los ítems que cobran relevancia en la presente ley y por el cual emitirá un juicio sobre los ciberdelitos como: acceso ilícito, interceptación ilícito, interferencia en los datos, interferencia en los sistemas, abusos de los dispositivos, falsificación y fraude informática, pornografía infantil, entre otros (SENADO S. , LEY 1928 DE 2018, 2018).

5.5.2 Ley 1620 de 2013 el gobierno Nacional por medio del Ministerio de Educación define una normatividad para controlar y tomar medidas disciplinarias afrente a los problemas relacionados con la violencia o acoso escolar garantizando la libre expresión y desarrollo de la persona.

Esta tiene como propósito:

- Educación para el ejercicio de los derechos humanos, sexuales y reproductivos.
- Prevención y mitigación del acoso escolar o bullying (matoneo)
- Prevención y mitigación del ciberacoso escolar o ciberbullying.
- Fomentar y fortalecer la educación por y para la paz, desarrollo de identidad y convivencia escolar.
- Fomentar mecanismos de prevención, protección, detección temprana y denuncia de aquellas conductas que atentan contra la convivencia escolar, ciudadanía y derechos humanos (SOMOSCAPAZES, s.f.).

Establecidos los criterios para ser aplicados en los entornos web orientado a los menores de edad para salvaguardar su integridad y libre desarrollo. Por ende, la ley define la protección contra cualquier abuso que se pueda presentar por la Internet.

5.5.3 Ley 1273 de 2009 normatividad Colombiana establece medida disciplinaria del ámbito penal a las personas que se vean involucrados en delitos informáticos como:

- Acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación

[46] Secretaria del Senado. Ley 1928 DE 2018. 2018. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

- Interceptación de datos informáticos
- Daño informático.
- Uso de software malicioso
- Violación de datos personales
- Suplantación de sitios web para capturar datos personales (SENADO S. D., 209).

En el marco jurídico de la seguridad informática, define el modelo ejemplar sobre los hechos que afectan a las personas; resaltando el valor que tiene una persona al citar: desde que nace se debe garantizar protección y bienestar por parte de un país.

En este apartado, hace referencia a juicio orientado en casos específicos de la ciberseguridad que tiene como responsabilidad los criminales frente a las siguientes posturas:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales (SENADO S. D., 209).

[47] SOMOSCAPAZES. Ley 162.. [En línea*. Disponible en: https://www.somoscapazes.org/ley1620.php

[48] Secretaria Senado. Ley 1273 de 2009. 2009. [En línea]. Disponible: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Estos aspectos de la ley, se debe tomar con responsabilidad y con medidas ejemplares para mitigar los ciberdelitos y las heridas que pueden ocasionar a un menor de edad cuando es objeto de lo delitos por el mal uso de los diferentes servicios web.

5.5.4 Ley 1336 de 2009 medida asumida por el gobierno de Colombia para hacer frente a los delitos informáticos asociado a los niños en el tema de la pornografía y comercio sexual entre otros. La importancia de la ley es la capacidad de retomar la Ley 679 del 2001 para incluir nuevas consideraciones según la modalidad con que operan los criminales.

La ley contempla el juicio penal en la defensa de los menores de edad que pueden ser víctima de algún abuso en especial la explotación sexual:

- Extinción de dominio a los hoteles, pensiones, hostales, residencias, apartahoteles y a los demás establecimientos que presten el servicio de hospedaje, cuando tales inmuebles hayan sido utilizados en actividades sexuales de niños, niñas y adolescentes (ICBF, 2009).
- Los entes como la Procuraduría y Fiscalía, deben velar por el cumplimiento de la ley mediante: ejecución de protocolos y lineamientos nacionales para la atención de las víctimas, representación judicial de los menores de edad dentro de los procesos penales relacionados en calidad de víctimas en contra de la libertad, integridad y formación sexuales, la sanción incide en la privación de la libertad e indización por aquellos hechos asociados a la utilización o explotación sexual de niños, niñas y adolescentes (ICBF, 2009).

5.5.5 Ley 765 de 31 de Julio de 2002 Disposiciones legales para contrarrestar la pornografía infantil desde la venta de elementos relacionados con este problema hasta el incitar a un menor a estas acciones en contra de su voluntad y con estas consideraciones se dicte normatividad para combatir esta problemática en el cual se ven envuelto los menores de edad.

[49] Secretaria Senado. Ley 1273 de 2009. 2009. [En línea]. Disponible: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[50] ICBF. Ley 1336 DE 2009. 2009. [En línea]. Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_1336_2009.htm

La normatividad genera los elementos para judicializar a las personas que promueven el delito y son merecedoras de castigo que dicta la ley. Con firme intención de evitar que esta situación se repita y propague a un corto tiempo. Destacando un protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de los niños en la pornografía (SENADO S. , LEY 765 DE 2002, 2002).

La ley tiene como propósito: reconocer el derecho del niño a la protección contra la explotación económica y la realización de trabajos que puedan ser peligrosos, entorpecer su educación o afectar su salud o desarrollo físico, mental, espiritual, moral o social (SENADO S. , LEY 765 DE 2002, 2002).

[51] ICBF. Ley 1336 DE 2009. 2009. [En línea]. Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_1336_2009.htm

[52] Secretaria Senado. Ley 765 de 2002. 2002. [En línea]. Disponible: http://www.secretariasenado.gov.co/senado/basedoc/ley_0765_2002.html

6 DESCRIPCION DE LOS OBJETIVOS

El estudio monográfico ha involucrado una serie de consulta web para obtener información en las diferentes instituciones judiciales como la Policía Nacional, ICBF, Dijín (CAI Virtual), Gobernación del Huila y Secretaria de Educación departamental. Al mismo tiempo, se elabora y aplica un cuestionario con el propósito de conocer de primera mano el nivel de conocimiento de los menores de edad sobre ciberseguridad; a razón que la mayoría de los casos no se logra materializar en una denuncia por tema personal, falta de pruebas, vergüenza, etc.

Las fuentes de información descrita anteriormente generan una base importante de conocimiento para su posterior análisis y construcción del informe para explicar de forma clara y concisa las debilidades suscitada en el marco teórico-práctico de la ciberseguridad en los niños, niñas y adolescentes en el departamento del Huila.

En tiempo de pandemia, la ciberseguridad es la otra cara de la moneda que preocupa los intereses del país como: las cifras más recientes del Centro Cibernético de la Policía Nacional que permite inferir sobre los delitos informáticos aumentaron el 59% en el primer semestre, respecto al mismo periodo del año pasado, debido a que la pandemia impulsó a los Colombianos el uso de las operaciones digitales (PORTAFOLIO, 2020).

Así las cosas, entre enero y junio de este año registraron 17.211 denuncias, 6.340 más que en el primer semestre del 2019. También se presentaron 2.103 casos de suplantación de sitios web, un delito que creció en 364% (PORTAFOLIO, 2020).

La preocupación de las entidades del orden nacional e internacional en especial UNICEF y sus aliados considera que millones de niños y niñas corren el riesgo de sufrir daños en un momento de su vida con el creciente auge en el uso del internet debido al confinamiento durante la pandemia de COVID-19 (UNICEF, os niños corren un mayor riesgo de sufrir daños en línea durante la pandemia mundial de la COVID-19, 2020).

[53] PORTAFOLIO. Delitos Informáticos la otra pandemia en tiempos del coronavirus. 2020. [En línea]. Disponible en: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

[54] UNICEF. Los niños corren un mayor riesgo de sufrir daños en línea durante la pandemia mundial de la COVID-19. 2020. [En línea]. Disponible en: https://www.unicef.org/es/comunicados-prensa/ninos-corren-mayor-riesgo-sufrir-danos-en-linea-durante-pandemia-COVID-19

UNICEF considera literalmente que los niños y jóvenes están afectados por el cierre de las escuelas en todo el mundo. Muchos de estos estudiantes toman sus clases y socializan cada vez más a través del internet. Pasar más tiempo en las plataformas virtuales puede exponer en mayor medida a los niños a la explotación sexual y el acoso en línea, ya que los ciberdelincuentes buscan aprovecharse de cualquier situación que puede ser generada en tempo de pandemia. La falta de contacto personal con sus amigos y parejas puede llevar a que asuman mayores riesgos, como el envío de imágenes sexuales, mientras que el tiempo sin estructurar que pasan en internet puede exponer a los niños a contenidos potencialmente dañinos y violentos, así como a un mayor riesgo de sufrir ciberacoso (UNICEF, os niños corren un mayor riesgo de sufrir daños en línea durante la pandemia mundial de la COVID-19, 2020).

El presente estudio permite modelar actualmente el entorno amenazante a los niños (as) y adolecentes frente al auge de las redes sociales, juegos, y otros servicios disponible en la internet. Las necesidades que hoy día ofrece la situación actual arrastran a la mayoría de los menores de edad a una vida dependiente de las tecnologías. Es por esta razón, que toma fuerza la necesidad de evaluar el nivel de conocimiento y buenas practica que conoce los menores de edad en el Huila frente al cambio generado por la pandemia. Según el informe presentado al público por la Revista Semana: Colombia se 'raja' en ciberseguridad para niños y adolescentes (REVISTA SEMANA, 2020). Es importante presentar al Huila una oportunidad para establecer una defensa activa e inteligencia: de la teoría a la práctica (INCIBE, 2018) para evitar que los ciberdelitos continúe en ascenso y consecuencias de esto afecte la sociedad que hoy conocemos.

---

[55] UNICEF. Los niños corren un mayor riesgo de sufrir daños en línea durante la pandemia mundial de la COVID-19. 2020. [En línea]. Disponible en: https://www.unicef.org/es/comunicados-prensa/ninos-corren-mayor-riesgo-sufrir-danos-en-linea-durante-pandemia-COVID-19

[56] REVISTA SEMANA. Colombia se 'raja' en ciberseguridad para niños y adolescentes: informe. [En línea]. 2020. Disponible en: https://www.semana.com/educacion/articulo/colombia-se-raja-en-ciberseguridad-para-ninos-y-adolescentes-informe/652523

[57] INCIBE CERT. Defensa activa e inteligencia: de la teoría a la práctica. [En línea]. 2018. Disponible en: https://www.incibe-cert.es/blog/defensa-activa-e-inteligencia-teoria-practica

El trabajo un ejemplo para futuras investigaciones y fuente de información que conlleve a garantizar los derechos y el reconocimiento a los niños como sujetos sociales (CALDERON CARRILLO , 2015) en el marco de la seguridad informática aplicado desde diferentes perspectiva especialmente a los niños frente al Internet: seguridad, educación y tecnología (VAUNELLO GLADYS , 2015) que nos permita cambiar la brecha que hoy nos aleja de entornos seguros y libre de amenazas en los menores de edad del Huila.

A continuación se describe los pasos a seguir y los resultados en el desarrollo de cada objetivo de la monografía:

6.1 Objetivo 1 Consultar la información actual sobre la ciberseguridad para los niños, niñas y adolescentes en el departamento del Huila en los últimos 5 años: Obtener información en fuente confiable en el Internet e instituciones departamental para el análisis respectivo. Las entidades corresponden a la Policía Nacional de Colombia (través del programa de infancia y Adolescencia, CAI Virtual), ICBF, Gobernación y Secretaria de Educación departamental. La función principal de las entidades descritas anteriormente velan por la integridad y seguridad de los niños, niñas y adolescentes en el Huila.

Una vez realizado el primer acercamiento a las entidades mencionadas; la Dijín a través del CAI Virtual proporciona información vital para la monografía sobre las denuncias registradas con respeto a los ciberdelitos de los últimos 5 años que han afectado a los niños, niñas y adolescentes de Huila. Las demás entidades carecían de la información en las respectivas bases de datos frente a la solicitud requerida. El resultado de la gestión realizada puede ser verificado en los anexos A, B, C y D al finalizar el documento donde se encuentra las respuestas de las entidades.

[39] CALDERÓN, D. Los niños como sujetos sociales. Notas sobre la antropología de la infancia. [En línea]. 2015. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-06362015000100007

[40] VUANELLO, G. Los niños frente a Internet: seguridad, educación y tecnología. [En línea]. 2015. Disponible en: https://www.redalyc.org/articulo.oa?id=60741185005

6.2 Objetivo 2 Establecer datos estadísticos de los ciberdelitos suscitados en el departamento del Huila en los últimos 5 años: Realizar gráficas y cuadro estadístico con la con información relacionada con los temas tratados en la encuesta para lograr tener la claridad en cuanto a los hechos, cantidad de ocurrencia y demás elementos que aportan a la identificación de los ciberdelitos que han afectado a los niños, niñas y adolescentes en el Huila de los últimos 5 años.

Ante la carencia de información suministradas por las entidades como el ICBF, Gobernación y Secretaria de Educación del Huila se procede aplicar un cuestionario a los niños, niñas y adolescentes por medio de los servicios de google form con el propósito de lograr una mayor cobertura en la población a nivel departamental y al mismo tiempo la facilidad para tabular y graficar la información.

6.3 Objetivo 3 Analizar los hechos o acciones que han ocurrido entorno de los ciberdelitos de los niños, niñas y adolescentes en el departamento del Huila: la información recabada será objeto de un respectivo tratamiento con el propósito de verificar el origen o motivo que han suscitado aquellas actuaciones que terminaron afectando la población de estudio mediante las siguientes consideraciones: falta de conocimiento, sitios web inseguros, uso inadecuado de la seguridad perimetral, desconocimiento de buenas prácticas, entre otros factores que han restado importancia a la ciberseguridad.

El análisis estadístico se basa con la información suministrada por la Dijín y los datos obtenidos por el cuestionario con mira de generar la comprensión sobre el uso de la ciberseguridad en los diferentes contextos donde puede interactuar un menor de edad en el internet. Estos datos soportan los argumentos para elaborar el informe y recomendaciones de las buenas práctica de la seguridad informática.

6.4 Objetivo 4 Elaborar un informé para establecer los hechos que han afectado a los niños, niñas y adolescentes del Huila y recomendaciones sobre la ciberseguridad: El documento contiene el análisis realizado sobre los ciberdelitos de los últimos 5 años en el Huila. En este punto, se comparte aquellas recomendaciones frente a la problemática planteada en la monografía; para aportar conocimientos sobre las buenas prácticas de la ciberseguridad en el Huila y establecer las estrategias preventivas para proteger a los niños, niñas y adolescentes en el internet.

El propósito de la monografía es aportar al desarrollo de nuevas tecnologías y software que este encaminado para generar opciones a los menores de edad y padres de familia en la forma de protegerlos contra los ciberdelitos e informar sobre los mismos avances. En otras instancias la Secretaria de Educación y Gobierno Departamental generé un compromiso en la implementación de estrategia en el aprendizaje y concientización de los conocimientos sobre la seguridad informática.

7 DESARROLLO DE LOS OBJETIVOS

7.1 CONSULTAR LA INFORMACIÓN ACTUAL SOBRE LA CIBERSEGURIDAD PARA LOS NIÑOS, NIÑAS Y ADOLESCENTES EN EL DEPARTAMENTO DEL HUILA EN LOS ÚLTIMOS 5 AÑOS.

Metodología: Este objetivo ha sido consultado en fuentes fiables en la Internet y en las instituciones del orden departamental con el propósito de obtener datos reales y verídicos en la elaboración del trabajo.

La investigación se realiza mediante un enfoque analítico para establecer un marco de referencia en la identificación y aplicación de los conceptos en ciberseguridad orientado a los niños, niñas y adolescentes del Huila. Las consultas se realizaron en las páginas web de la Policía Nacional, ICBF, Fiscalía, UNICEF, ONU, INCIBE, Congreso de la Republica, etc. Del orden informativo como El País, Diario del Huila, La Nación, La FM, etc. Empresa de seguridad informática como Kaspersky y Avast, por ultimo las instituciones universitarias como la UNAD, Unilibre y Unicatólica.

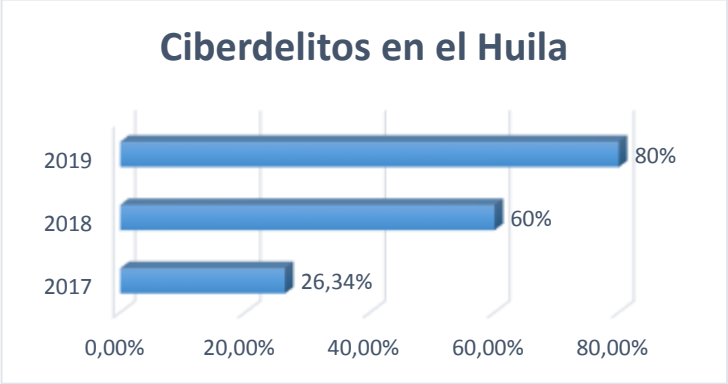
La realidad de los ciberdelitos en Neiva es casi desconocida; es una verdad que solo lo saben las víctima; la mayoría de estas no denuncian por el tipo de señalamiento que puede suscitarse en el momento de la denuncia ante una sociedad prejuiciosa y sin argumentos para cuestionar una víctima (VARGAS, 2018).

El Diario del Huila, ha identificado el aumento en los índices de la delincuencia informática en el departamento como respuesta del flagelo y su creciente auge en las redes sociales y dispositivos electrónicos para el acceso. Según cifras del Cuerpo Técnico de Investigación CTI, mientras en 2017 entre enero y febrero los casos presentaron un aumento de 26,34% y por el 2018, en el mismo periodo, el incremento fue de 60%; se estima que la cifra puede estar en un 75 a 80% en el 2019 (VARGAS, 2018) como lo ilustra la siguiente figura:

---

[58] VARGAS, L. Los delitos informáticos, modalidad delictiva que 'acecha' a los neivanos. 2018. [En línea]. Disponible en: https://www.diariodelhuila.com/los-delitos-informaticos-modalidad-delictiva-que-acecha-a-los-neivanos#:~:text=14%2008%3A34-,Los%20delitos%20inform%C3%A1ticos%2C%20modalidad%20delictiva%20que%20'acecha'%20a%20los,sancionado%20con%20pena%20m%C3%A1s%20grave.

Figura 2. Ciberdelitos del Huila



Fuente: https://www.diariodelhuila.com/los-delitos-informaticos-modalidad-delictiva-que-acecha-a-los-neivanos#:~:text=14%2008%3A34-,Los%20delitos%20inform%C3%A1ticos%2C%20modalidad%20delictiva%20que%20'acecha'%20a%20los,sancionado%20con%20pena%20m%C3%A1s%20grave.

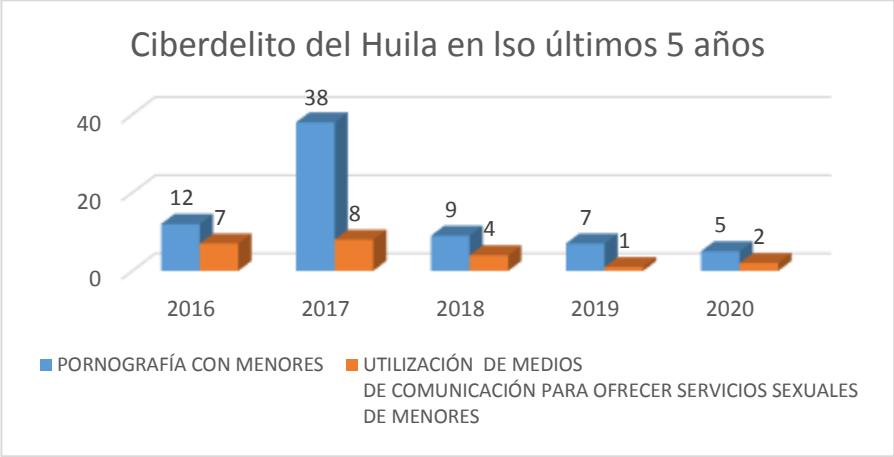
Actualmente la Gobernación y Secretaria de Educación Departamental no cuenta con información sobre la problemática de la ciberseguridad, el ICBF del Huila se abstiene de compartir información por el manejo de los datos personales habas data; caso contrario, la Dijín a través del CAI Virtual provee las denuncias registrada por los menores de edad en los últimos 5 años y puede ser corroborada en el Anexo D.

El desconocimiento de las buenas prácticas de la ciberseguridad ha permitido que las redes sociales y el Internet se convierte en un ciberespacio de alto riesgo para cualquier persona en especial a los menores de edad; con unos minutos necesita el ciberdelincuente para lograr engañar y seducir a sus víctimas buscado su momento de poder y fama en el medio de los hacking. Es por esta razón, que la pornografía, perfiles falsos en la redes sociales, entre otros delitos genera un daño irreparable en los menores de edad (VARGAS, 2018) y debe ser estudiado con detenimiento para comprender el posible talón de Aquiles de la seguridad informática en los menores de edad.

[58] VARGAS, L. Los delitos informáticos, modalidad delictiva que 'acecha' a los neivanos. 2018. [En línea]. Disponible en: https://www.diariodelhuila.com/los-delitos-informaticos-modalidad-delictiva-que-acecha-a-los-neivanos#:~:text=14%2008%3A34-,Los%20delitos%20inform%C3%A1ticos%2C%20modalidad%20delictiva%20que%20'acecha'%20a%20los,sancionado%20con%20pena%20m%C3%A1s%20grave.

En la figura 3 se puede observar los casos reportado por la Dijín sobre los delitos asociados a la pornografía infantil; involucrando con esta actividad sometimiento a los menores de edad y las puertas abiertas a cualquier individuo a la penumbre de la ilegalidad. Estos hechos carecen de límites y son especialista para negar el respecto a los derechos consignado en la carta magna de la constitución política de Colombia y tratados internacionales. Razón por la cual, es importante considerar la siguiente información suministrada por la Dijín y proceder a estudiar la problemática para comprender e proceder de los hechos delictivos en el Huila frente a la pornografía infantil y uso de los medios de comunicaciones para publicar contenidos íntimos o privados en la internet.

Figura 3. Ciberdelitos del Huila durante los últimos 5 años.



Fuente: Anexo D

La siguiente tabla corresponde a los datos de la figura 3 según el Anexo D de presente documento:

Tabla 2. Ciberdelitos de los últimos 5 años

DESCRIPCION CONDUCTA	2016	2017	2018	2019	2020
ARTÍCULO 218. PORNOGRAFÍA CON MENORES	12	38	9	7	5
ARTÍCULO 219 A. UTILIZACIÓN O FACILITACIÓN DE MEDIOS DE COMUNICACIÓN PARA OFRECER SERVICIOS SEXUALES DE MENORES	7	8	4	1	2
TOTAL	**19**	**46**	**13**	**8**	**7**
Fuente: Anexo D					

La ciberseguridad en el Huila y en Colombia es el mecanismo de control y defensa contra cualquier tipo de ciberdelito y el resultado de confianza a los menores de edad. Según la Red de PAPAZ y frente al tema de ciberseguridad, se debe tener en cuenta las siguientes recomendaciones:

- Los contenidos sexuales se puede acceder fácilmente y es necesario generar una prevención desde el hogar (EL PAIS, 2019).
- Contactos por redes sociales, que los padres deben enseñar a sus hijos a diferenciar de lo que realmente es un amigo, porque muchos se disfrazan de lo que no son y engañan con facilitad a nuestros hijos (EL PAIS, 2019).

Aun así, estas son cifras que no alcanzan abarcar todo el espectro de la pornografía infantil; el titán del ciberespacio que reúne miles de personas en el mundo. Este problema es bastante complejo, porque tiene la posibilidad ideal de ser muy transfronterizo en la medida en que se pueden enviar contenidos sin ningún problema", aseguró Mario Gómez, fiscal para la Infancia y Adolescencia a nivel nacional (EL PAIS, 2019).

El auge de los ciberdelitos está estrechamente relacionado con aquellas personas supuestamente amigas con perfiles falsos, procurando entre otras cosas:

- Engañar a los niños o adolescentes, para establecer noviazgos virtuales y de ahí, hacer solicitudes de fotos y videos de carácter sexual (EL PAIS, 2019).
- Una vez que logran establecer una relación virtual, acuden a diferentes herramientas y conocimientos en tecnología para obtener la dirección IP de la víctima. Con esto, ya no solo saben la ubicación exacta del menor de edad, sino que pueden activar la webcam de sus dispositivos (computador, Tablet, celular) para grabar lo que ocurre en frente y así obtener imágenes comprometedoras (EL PAIS, 2019).

[59] EL PAÍS, Redacción. Alarmante aumento de pornografía infantil en Internet, claves para proteger a los niños. (En línea). 2019. Disponible en: https://www.elpais.com.co/judicial/alarmante-aumento-de-pornografia-infantil-en-internet-claves-para-proteger-a-los-ninos.html

La ciberinducción es otro medio de las redes sociales y la Internet valiéndose de retos, juegos o aplicaciones; involucran a un menor para realizar aquellas actuaciones que terminan generando una afectación; también se pueden hacer mención del Ciberbullying en las instituciones educativas. La Policía Nacional indica: "Con el auge de las redes sociales, los juegos de realidad aumentada y la comunicación por aplicaciones de mensajería instantánea, los menores de edad, están mayormente expuestos a ser blanco de los depredadores que se encuentra en el ciberespacio. Por esta razón es recomendable:

- De ahí que apoyados en el trabajo experto del Centro Cibernético Policial de la Dirección de Investigación Criminal e Interpol, la tarea institucional está enfocando sus esfuerzos detectando nuevas modalidades del Ciberdelito entre estos la llamada modalidad de ciberinducción (POLICIA NACIONAL, 2018).
- Fiscalía Seccional Huila, invita a la ciudadanía a utilizar la plataforma para denunciar como www.fiscalia.gov.co, https://caivirtual.policia.gov.co/ y www.policia.gov.co, línea 122, 018000919745 y 123 en la que podrá interponer denuncias por delitos como hurto en todas sus modalidades; extorsión, explotación sexual infantil, delitos informáticos, falsedad personal en documento público y privado, y estafa, entre otros (FISCALIA, 2020).
- Ante organismos internacionales que vela por la seguridad de los niños, niñas y adolescentes puede adquirir información y la forma para denunciar ciberdelitos; el link es https://teprotejo.org/

El estudio sobre la ciberdelincuencia que afecta a los niños, niñas y adolescentes en el departamento de Huila, permite conocer la magnitud del problema que a diario se ven expuesto y con ello la vulnerabilidad que ha llevado a incrementar los casos reportados por ciberdelitos. Aunque la información obtenida hasta el momento no permite un análisis general en el Huila sobre la ciberdelincuencia; es por ello que se realiza una encuesta aplicada a los niños, niñas y adolescentes del Huila para aportar elementos suficientes en los resultados del estudio para estimar indicadores verdaderos sobre la ciberseguridad y así mismo interpretar los datos para aportar información que en el futuro pueden servir como soporte para establecer mecanismo y estrategia a corto y mediano plazo en acciones efectivas en el campo de la ciberseguridad.

[60] POLICIA NACIONAL. Protección y prevención, aliados de los colombianos en la internet. [En línea]. 2018. Disponible en: https://policia.gov.co/noticia/proteccion-y-prevencion-aliados-colombianos-internet

[61] FISCALIA. Cierre temporal de las Salas Recepción de Denuncia de la Fiscalía en Huila. 2020. [En línea]. Disponible en: https://www.fiscalia.gov.co/colombia/seccionales/cierre-temporal-de-las-salas-recepcion-de-denuncia-de-la-fiscalia-en-huila/

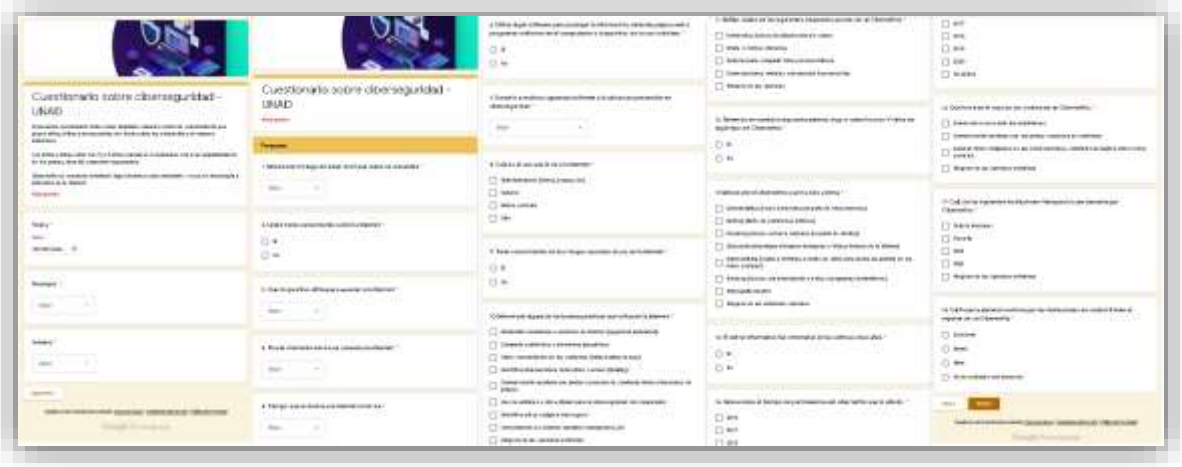
7.2 ESTABLECER DATOS ESTADÍSTICOS DE LOS CIBERDELITOS SUSCITADOS EN EL DEPARTAMENTO DEL HUILA EN LOS ÚLTIMOS 5 AÑOS.

Metodología: Este objetivo parte de la aplicación de un cuestionario en google forms a los niños, niñas y adolescentes del Huila; como fuente de información complementaria al estudio.

Las entidades del orden departamental como la gobernación, secretaria de educación departamental, ICBF y Policía Nacional; están limitadas en cuanto a denuncias que deben ser interpuesta por las víctimas que generalmente lo hacen en compañía de sus padres o tutores. Es importante dejar en claro que muchos de los casos son desconocido por las entidades del gobierno, estas actuaciones objeto de vergüenza u otras consideraciones de los afectados para evitar algún tipo cuestionamiento.

Teniendo en cuenta los datos recolectados en el primer objetivo de la monografía y la poca información recabada; se diseña y aplica un cuestionario en google forms como se presenta en la siguiente figura:

Figura 4. Formulario de la encuesta



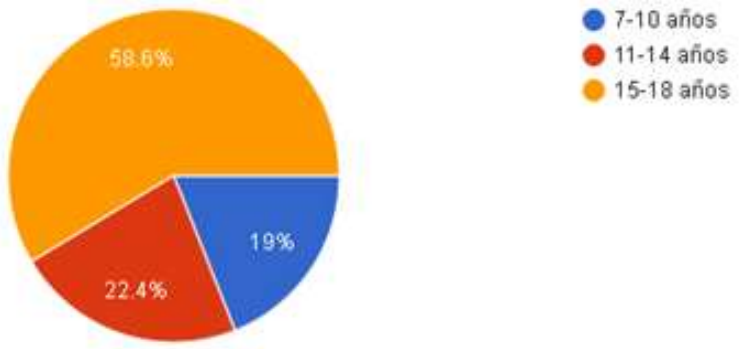
Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

En adelante se presenta el análisis de las gráficas obtenidas desde google form de acuerdo a las 18 preguntas según el formato y aplicado a los menores de edad en el Huila; la información del estudio es:

Pregunta 1: Seleccione el rango de edad en el que usted se encuentra

El cuestionario inicia con el rango de edad para determinar la población que puede estar expuesta a los ciberdelitos en el Huila.

Figura 5. Edad de los encuestados



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

El propósito de esta pregunta es identificar la edad predominante en la encuesta que puede ser víctima de un ciberdelito en el uso constante del internet; además, teniendo en cuenta los motivos actuales de la pandemia es importante dejar en claro la posibilidad enorme de los menores de edad para sufrir un delito informático.

El resultado de la pregunta 1 ha permitido identificar que el 51.7% pertenece al género masculino y 48.3% al femenino. Esta cifra nos permite aludir casi una igualdad en género encuestado.

Pregunta 2: Usted tiene conocimiento sobre la Internet

La segunda pregunta del cuestionario es de tipo cerrada para conocer si tiene conocimiento sobre el concepto de internet para dimensionar la globalidad de un tema y al mismo tiempo los riesgos asociados a este.

Figura 6. Conocimiento del internet

Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

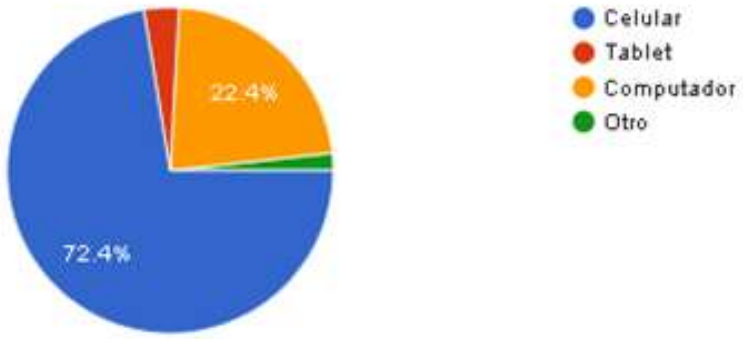
La pregunta 2 es muy sencilla pero fundamental para identificar un tema tan vital como tener claro el concepto de Internet y a su vez es una pregunta indirecta para asociar las responsabilidades en el uso de este servicio.

El resultado tiene un alto grado de satisfacción por que el 98.3% tiene conocimiento sobre el internet y sus bondades; a diferencia del 1.7% que no tiene conocimiento sobre este servicio.

Pregunta 3: Que dispositivo utiliza para acceder a la Internet

En todo acceso de internet es importante identificar el dispositivo de mayor uso para establecer entre otras cosas la seguridad perimetral que tiene definida por el fabricante y el riesgo tan alto que involucra los dispositivos móviles.

Figura 7. Dispositivo para acceder a internet.



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

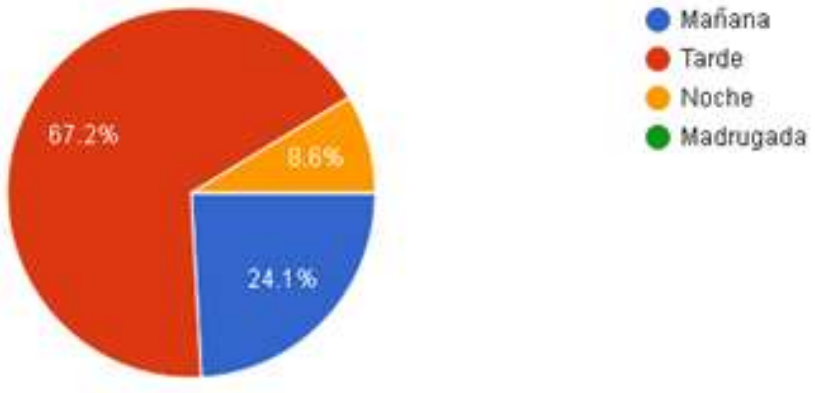
Esta pregunta es interesante, teniendo en cuenta que la ciberseguridad debe aporta mediantes controles los servicios que permita asegurar los dispositivos mencionados que conlleve a mitigar los riesgos que puede afectar a un usuario sobre un ciberdelito.

El celular es el dispositivo con mayor porcentaje de uso por los menores de edad para acceder a internet con un 72.4%, seguido a este el computador con 22.4%. Es comprensible que estos dos dispositivos con mayor uso deben implementar medidas de seguridad junto a las buenas prácticas para garantizar la ciberseguridad.

Pregunta 4: En qué momento del día se conecta a la Internet

Los horarios de acceso a internet, es un elemento importante para el estudio porque permite identificar el grado de vulnerabilidad que está expuesto un menor de edad ante la falta de una supervisión por parte de los padres o persona responsable; los horarios nocturnos es donde los ciberdelincuente se muestran para lograr aprovecharse de esa vulnerabilidad pueda cometer el ciberdelito.

Figura 8. Horario de acceso a la Internet



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

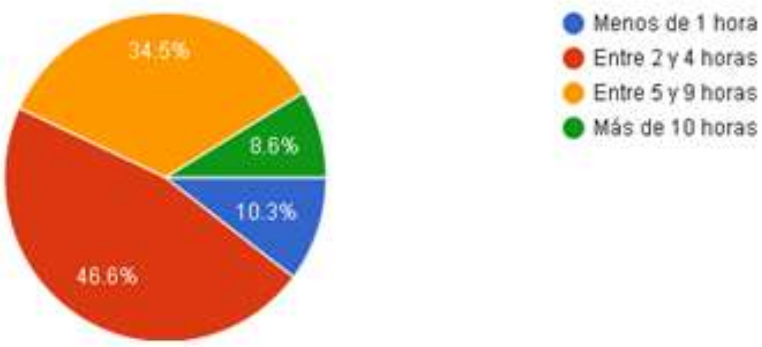
La pregunta aunque tiene una respuesta simple, permite aporta al estudio las horas donde un menor de edad pueden ser propenso a un ciberdelito por la ausencia de una supervisión y el momento ideal en el del día para materializar un ciberdelito.

El 67.2% de la población encuestada acceden a internet en hora de la tarde, seguido a este está el horario de la mañana con un 24.1% y 8.6% en la noche. Aunque los horario con mayor porcentaje no es un riesgo alto, si se debe tener cuidado por la ausencia de los padres por tema de trabajo u otras responsabilidades.

Pregunta 5: Tiempo que le dedica a la Internet en el día

Entre mayor sea el tiempo de un niño(a) o adolescentes invierta en internet, es un factor determinante para ser víctima de los diferentes ciberdelitos que se puede despender de una debilidad por la parte de la víctima y aprovechada por un ciberdelincuente. Esta pregunta está orientada a determinar aquellas variables que derivada del flagelo como la ciberdelincuencia en menores de edad en el Huila.

Figura 9. Cantidad de hora diaria en Internet



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

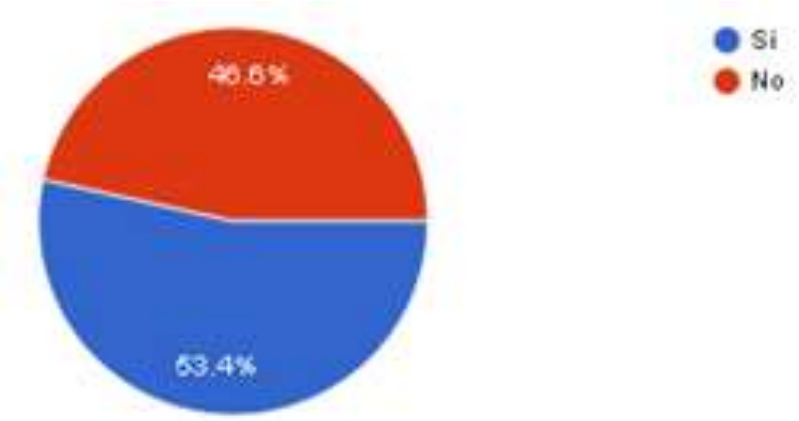
El tiempo dedicada para acceder a internet, es una característica que debe ser analizada en el estudio porque aporta juicio en cuanto a la dependencia a este servicio y al mismo tiempo lo propenso que puede llegar a estar un menor de edad a un ciberdelito.

El resultado de esta pregunta ha permitido conocer que el 46.6% de los menores de edad pasan entre 2 a 4 hora es internet, el 34.5% entre 5 y 9 horas, el 10.3% menos de una hora y 8.6% más de 10 horas. Esta información permite apreciar que los menores de edad invierten buen pate de su tiempo en la internet.

Pregunta 6: Utiliza algún software para proteger la información, detectar página web o programas maliciosos en el computador o dispositivo en el uso cotidiano

Esta pregunta se basa si el menor de edad conoce el significado de un software de protección o seguridad contra alguna amenaza y por otro lado si utiliza estos programas para determinar la primera barrea de cuidado. La pregunta es importante teniendo en cuenta que los menores de edad utiliza con mayor frecuencia los dispositivos móviles y estos carecen de seguridad perimetral o ingreso seguro a páginas sin el protocolo SSH o HTTPS.

Figura 10. Uso de software benigno



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

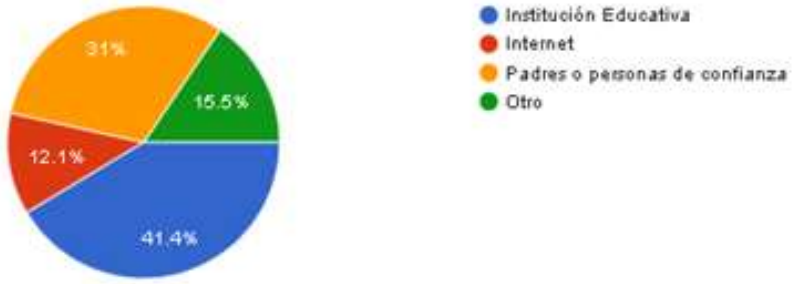
Es importante definir si un menor de edad tiene conocimiento sobre el software de protección perimetral para la información que puede ser gestionada en un dispositivo para el procesamiento de datos, difusión de los datos en sitios web posiblemente inseguros, entre otras actividades; por esta razón, la pregunta ayuda a encontrar las debilidades en cuanto a las buenas prácticas de la ciberseguridad.

El 53.4% si utiliza software de protección como antivirus o antispyware y el 46.3% no. Esta pregunta genera un desaire en la ciberseguridad, toda vez que el 46.3% de los menores están expuesto a un ciberataque y demás sin el mínimo conocimiento; exponiendo su datos privado y personales para ser difundido por la redes sociales e internet.

Pregunta 7: Donde ha recibido capacitación frente a la cultura de prevención en ciberseguridad

Al conocer la institución o persona donde el menor de edad ha recibido conocimiento sobre la ciberseguridad es comprender los elementos para proteger ante una amenaza en el internet. La pregunta es muy clara y directa para recabar la información necesaria en el análisis requerido por el estudio.

Figura 11. Lugar donde adquirió conocimiento sobre la ciberseguridad



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

Esta pregunta conduce a entender el foco del conocimiento y prácticas adquirida por el menor de edad para una defensa activa y permanente en los hechos preventivos ante los ciberdelitos.

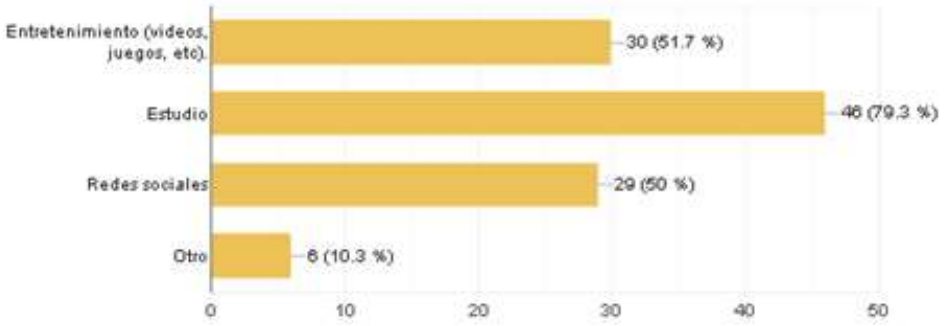
El 41.4% de los menores de edad encuestado adquirió conocimientos de ciberseguridad en las instituciones educativas, el 31% por los padres, 15.5% por otros medios y 12.2% en internet. Esta pregunta confirma la importancia de las instituciones educativas y padres de familia como actores importantes y fuente de conocimiento para adquisición y concientización para generar una cultura de ciberseguridad.

Pregunta 8: Cuál es el uso que le da a la Internet

El uso de internet tiene una ilimitada aplicación según la necesidad de un menor de edad y sobre todo la interacción social. Esta información genera un aporte importante en el estudio y el análisis respectivo de los datos.

Los riesgos están sujeto a los menores de edad según la necesidad para ingresar a las redes sociales y otros servicios de su interés. El internet es una red de comunicación que en su mayor porcentaje genera ocultamiento de información a las personas sin experticia por la cantidad de perfiles falsos que hay en la actualidad y oros situaciones que agiliza aun criminal en el ciberespacio.

Figura 12. Actividad principal en internet



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

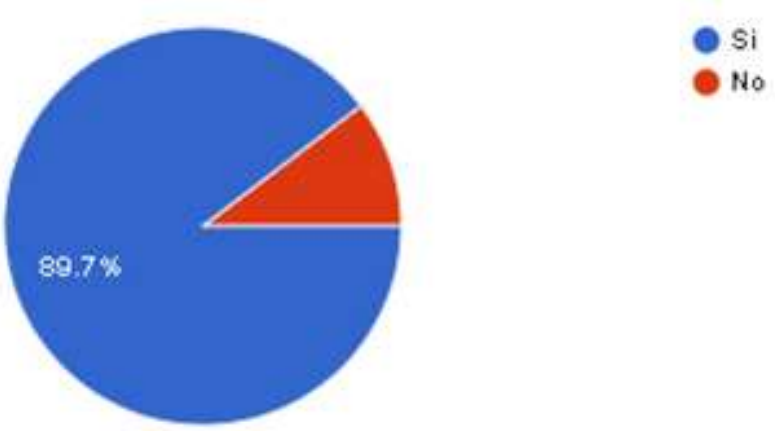
En la actualidad hay diferentes intereses que motiva a un menor de edad para estar conectado a internet; motivo que lleva a comprender los riesgos involucrados en cada conexión. La importancia de la pregunta conlleva a determinar cuáles son los servicios de mayor consumo para evaluar el riesgo que puede afectar a un menor de edad.

Los resultados de la pregunta permitió obtener con mayor porcentaje de los encuestados acceden a internet para estudiar con un 79.3%, entretenimiento 51.7%, redes sociales 50% y para otros servicios 10.3%. Los datos obtenidos permite interpretar un 50% de los encuestados ingresan a internet para entretenimiento y redes sociales donde las posibilidades es alta de encontrar perfiles falsos, intercambio de información privada, textos inapropiados, entre otros factores para materializar un ciberdelito.

Pregunta 9: Tiene conocimiento de los riesgos asociado al uso de la Internet

Una vez identificado el motivo de los encuestados para acceder al internet, es importante que un menor de edad puede tener la claridad sobre los problemas que se desprende del uso del internet y las redes sociales sin la debida protección y herramienta para el cuidado personal.

Figura 13. Conoce el riesgo del internet



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

La finalidad de la pregunta es comprender si los menores de edad tienen la capacidad o puede dimensionar sobre los riesgos asociados al uso de internet y servicios que se prestan algún beneficio de este servicio.

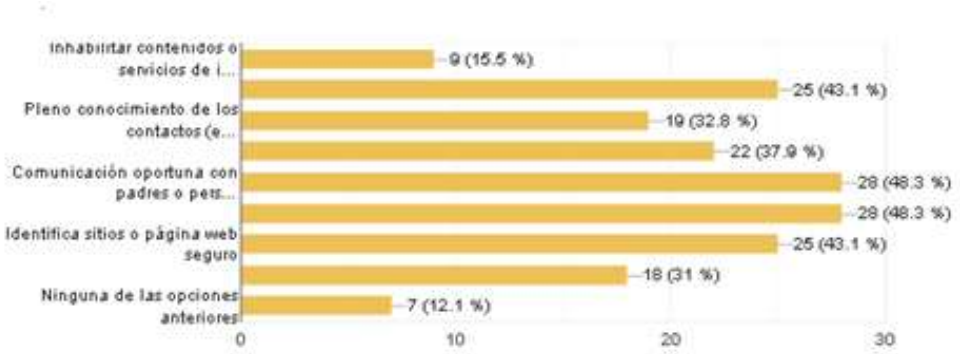
El 89.7% de los encuestado tiene conocimiento sobre los riesgos o problemas que implica el internet y 10.3% no. Es importante hacer referencia entre conocer el riesgo y la forma de prevención; por el cual, se evidencia un conocimiento opaco en la forma de acceder seguro al internet.

Pregunta 10: Seleccione alguna de las buenas prácticas que utiliza en la Internet

Esta pregunta es el inicio sobre el conocimiento directo de la ciberseguridad en la forma preventiva que los menores de edad generan los mecanismo de prevención y comunicación para evitar los ciberdelitos.

Las buenas practicas es la forma que los encuestados genera la primera parte de una defensa ante los riesgo del internet y sus diferentes servicios; en la actualidad es innumerable las plataformas de entretenimiento al alance de cualquier menor de edad sin la debida seguridad de acceso e identificación de los usuarios.

Figura 14. Buenas prácticas de ciberseguridad



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

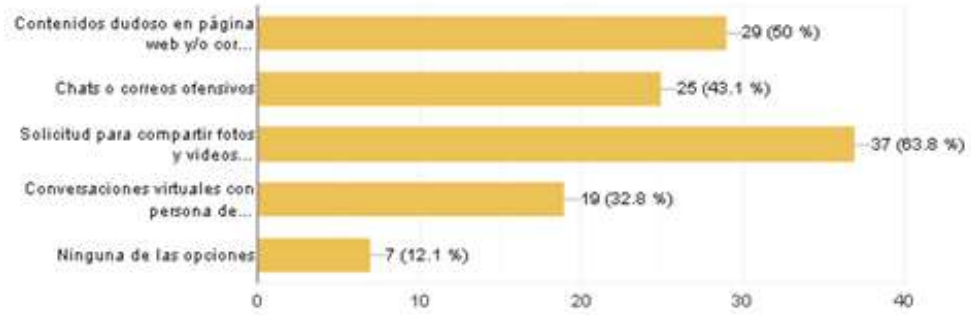
La pregunta define unas actividades puntuales de las buenas prácticas de la ciberseguridad y genera el conocimiento sobre el tema. El resultado aporta juicio que se tendrá en cuenta en el análisis y su posterior informe con las recomendaciones de la monografía.

El 48.3% de los encuestados aplica alguna de las recomendaciones de las buenas practicas mediante la comunicación oportuna con padres o persona responsable, compartiendo la misma cifra esta el uso de software como antivirus o antispyware, el 43.1% tienen en cuenta compartir contenidos apropiados e identificación de páginas web seguros, el 37.9% identifica proposiciones indecentes o acoso, el 32.8% tiene pleno conocimiento de los contactos, el 31% actualiza los sistema operativo, navegadores, etc. El 15.5% inhabilita con el proveedor de internet o dispositivos contenidos no apropiados y 12.1% No aplica ninguna de las anteriores medidas de seguridad.

Pregunta 11: Señale cuales de las siguientes situaciones puede ser un Ciberdelito

De esta pregunta se espera obtener la otra parte de la respuesta con respeto a la ciberseguridad para identificar las acciones que desencadena el ciberdelito y la forma como se presenta entre una comunicación en sus diferentes formas como las redes sociales y otras plataformas con el propósito de intercambiar información en páginas web.

Figura 15. Conocimiento sobre ciberdelito



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

La pregunta 11 tiene un propósito que los menores de edad encuestados puedan identificar la procedencia de un ciberdelito o como detectar para evitar ser víctima de este flagelo delictivo; en resumen, lograr anticipar una amenaza o situaciones que pueda afectar la integridad de los niños, niñas y adolescentes.

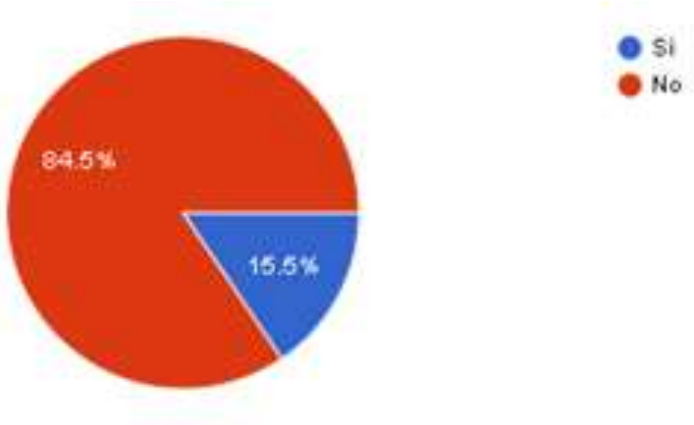
Los datos obtenidos permite comprender los siguiente: el 63.8% de los menores de edad puede identificar el origen de un ciberdelito como solicitar que pueda compartir fotos, videos u otro contenido íntimos. El 50% contenidos dudoso en página web o correos, 43.1% chat o correos ofensivos, 32.8% conversaciones virtuales con personas desconocidas y 12.1% no identifica las opciones de la pregunta como actividades relacionadas a un ciberdelito.

Pregunta 12: Teniendo en cuenta la respuesta anterior, diga si usted ha sido Víctima de algún tipo de Ciberdelito

La pregunta es directa y busca conocer si los encuestados han sufrido algún tipo de ciberdelito reconocido en Colombia. La respuesta es fundamental para el análisis de la monografía al identificar de la población víctima de ciberdelitos.

Es importan en la encuesta definir si los encuestados han sufrido en algún momento de su vida o no de un ciberdelito; el aborda la información obtenida conducirá a resultados preciso para el Huila en la búsqueda de soluciones que mitigue la afectación de la problemática abordad en la encuesta.

Figura 16. Ha sido víctima de ciberdelitos



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

A partir de esta pregunta se inicia el proceso para identificar si los encuestados han sufrido de los ciberdelitos. Esta pregunta es el primer paso para identificar el historial de las victimas durante los últimos 5 años en el Huila.

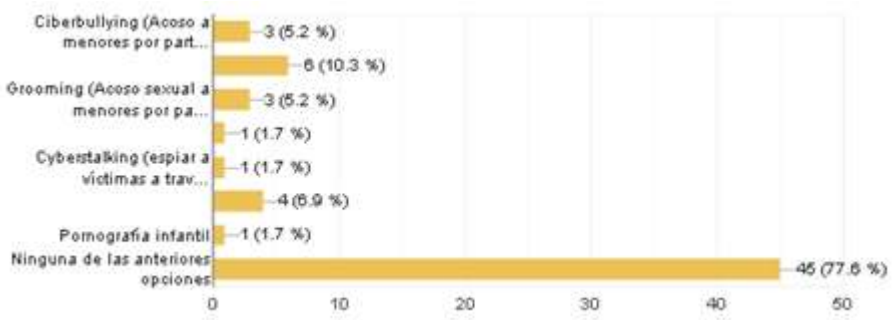
El 84.5% de los encuestados no han sufrido de un los ciberdelitos y el 15.5% sí. Aunque las cifras no son tan preocupantes para el Huila; es entendible que los encuestados no han sido víctimas por cuestiones ajenas a los ciberdelincuente porque existe la carencia de las buenas prácticas de los menores de edad para obtener el presente resultado.

Pregunta 13: Seleccione el ciberdelito que ha sido víctima

La pregunta tiene un listado de ciberdelitos identificados en Colombia y el Huila para que los encuestados puedan definir cuál de ellos ha sido víctima. Esta opción puede seleccionar una o varias opciones para responder.

Los ciberdelitos descrito en la pregunta han sido consultados en varias páginas web con el sustento jurídico y puede ser verificado en la referencia bibliográfica en este documento.

Figura 17. Ciberdelito que ha sido víctima



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

El resultado de la pregunta tiene un propósito establecer los ciberdelitos que han sido victima los encuestados por medio de la lista que se ha definido para ello en el formato de google forms.

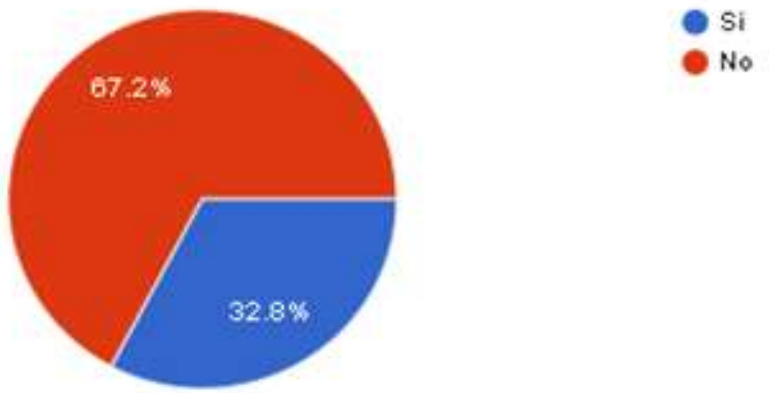
La pregunta ha generado la siguiente información: el 77.6% de los encuestados no ha sufrido ningún ciberdelito, el 10.3% son víctimas de sexting, el 6.9% de hacking, el 5.2% de grooming y el ciberbullying; el 6.9%, 1.7% en sextorción, Cyberstalking y pornografía infantil.

Pregunta 14: El delito informático fue reiterativo en los últimos cinco años

El estudio esta enfocado en identificar los ciberdelitos de los últimos 5años en el Huila; por ello la pregunta permite abordar un dato clave en el análisis y responder a la cantidad de casos identificados en el Huila.

Lo importante de la encuesta es dar respuesta al título de la monografía, por ello la importancia de conocer los casos y analizar la información obtenida para finalizar con la socialización de los resultados con la UNAD.

Figura 18. El ciberdelito fue reiterativo los últimos 5 años



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

La respuesta a la pregunta permite dimensionar los ciberdelitos que ha sido reiterativo en le Huila en los últimos 5 años e incluir los datos en el estudio mediante la generación de información actual del Huila con respecto a la ciberseguridad.

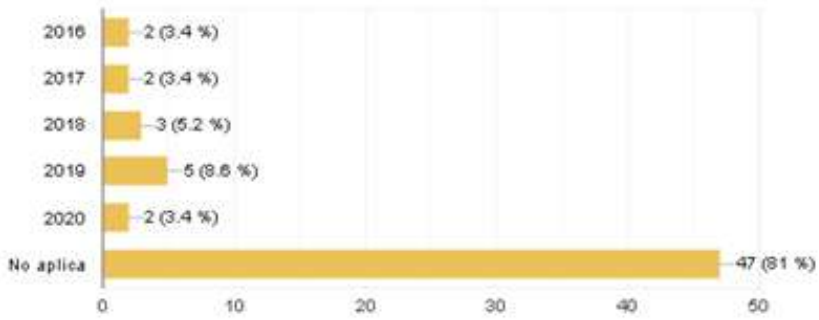
La encuesta arrojo un 67.2% no fue reiterativo el ciberdelito frente a un 32.8% caso contrario. Esta información da sustento que los ciberdelitos en el Huila son pocos frente a otros problemas del tema central.

Pregunta 15: Seleccione el tiempo de permanencia del ciberdelito que lo afecto.

La pregunta está dirigida en seleccionar el tiempo en año que permaneció el ciberdelito en el cual el menor de edad fue víctima teniendo en cuenta las preguntas anteriores.

Estos datos permitirán identificar la incidencia del ciberdelito durante los últimos 5 años y conocer la trascendencia de esta problemática en el departamento del Hila y a nivel nacional.

Figura 19. Porcentaje de ciberdelito por año



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

En este punto de la encuesta se ha recolectado información crucial para el estudio y definir lo importante en la trayectoria de los ciberdelitos en el Huila con el interés de realizar el estudio de la ciberseguridad.

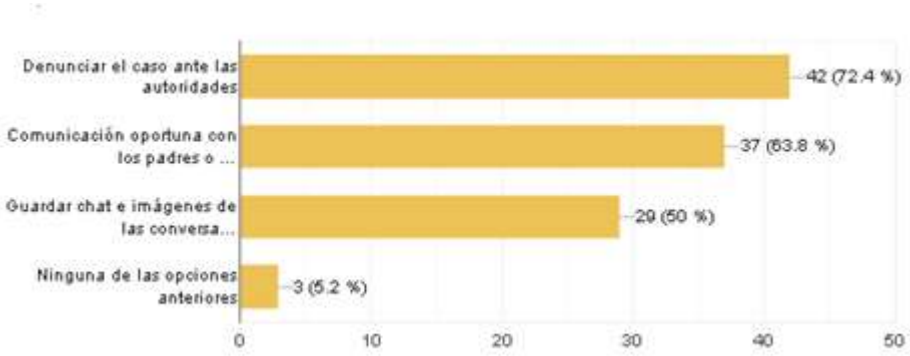
El resultado de la pregunta 19 deja en claro que el 81% de los menores de edad no fueron víctimas ni han permanecido el ciberdelito en los últimos 5 años, 8.6% sucedió entre el 2019, el 5.2% en el 2018, el 3.4% entre el año 2015, 2017 y 2020. Los datos obtenidos dejan ver el panorama tranquilo sobre los ciberdelitos en el Huila.

Pregunta 16: Que haría en el caso de ser víctima de un Ciberdelito.

No se puede desconocer parte de la ciberseguridad es identificar la forma preventiva y el proceder para detener los problemas que a diario sucede en el internet y sus diferente servicios de entretenimiento.

Los menores de edad deben seleccionar algunas de las medidas listada en el cuestionario para detener la fuerza de un ciberdelito y evitar ser una víctima más junto a los daños emocionales que trae el delito.

Figura 20. Actividades para denunciar un ciberdelito



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

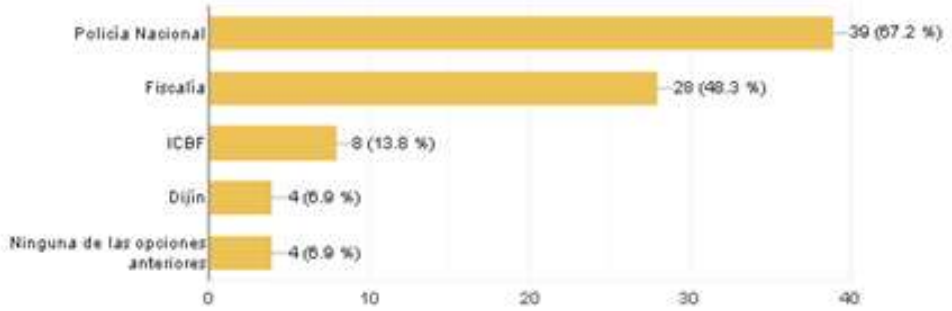
Esta pregunta se elabora con el propósito de conocer la certeza de los encuestados sobre los procedimientos que deben optar en el caso de desarrollar un ciberdelito. Para este ítem es apremiante identificar la postura de los menores de edad para escalar los delitos ante las entidades judiciales o persona competente.

Los resultados es: el 72.4% presentaría el caso ante las autoridades competente, 63.8% hablarían con los padres o acudientes, el 50% almacenaría las pruebas para denunciar y el 5.2% no haría nada frente al caso. Con énfasis de 3 de los 58 encuestados no harían nada ante los ciberdelitos; es por ello que las víctimas terminan sufriendo en silencio evitando el denunciar por tabú o temas ajenos a la realidad que los aparta del procedimiento correcto para generar ambiente seguro a los menores de edad del Huila.

Pregunta 17: Cuál de las siguientes instituciones interpondría una denuncia por Ciberdelito

La pregunta está enfocada en conocer las entidades en donde pueden presentar las denuncias por ciberdelitos. Los menores de edad y padres son los primeros que deben conocer las entidades encargadas del asunto por el debido cumplimiento de la ley y protección para los niños, niñas y adolescentes.

Figura 21. Instituciones para tomar las denuncias por ciberdelito



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

En algunas situaciones las víctimas y padres no presentan denuncias porque no saben cómo proceder o desconocen las entidades que los pueden ayudar con el problema; es por esta razón que la pregunta toma importancia en el análisis realizado por estudio de la monografía.

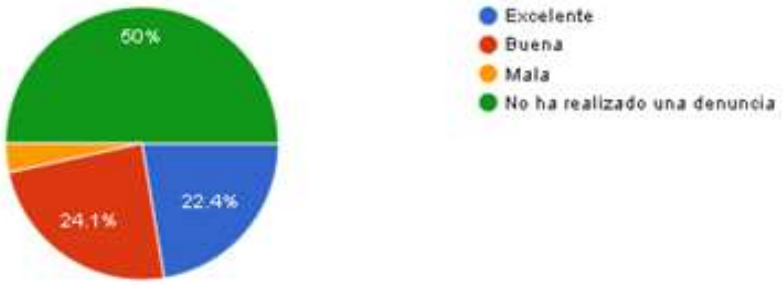
El resultado de la encuesta parte de esta pregunta; el 67.2% presentaría la denuncia con la Policía, 40.3% en la Fiscalía, 13.8% con el ICBF, 6.9% con la Dijín y el mismo porcentaje no tiene idea donde presentar la denuncia. En resumen la población encuestada tiene claro donde radicar la denuncia en la caso de presentase un ciberdelitos en los menores de edad en el Huila.

Pregunta 18: Califique la atención recibida por las instituciones de control frente al reporte de un Ciberdelito

La satisfacción de las víctimas y familia en cuanto a las denuncias presentada ante las entidades competentes por ciberdelitos en calidad de las víctimas en menor de edad; es un componente importante para lograr que las denuncias se tomen en serio y logre los resultados esperados.

La idea principal de la pregunta es que los menores de edad y sus familias tengan plena seguridad y tranquilidad que les prestaran la ayuda necesaria en el caso de las denuncias interpuestas y modelación de la perspectiva en cuanto a la confianza que depositan a las autoridades del gobierno departamental y nacional.

Figura 22. Confianza de las víctimas con respeto a las instituciones.



Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

El propósito de este dato obtenido por la pregunta es conocer estadísticamente la confianza que los padres y menores de edad refleja a las autoridades competen del Huila frente a las denuncias registradas.

Los resultados son: el 50% de los encuestados no han presentado denuncia por ciberdelito a menor de edad ante las autoridades, el 24.1% considerar que el actual de los entes es buena, el 22.4% es excelente el trabajo de las entidades y el 3.5% es mala. Concluye que los encuestados tienen un buen concepto de las autoridades en el momento de remitir las denuncias o problemas entorno de la ciberseguridad.

En general, la encuesta tiene información sobre la realidad del estudio en ciberseguridad y con ello definir elementos importantes para la toma decisiones en el futuro mediante los controles y estrategias correctas en pro de la seguridad de los niños, niña y adolescente del Huila.

En la sección siguiente de la monografía; se estudia a profundidad los datos estadísticos para determinar todas aquellas situaciones que han debilitado la ciberseguridad en los diferentes entornos web que interactúa los ciudadanos del Huila en especial los menores de edad.

7.3 ANALIZAR LOS HECHOS O ACCIONES QUE HAN OCURRIDO ENTORNO DE LOS CIBERDELITOS DE LOS NIÑOS, NIÑAS Y ADOLESCENTES EN EL DEPARTAMENTO DEL HUILA.

Metodología: Este objetivo se basa en analizar la información inquirida en las entidades de gobierno y cuestionario realizado para establecer el punto de quiebre de la ciberseguridad en el departamento del Huila.

El desarrollo de la investigación ha permitido comprender un grado asequibilidad del conocimiento que posee los niños, niñas y adolescentes del Huila frente al servicio que presta el internet (98.3%) y los riesgos asociados al mal uso (89.7%). Por el cual, se puede comprender una base importante de la seguridad informática en los entornos que a diarios son de uso frecuente para establecer relaciones sociales por medio del internet.

No todo es perfecto a la hora de la ciberseguridad; la práctica con respeto al tema; según resultados obtenido del cuestionario se puede precisar que no se toman las medidas pertinentes sobre el tema: considerando que el 46.3% de los encuestados no enfatizan en el uso de software para la ciberseguridad como son los antivirus, antispyware, entre otros. Teniendo en cuenta los dispositivo móviles usados con mayor frecuencia por los menores de edad en el acceso a Internet y salvaguardando la información personal y privada almacenada en estos dispositivos como por ejemplo no almacenar la información vital de los usuarios, tener instalados antivirus u otros programas de seguridad perimetral, acceder a sitios web seguro, no ingresar a correos dudoso, etc. Estas medidas o controles que pueda aplicar un menor de edad y padres, permitirá un primer elemento de seguridad contra los cibercriminales. Es importante dejar en claro que la seguridad perimetral de los celulares y Tablet no es efectivos frente a los innumerables casos ciberdelitos en la red.

El principal motivo de acceso a la Internet por parte de los menores de edad se debe a estudio (79.3%); seguido a esta actividad está el entretenimiento y redes sociales (50% aproximadamente). Los adolescentes de hoy en día se han encontrado en un mecanismo más sutil para satisfacer necesidades de la comunicación y reforzar relaciones sociales (PSISE, s.f.) a través del uso de la Internet.

[62] PSISE. ¿Cuáles son los peligros de las redes sociales para los adolescentes?. Disponible en: https://psisemadrid.org/cuales-son-los-peligros-de-las-redes-sociales-para-los-adolescentes/

Razón, que se debe proceder de la forma correcta y oportuna para amparar a la población de estudio en cualquier forma delictiva por medio del internet.

Es muy importante tener en cuenta aquellos aspectos de la sociedad adolescente**,** tanto a nivel de intimidad, sexualidad e identidad que han sido transferidos en parte a la era digital que nos encontramos**.** Es aquí donde toma valor la tesis por el cual un adolecente comparte mayor tiempo en el internet para satisfacer las principales necesidades (PSISE, s.f.).

Entre el 30% y 40% de los menores de edad han implementado alguna de las opciones de las buenas prácticas de la ciberseguridad definida en el cuestionario; por otro lado, el 60% de ellos navega en internet sin el mínimo cuidado para estar seguros. Esta situación ha demostrado un alto grado de vulnerabilidad por parte de esta población y al mismo tiempo los dispositivos móviles aumentando la posibilidad de ser víctima de un ciberdelito; en resumen, la adolescencia y la niñez están expuesto ante los cibercriminales por la falta de conocimiento sobre las buenas prácticas de ciberseguridad. Cuando el individuo contribuye a denunciar, esto lleva a debilitar un ciberdelito; de lo contrario impulsa la cibercriminalidad y aumenta las cifras de una problemática insaciable y destructiva.

El 39.7% de los encuestado tiene conocimiento para identificar un ciberdelito; esta situación permite comprender el índice precario en el dominio de los conceptos. En este punto de la investigación la cifra es realistas y veraz para hacer referencia al conocimiento básico que posee los menores de edad con respeto a la ciberseguridad. Sin embargo lograr identificar un ciberdelito no es fácil, pero tan poco difícil; es necesario establecer un juicio correcto en pro de la seguridad informática que permita un giro en la toma de medidas preventivas y correctivas orientada desde la ciberseguridad.

Aunque el 84.5% no ha sido víctima de un ciberdelito, es claro interpretar que no ha sido por prevención del menor de edad; si no la falta de interés por parte de un cibercriminal; con la información obtenida en la investigación se puede concluir que los adolescente pueden ser víctimas potenciales de los ciberdelitos en cualquier momento que se encuentra navegando en la internet.

[62] PSISE. ¿Cuáles son los peligros de las redes sociales para los adolescentes?. Disponible en: https://psisemadrid.org/cuales-son-los-peligros-de-las-redes-sociales-para-los-adolescentes/

En relación de los ciberdelitos de los últimos 5 años se puede contrastar los datos emitido por la Policía Nacional frente a los obtenidos por la encuesta. En primer lugar, la Policía ha suministrado la cantidad de los casos denunciado solo por el delito de pornografía infantil un 14.2% de la población ha sido afectada en promedio por año y la difusión de este delito en la Internet con un 4.4% en promedio por año.

En comparación a la encuesta el 1.7% ha sido víctima de pornografía infantil y el 10.3% por sexting. Además, la encuesta ha permitido conocer el porcentaje de otros ciberdelitos como Ciberbullying con un 5.2%, el Grooming 5.2%, Sextorción1.7%, Cyberstalking 1.7% y Hacking 6.9%; estas últimas cifras es producto del cuestionario y desconocido por las instituciones como la Policía Nacional de Colombia especialmente en el Huila.

El 32.8% de los encuestados, hace mención a los ciberdelitos que han sido afectado durante los últimos 5 años: donde los cibercriminales tiene una gran ventaja para extorsionar y obtener un beneficio de la situación que compromete con la integridad y bienestar de la víctima por el desconocimiento de las buenas prácticas de la ciberseguridad. Aunque el 4.26% (en promedio) de los casos tiene una permanecía en el transcurso de los últimos cinco años. Estas cifras son inferiores teniendo en cuenta los resultados generales de la encuesta donde hay una debilidad importante en la aplicación de la seguridad preventiva por parte de los usuarios e instituciones Huilense sin olvidar las denuncias oportunas. Estas consideraciones deben comprometer a las autoridades competentes e instituciones educativas para hacer frente al flagelo que se ve comprometido los menores de edad frente al ciberdelito.

El comportamiento de un individuo ante un ciberdelito ha demostrado que el 46.5% (en promedio) sabe que hacer frente a la situación. La otra parte, no es muy alentador el resultado; aun así, se puede mejorar el resultado por medio de estrategias que permita comprender una base de conocimiento necesaria para proceder ante una situación adversa y generar la conducta bajo el autocontrol de las actividades y circunstancia mientras esta en la Internet.

Otras medidas evidenciadas por la encuesta, permite descubrir que el 27.24% (en promedio) saben a dónde acudir para presentar una denuncia o asistir para asesoría frente a los ciberdelitos; el 23.3% tiene un concepto bueno de la entidades encargada para resolver las denuncias por ciberdelitos. Es aquí, donde las entidades departamentales y nacionales deben mejorar los mecanismos y protocolos de atención para devolver la confianza a la ciudadanía en general.

El 41.4% de los menores de edad encuestados han adquirido información sobre la ciberseguridad en los centros de educación y en segundo lugar los padres o acudientes con un 31%. Por el cual es necesario fortalecer la confianza entre los educandos, padres de familia y menores de edad en la impartición de los conocimientos y habilidades e los actores involucrados en el proceso.

En general, el análisis ha permitido conocer desde el punto de vista de los niños, niñas y adolescentes del Huila; una importante debilidad en el sistema actual de educación y comunicación entre los menores de edad, padres de familia y educandos; para lograr definir aptitudes propias en la aplicación de los conocimientos técnicos y conceptuales de la ciberseguridad. En el caso de las entidades de justicia deben ajustar los procedimientos y resultados que permita recobrar la confianza entre la institución y las victimas en el Huila.

7.4 ELABORAR UN INFORMÉ PARA ESTABLECER LOS HECHOS QUE HAN AFECTADO A LOS NIÑOS, NIÑAS Y ADOLESCENTES DEL HUILA Y LAS RECOMENDACIONES SOBRE LA CIBERSEGURIDAD.

Metodología: Este objetivo tiene como finalidad establecer las recomendaciones sobre el uso apropiado de los conceptos y herramientas disponibles en la actualidad sobre la ciberseguridad aplicado a los menores de edad en el departamento del Huila.

7.4.1 Informe la monografía parte de la información suministrada por la Policía Nacional y la encuesta aplicada a los menores de edad en el Huila. Las entidades como la Gobernación y Secretaria de educación departamental carecían de información en sus bases de datos sobre los ciberdelitos en los últimos 5 años que hayan afectado a los menores de edad en el departamento. En el caso del ICBF se abstuvo de suministrar información por la protección de los datos.

La encuesta suministra datos estadísticos importantes para el análisis de la información sobre la ciberseguridad en el departamento del Huila, según el siguiente cuadro:

Tabla 3. Resumen porcentual del cuestionario

PREGUNTA	RESPUESTA								
Usted tiene conocimiento sobre la Internet	Si				No				
	98.3%				**1.7%**				
Utiliza algún software para proteger la información, detectar página web o programas malicioso en el computador o dispositivo de su uso cotidiano	Si				No				
	53.4%				**46.6%**				
Donde ha recibido capacitación frente a la cultura de prevención en ciberseguridad.	Inst. educativa		Internet		Padres o persona de confianza		Otro		
	41.4%		**12.1%**		**31%**		**15.5%**		
Cuál es el uso que le da a la Internet	Entretenimiento		Estudio		Redes sociales		Otro		
	51.7%		**79.3%**		**50%**		**10.3%**		
Tiene conocimiento de los riesgos asociado al uso de la Internet	Si				No				
	89.7%				**10.3%**				
Seleccione alguna de las buenas prácticas que utiliza en la Internet	Inhabilitar contenidos o servicios de internet	Comparte contenidos o elementos apropiados	Pleno conocimiento de los contactos	Identifica proposiciones indecentes o acoso	Comunicación oportuna con padres o persona de confianza frente situaciones de peligro	Uso de antivirus u otro software para la ciberseguridad en el computador	Identifica sitios o página web seguro	Actualización de sistema operativo, navegadores, etc.	Ninguna de las opciones anteriores
	15.5%	**43.1%**	**32.8%**	**37.9%**	**48.3%**	**48.3%**	**43.1%**	**31%**	**12.1%**
Señale cuales de las siguientes situaciones puede ser un Ciberdelito	Contenidos dudoso en página web y/o correo		Chats o correos ofensivos	Solicitud para compartir fotos y videos íntimos		Conversaciones virtuales con persona desconocidas		Ninguna de las opciones	
	50%		**43.1%**	**63.8%**		**32.8%**		**12.1%**	
Teniendo en cuenta la respuesta anterior, diga si usted ha sido Víctima de algún tipo de Ciberdelito	Si				No				
	15.5%				**84.5%**				
Seleccione el ciberdelito que ha sido víctima	Ciberbullying (Acoso a menores por parte	Sexting (Envío de contenidos	Grooming (Acoso sexual a menore	Sextorsión (chantajear utilizand	Cyberstalking (espiar a víctimas a través de datos personales disponible en las redes sociales)		Hacking (Acceso sin autorización a datos	Pornografía infantil	Ninguna de las anteriores

	de otros menores)	eróticos)	s por parte de adultos)	o imágen es o vídeos íntimos de la víctima)		o programa s informátic os)		opcione s
	5.2%	**10.3%**	**5.2%**	**1.7%**	**1.7%**	**6.9%**	**1.7%**	**77.6%**
El delito informático fue reiterativo en los últimos cinco años	Si				No			
	32.8%				**67.2%**			
Selecciones el tiempo de permanencia del ciberdelito que lo afecto.	2016	2017		2018	2019		2020	No aplica
	3.4%	**3.4%**		**5.2%**	**8.6%**		**3.4%**	**81%**
Que haría en el caso de ser víctima de un Ciberdelito**.**	Denunciar el caso ante las autoridades	Comunicación oportuna con los padres o persona de confianza		Guardar chat e imágenes de las conversaciones, contenido de página web o redes sociales.			Ninguna de las opciones anteriores	
	72.4%	**63.8%**		**50%**			**5.2%**	
Cuál de las siguientes instituciones interpondría una denuncia por Ciberdelito	Policía Nacional	Fiscalía		ICBF	Dijín		Ninguna de las opciones anteriores	
	67.2%	**48.3%**		**13.8%**	**6.9%**		**6.9%**	
Califique la atención recibida por las instituciones de control frente al reporte de un Ciberdelito	Excelente	Buena		Mala	No ha realizado una denuncia			
	22.4%	**24.1%**		**3.4%**	**50%**			
Fuente: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform								

La información estadística del cuadro anterior permite evidenciar la necesidad para fortalecer los escenarios educativos orientado a los menores de edad sobre las medidas preventivas de la ciberseguridad y a los padres o acudientes; fortaleciendo el actuar de los niños, niñas y adolescentes en las buenas prácticas de la seguridad informática a partir del conocimiento y prácticas que ofrece hoy en día esta rama de la TIC. En el caso de las entidades competentes del orden departamental deben actualizar los protocolos de atención e investigación para devolver la confianza a las víctimas y sus familias.

A partir de la identificación de los ciberdelitos que han afectado a los niños, niñas y adolescentes del Huila puede ser ocasionada por las debilidades del sistema actual del gobierno nacional y departamental en cuanto al

procedimiento para implementar la ciberseguridad en el actuar del menor de edad frente al internet; por esto, se da conocer algunas recomendaciones.

7.4.2 Recomendaciones Los resultados obtenidos en el estudio; ha logrado obtener los siguientes resultados que deberá ser aplicado en la ciberseguridad de los niños, niñas y adolescentes del Huila según los siguientes escenarios:

- Establecer y aplicar las buenas prácticas en el uso de las TICS orientado a los menores de edad y padres.
- Definir una estrategia de enseñanza-aprendizaje en las instituciones educativas sobre la ciberseguridad.
- Responsabilidad y protocolos de las entidades competentes en la defensa de los derechos fundamentales y otros de los menores de edad en el departamento para una debida atención.

Buenas prácticas: la seguridad de los niños, niñas y adolescentes del Huila; es primordial, por esto el conocimiento y habilidades como estrategia de la ciberseguridad es fortalecer las medidas a seguir por parte de los padres o tutores y menores de edad para articular las siguientes actividades:

- Seguridad perimetral con los proveedores de internet, navegadores, etc. El acceso a internet debe bloquear sitios web no recomendado para los menores de edad.
- Instalar antivirus, antispyware u otro software que permita controlar y asegurar los contenidos e ingreso a sitios web, correos y escanear la información almacenada en el computador para encontrar alguna vulnerabilidad en el dispositivo usado para acceder a los servicios requeridos.
- Identificar los sitios web y correo seguros, para no comprometer la información personal, contenidos privados, etc.
- Plena identificación de los contactos en las redes sociales y sitios web.
- Contenidos apropiados para compartir en las redes sociales e internet.
- La confianza con un contacto no es el derecho ni el espacio correcto para compartir información personal, íntima y de índole privada.
- El chat y correo deben estar sujeto a un lenguaje propio y de respecto.
- Actualización del sistema operativo, navegadores y software en los computadores, celulares y dispositivo que permiten el acceso a internet.
- No almacenar información personal, íntima y privada en los dispositivos, ni en la nube.
- No abrir cuentas en las redes sociales u otras plataformas en internet a los menores de edad.
- Monitorear los sitios de internet que accede un menor de edad.

- No autoguardar y compartir las credenciales de acceso a las plataformas o redes sociales excepto a los padres.
- Diferenciar entre un amigo y un contacto en las redes sociales (AULASIENA).
- Diferencia entre mensaje apropiado a un maltrato escrito.
- Identificar proposiciones inadecuadas en el internet.
- Limitar el tiempo y horario de internet (SOFISTIC, s.f.)
- Limitar el acceso a tu perfil. Mantener la información en privado (UNILIBRE, 2016).
- Nunca envíes tus datos completos, nombres y apellidos, lugar de residencia, etc. (UNILIBRE, 2016)
- Elije un alias que sea diferente de tu nombre real. Evita el uso de cualquier información personal que ayude a identificar o localizar a alguien que estuviera en línea (UNILIBRE, 2016).
- Piénsalo dos veces antes de publicar una fotografía o videos personales. Las fotos y videos pueden ser utilizadas para identificarte y también pueden ser alteradas o compartidas sin tu conocimiento. (UNILIBRE, 2016)
- Vigilar qué permisos asignada a las 'apps' que usamos para asegurarnos de que no se comparten datos privados que debamos proteger (GOMEZ, s.f.).
- Incluir el doble factor de autenticación como medida de seguridad para el acceso a las plataformas que utilicen los niños y dispositivos de acceso (GOMEZ, s.f.).
- Los padres deben ser un referente para los menores y favorecer un entorno de confianza con ellos en el que nos puedan compartir y ayudarles en sus inquietudes y amenazas en la red (GOMEZ, s.f.)

Estrategias para el sector educativo Debe encaminar los programas educativos en las buenas prácticas de la ciberseguridad y reforzar las actividades que permita generar conciencia y concomimiento a los menores de edad, padres de familia y educandos a partir de:

[63] AULASIENA. 9 consejos de seguridad en Internet para niños. Disponible en: https://aulasiena.com/9-consejos-seguridad-internet-ninos/

[64] SOFISTIC. Utiliza herramientas de control parental. Disponible en: https://www.sofistic.com/blog-ciberseguridad/ensenar-seguridad-internet-ninos/

[65] UNILIBRE. Redes sociales: El uso y el abuso. 2016. [en Línea]. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/2349-redes-sociales-el-us-y-el-abuso

- Los padres deben ser digitales y bien informados en las TICS (AULASIENA): ellos deben asentar el ejemplo en el buen uso de la TIC, diálogo y la capacidad de resolver inquietudes de los hijos con el apoyo de las instituciones educativas.
- Estar alerta ante comportamientos extraños: los niños se despierten en la madrugada, se auto mutilen, etc. (POLICIA, 2017).
- Verificar las partes del cuerpo no visibles ya que se realizan autoflagelaciones específicas de códigos o símbolos como la "ballena" y otros símbolos (POLICIA, 2017)
- No permitir que se encuentren en lugares extraños con gente desconocida con el fin de realizar competencias o juegos inusuales (POLICIA, 2017).
- Escuela de padres: las instituciones educativas deben generar los espacios para capacitar y evaluar a los padres de familia frente al tema de ciberseguridad y la posición que deben ocupar por si se presenta un ciberdelito o la confianza que se pone a prueba con los hijos e búsqueda de elementos para mitigar la problemática.
- La secretaria de educación departamental debe contratar en su planta de docencia a profesional especializado en ciberseguridad para apoyar la formulación de proyectos educativos y aterrizar una estrategia en el proceso aprendizaje-enseñanza con los docentes de las diferentes instituciones educativas.
- Los planes de estudios y PEI debe incluir con suma importancia la ciberseguridad en la formación de sus alumnados y transformación del mundo digital para los menores de edad y padres de familia.
- Capacitar y evaluar a los docentes para fortalecer los conceptos y habilidades del conocimiento a impartir sobre la ciberseguridad.
- Generar guía de estudio para impartir al individuo conocimiento desde temprana edad o desde que inicia su proceso de formación (INCIBE, INCIBE acerca la ciberseguridad a niños de 5 a 8 años mediante un nuevo recurso, 2019).

---

[66] GOMEZ, A. En época de COVID-19, ¿sabes cómo proteger a tus hijos en las redes sociales?. Ën línea]. Disponible en: https://www.bbva.com/es/en-epoca-de-covid-19-sabes-como-proteger-a-tus-hijos-en-las-redes-sociales/

[67] POLICIA NACIONAL. ¿Sabe cómo prevenir que niños, niñas y adolescentes sean víctimas de la Ciberinducción al daño físico?. 2017. [En línea]. Disponible en: https://www.policia.gov.co/noticia/sabe-como-prevenir-que-ninos-ninas-y-adolescentes-sean-victimas-ciberinduccion-al-dano

- El material didáctico para los niños (as), debe ser muy interactivo para generar el conocimiento de la ciberseguridad desde el uso de los elementos que interactúa un infante hasta los servicios que pueden encontrar en estos medios. No podemos desconocer que los niños (as) a temprana edad son muy ágil para el manejo de los dispositivos móviles en la facilidad de acceso por parte de los padres para generar un elemento de entretenimiento.

Autoridades competentes en la defensa de los derechos de los menores de edad en el departamento Deben pensar en mejorar los protocolos para atender los casos que giran alrededor de los ciberdelitos especialmente a los menores de edad. Teniendo en cuenta que los ciudadanos no denuncian por la reputación de las entidades y el trato directo a las víctimas. Es decir, una víctima o familiar se siente ridiculizado y la demora en atender las denuncias. La magnitud de los ciberdelitos deja sin base a las intuiciones porque la gran mayoría de los casos no se pueden resolver; estos factores son determinantes al llevar a pensar en la inoperancia de las instituciones por parte de los ciudadanos en general.

Pese a que el mundo ha sufrido drásticos cambios a causa de la pandemia del COVID-19, aún siguen produciéndose fenómenos que ponen en riesgo la seguridad de los usuarios en las plataformas tecnológicas, en especial los niños. En estos momentos la ciberseguridad es un tema de gran importancia para proteger a los menores de edad porque en la actualidad se encuentran estudiando en la modalidad online desde sus domicilios y que se conectan a redes sociales durante su tiempo libre (LAFM, s.f.).

[68] INCIBE. INCIBE acerca la ciberseguridad a niños de 5 a 8 años mediante un nuevo recurso. 2019. [En línea]. Disponible en: https://www.incibe.es/sala-prensa/notas-prensa/incibe-acerca-ciberseguridad-ninos-5-8-anos-mediante-nuevo-recurso

[69] LAFM. Tips de ciberseguridad para proteger a los niños mientras estudian online. [En línea]. Disponible en: https://www.lafm.com.co/tecnologia/tips-de-ciberseguridad-para-proteger-los-ninos-mientras-estudian-online

Los riesgos para los niños ya no es problema en el uso del computador; hoy en día con la demanda de los teléfonos inteligentes, tablets: ha generado que en cualquier dispositivo tiene el beneficio de conectarse a Internet; conlleva a una serie de peligros para ellos al estar expuestos a ciberdelincuente como abusadores, hacking, ciber-bullying, programas espías, acceso a contenidos nocivos, etc. (RODRIGUEZ, 2015).

Los aspectos relacionados en este ítem, permiten una defensa orientada desde la perspectiva de las víctimas ejerciendo los controles sugeridos por la seguridad informática. La generalidad del estudio es presentar la información sustancial en la lucha contra los ciberdelitos mediante la responsabilidad de los actores en este proceso, conciencia y canales de comunicación para la protección de los individuos frente al flagelo de inseguridad en la internet.

[70] RODRIGUEZ, J. La seguridad en Internet no es un juego de niños. 2015. [En línea]. Disponible en: https://www.b-secure.co/blog/la-seguridad-en-internet-no-es-un-juego-de-ni%C3%B1os

8 CONCLUSIONES

La recolección de información ha dejado un sin sabor; porque las mismas entidades del orden departamental deberían velar por el cumplimiento de la leyes y la atención a una problemática que trasciende a nivel internacional y es asumida como tema de estudio por la monografía teniendo en cuenta las consideraciones que aplica al caso y los vacíos en cuanto a la información y procedimientos actuales definidos para las víctimas de los ciberdelitos especialmente los menores de edad en el Huila.

La carencia de información por parte de las instituciones del Huila ha nutrido la necesidad de abordar la problemática identificada en la monografía; para analizar la situación con mira de aportar conocimiento desde la UNAD que sirva de referente para generar entornos seguros en la Internet y despertar las aptitudes del menor de edad para cuidarse de los ciberdelitos por medio de hábitos según las buenas prácticas de la seguridad informática. Los resultados del presente trabajo es La oportunidad para realizar un aporte significativo a la sociedad a través de las recomendaciones a la sociedad en general teniendo en cuenta el flagelo que afecta al Huila y cada día aumenta los casos reportados toda vez que los ciberdelincuente sofistican su procedimiento criminal.

La información estadística suministrada por la encuesta, ha permitido comprender la perspectiva que tiene los niños, niñas y adolescentes frente a la ciberseguridad y el nivel de conocimiento para hacer frente a los ciberdelitos. Aunque los datos no son tan críticos, si permite hacer unas reflexiones preocupantes e importante frente al tema sobre todo en tiempo de pandemia.

El análisis realizado en la monografía; dimensiona la situación actual y futura del Huila frente a la ciberseguridad, teniendo en cuenta que los menores de edad desconocen los elementos importantes en el tema y las buenas prácticas con el ánimo autocuidarse mientras navegan en internet. Es importante dejar en claro que los menores de edad en un futuro no muy lejano pueden ser víctimas de los ciberdelitos con una probabilidad alta de continuar con el esquema evidenciado por el estudio.

Los organismos como la ONU y UNICEF enfatizan sobre los cuidados a tener en cuenta con los menores de edad y garantizar sus derechos de forma departamental, nacional e internacional. No ajeno a esto, la monografía aporta las estrategias y recomendaciones a seguir en tres frentes de ataque que puedan mitigar la cibercriminalidad en el Huila de forma preventiva y correctiva.

El proyecto pretende cambiar la percepción de la sociedad al considerar más importante el dinero que las personas; teniendo en cuenta que la mayoría de las consultadas realizada en internet está centrada en investigar las debilidades o vulnerabilidades de los sistemas de información de las empresas con el ánimo de contribuir a salvaguardar sus activos y con ello contrarrestar los delitos que termine costando mucho dinero. Aun así, no se debe menosprecia la contribución de la seguridad informática en las empresas; se buscar orientar las investigaciones al diario vivir (omisión o acción) de las personas para mitigar los errores que lleva a materializar un ciberdelito por la falta de cultura en las buenas prácticas y terminan costando en todo sentido a la persona o sociedad por la forma tan deliberada de hacer las cosas. Por esta razón, la monografía está centrada en comprender el enfoque social y compartir recomendaciones desde la ciberseguridad a los habitantes del Huila.

Por último concluyo que la monografía espera despertar en el futuro trabajos investigativos que contribuyan a la sociedad en el desarrollar de soluciones encaminada a los resultados generados por el presente documento. Por otra parte, concientizar a las entidades del orden judicial, administrativa y educativa en el Huila para empezar a preocuparse por la problemática que puede afectar a los niños, niñas adolescentes del departamento para establecer e implementar mecanismos que permita generar las habilidades de cada persona, aporta recursos o incentivos para apoyar futuras investigaciones y sobre todo generar acuerdos, normas o leyes que brinde el sustento jurídico para considerar a los menores de edad como una prelación ante los altos índices de cibercriminalidad del país y pronto tocara las puertas en el Huila.

9 BIBLIOGRAFIA

9.1 REFERENCIA SITIO WEB

BOLAÑOS DÍAS, Andrés y Narváez Narváez, Teresa. Análisis comparativo sobre delitos informáticos en Colombia con relación a seis países de Latinoamérica. San Juan de Pasto. [En línea]. 2014. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2656/1/59830899.pdf

ABUSHIHAB COLLAZOS, Amir. Cibercrimen una aproximación a la delincuencia informática. [En línea]. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/1995/abushihabamir2016.pdf?sequence=1&isallowed=y

PASCUAL, Iván. Ciberdelincuencia Desarrollo y persecución tecnológica. [En línea]. 2013. Disponible en: http://oa.upm.es/22176/1/PFC_IVAN_MATEOS_PASCUAL.pdf

RENDLE, Ben. Gestionar el riesgo de la ciberdelincuencia. [En línea]. 2014. Disponible en: https://pmi-mad.org/index.php/socios/articulos-direccion-proyectos/779-grcd-sp-1966650659

ACURIO DEL PINO, Santiago. Delitos Informáticos: Generalidades. [En línea]. Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

SYMANTEC. Tendencias de seguridad cibernética en américa latina y el caribe. [En línea] 2014. Disponible en: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

MINISTERIO TIC. Ministerio TIC participó en firma del 'Pacto de Cero Tolerancia con la Pornografía Infantil en Internet. [En línea]. 2016. Disponible en: https://www.mintic.gov.co/portal/604/w3-article-14513.html

MINISTERIO TIC. “Colombia es referente mundial en la lucha contra la ciberdelincuencia y el cibercrimen": Ministro David Luna. [En línea]. 2016. Disponible en: https://www.mintic.gov.co/portal/604/w3-article-19964.html

PRESIDENCIA DE LA REPÚBLICA. Avance clave en seguridad digital para Colombia, el Congreso aprobó ley de adhesión a Convención de Budapest. [En

línea]. 2018. Disponible en: http://es.presidencia.gov.co/noticia/180621-Avance-clave-en-seguridad-digital-para-Colombia-el-Congreso-aprobo-ley-de-adhesion-a-Convencion-de-Budapest

EL PAÍS. "Es necesario innovar en la lucha contra el cibercrimen": Santos. [En línea]. 2017. Disponible en: https://www.elpais.com.co/colombia/es-necesario-innovar-en-la-lucha-contra-el-cibercrimen-santos.htm l

REVISTA MILITAR DIGITAL. Fuerzas Armadas de Colombia contrarrestan ciberdelincuencia. [En línea]. 2017. Disponible en: https://dialogo-americas.com/es/articles/colombian-armed-forces-counter-cybercrime

MCAFEE. Informe sobre Criminología Virtual de McAfee. [En línea]. Disponible en: https://www.estudiocriminal.eu/wp-content/uploads/2017/03/Informe-sobre-criminologia-virtual-de-McAfee.pdf

RODRÍGUEZ ARBELÁEZ, Juna. Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. [En línea]. Disponible en: http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf

TORRES ROJAS, Lesdy. Ensayo de diplomado para optar al título de profesional en relaciones internacionales y estudios políticos. [En línea]. 2018. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/18104/TorresRojasLesdyDaniela2018.

ICBF. Ley de Infancia y Adolescencia. [En línea]. Disponible en: https://www.icbf.gov.co/bienestar/ley-infancia-adolescencia

CANAL INSTITUCIONAL. Así trabaja el Centro Cibernético Policial. [En línea]. 2018. Disponible en: https://www.canalinstitucional.tv/noticias/asi-trabaja-centro-cibernetico-policial

DELITO INFORMÁTICO. Los delitos cibernéticos, un problema que va en aumento. [En línea]. 2018. Disponible en: https://delitosinformaticos.com/03/2018/delitos/los-delitos-ciberneticos-problema-va-aumento

CANCILLERÍA. Congreso de Colombia aprobó ley de adhesión a la Convención de Budapest (20-06-2018). La propuesta del Gobierno pasó los cuatro debates y entrará a sanción presidencial. [En línea]. 2018 Disponible en: http://www.cancilleria.gov.co/en/newsroom/news/2018-06-25/19306

PRESIDENCIA. Ley No.1928 24 JUL2018. [En línea]. Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

MINISTERIO TIC. Ley 1273 de 2009. [En línea]. Disponible en: https://www.mintic.gov.co/portal/604/w3-article-3705.html

COOPERACIÓN ESPAÑOLA. Herramientas para luchar contra la ciberdelincuencia en Iberoamérica. [En línea]. Disponible en: http://www.aecidcf.org.co/MDC/content/herramientas-para-luchar-contra-la-ciberdelincuencia-en-iberoam%C3%A9rica

POLICÍA NACIONAL. Denunciar delitos informáticos. [En línea]. Disponible en https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Lifeder. Cuadro Comparativo: Características, Tipos, Ejemplos. [En línea]. Disponible en: https://www.lifeder.com/cuadro-comparativo/

PORTAL EDUCATIVO. ¿Qué es una línea de tiempo y cómo se organizan. [En línea]. Disponible en: https://www.portaleducativo.net/quinto-basico/507/Que-es-una-linea-de-tiempo-como-se-organizan

RODRIGUEZ, Hellin. La teoría de las metas de logro. [En línea]. Disponible en: https://www.tdx.cat/bitstream/handle/10803/10787/HellinRodriguez02de06.pdf

LA NACIÓN. El reto tecnológico. Disponible en: https://www.nacion.com/opinion/el-reto-tecnologico/VDNLZUIL3FEY5KG3DYRV2LMVJY/story/

UNIVERSIDAD LIBRE. Redes sociales: El uso y el abuso. [En línea]. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/2349-redes-sociales-el-us-y-el-abuso

KIDS HEALTH. Abuso infantil. [En línea]. Disponible en: https://kidshealth.org/es/parents/child-abuse-esp.html

REDES ZONE. Privacidad y seguridad en redes sociales. [En línea]. Disponible en: https://www.redeszone.net/seguridad-informatica/redes-sociales/

OSI. Redes sociales. [En línea]. Disponible en: https://www.osi.es/es/redes-sociales

INFORMÁTICA FORENSE. Cómo utilizar las redes sociales de forma segura. [En línea]. Disponible en: https://www.informaticaforense.com.co/como-utilizar-las-redes-sociales-de-forma-segura/

CYBSEC. Seguridad en las Redes Sociales. [En línea]. Disponible en: http://www.cybsec.com/upload/seguridad_en_redes_sociales_v1_1.pdf

VANEGAS GALLARDO, Alberto. Seguridad informática en el hogar. [En línea]. Disponible en: http://www.ii.unam.mx/es-mx/AlmacenDigital/Notas/Paginas/seguridadinformatica.aspx

CR CONSULTORES LEGALES. Adolescentes, privacidad y ciberdelincuencia. [En línea]. 2016. Disponible en: https://www.crconsultoreslegales.com/1065-2/

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Amenazas y recomendaciones para menores de edad en el uso de la tecnología. [En línea]. Disponible en: https://revista.seguridad.unam.mx/numero-28/amenazas-y-recomendaciones

ELLISON, kille. Por qué el cibercrimen no es un juego de niños. [En línea]. 2016. Disponible en: https://www.welivesecurity.com/la-es/2016/02/29/cibercrimen-no-es-juego/

POLICÍA NACIONAL. Amenazas del Cibercrimen en Colombia 2016-2017. [En línea]. 2017. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

VELIS, Roció. Ciberdelincuencia de género: el nuevo maltrato silencioso. [En línea]. 2017. Disponible en: http://elcorreoweb.es/temas-de-portada/ciberdelincuencia-de-genero-el-nuevo-maltrato-silencioso-AC3567604

GARCÍA, José. Aumentan casos de ciberdelitos contra menores en el país. [En línea]. 2015. Disponible en: https://www.eltiempo.com/archivo/documento/CMS-16207955

EL HERALDO. Delitos sexuales en internet: más de 3.000 niños han sido víctimas en Colombia. [En línea]. 2018. Disponible en: https://www.elheraldo.co/colombia/delitos-sexuales-en-internet-mas-de-3000-ninos-han-sido-victimas-en-colombia-448042

CARRIZO, Mercedes. Las redes sociales como factor determinante de transgresión en la comunicación entre adolescentes. [En línea]. 2012. Disponible en: http://di.usal.edu.ar/archivos/di/carrizo_mercedes.pdf

INFORMÁTICA FORENSE COLOMBIA. Grooming. [En línea]. 2018. Disponible en: https://www.informaticaforense.com.co/grooming

BÉCARES, Bárbara. MinTIC colombiano quiere perseguir el acoso a menores en la Red. [En línea]. 2016. Disponible en: https://www.siliconweek.com/software/mintic-colombiano-quiere-persguir-acoso-menores-la-red-67134

ROJAS MORALES, Danyorsa. Cirberacoso de niños, niñas y adolescentes en las redes sociales: un estudio sobre los sistemas de protección y prevención judicial. [En línea]. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/2564/1/PROYECTO%20DE%20REFLEXION%20CIBERACOSO%20NI%C3%91OS%2C%20NI%C3%91AS%20Y%20ADOLESCENTES%20EN%20%20LAS%20REDES%20SOCIALES.pdf

PÉREZ, Albéniz. Uso y abuso de tecnologías en adolescentes y su relación con Algunas variables de personalidad, estilos de crianza, consumo de alcohol y autopercepción como estudiante. [En línea]. Disponible en: http://riubu.ubu.es/bitstream/10259/219/1/Garrote_P%C3%A9rez_de_Alb%C3%A9niz.pdf

E-JUSTICIA. Compendio normativo sobre ciberdelincuencia. [En línea]. 2018. Disponible en: http://www.cumbrejudicial.org/asamblea-plenaria/documentacion-posterior-asamblea-plenaria-edicion-xix/download/1003/673/15

UNIVERSIDAD LIBRE. Las redes sociales y la violación al derecho a la intimidad. [En línea]. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/258-las-redes-sociales-y-la-violacion-al-derecho-a-la-intimidad

UNICEF. Niños en un mundo. [En línea]. 2017. Disponible en: digitalhttps://unicef.org.co/sites/default/files/informes/SOWC_2017_SP%20vcomplete.pdf

GARCIA GANCHON, Jonathan. TFM - Ad hoc Seguridad y Riesgo: Ciberbullying, Grooming y Sexting. [En línea]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72526/6/ingjonathangarciaTFM0118memoria.pdf

SENADO DE COLOMBIA. PROYECTO DE LEY ____ DE 2018. Por la cual se formulan los lineamientos de política pública para la prevención de delitos realizados a través de medios informáticos o electrónicos, en contra de niñas, niños y adolescentes, se modifica el Código Penal y se dictan otras Disposiciones. [En línea]. Disponible en: http://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2018%20-%202019/PL%20074-18%20Crimenes%20Ciberneticos.pdf

PARTIDO MIRA. Aprobado proyecto de Ley de MIRA que busca combatir ciberdelitos. [En línea]. Disponible en: https://partidomira.com/aprobado-proyecto-de-ley-de-mira-que-busca-combatir-ciberdelitos/

KASPERSKY. ¿Qué es la ciberseguridad?. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

ROBLES PUESTES, Hernando. Panorama actual de la seguridad informática o de la Ciberseguridad, a nivel del país y las tendencias actuales y futuras a nivel global. [En línea]. 2018. Disponible en: https://repository.unad.edu.co/handle/10596/24018

UNIVERSIDAD DE LOS ANDES. Ciberseguridad en la era del internet de las cosas. [En línea]. Disponible en: https://sistemas.uniandes.edu.co/images/forosisis/revista/8/pdf/FOROS-ISIS-8.pdf

IEEE. Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. [En línea]. 2010. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

BERCIANO, Javier. La importancia y la necesidad de proteger la información sensible. [En línea]. Disponible en: http://www.redseguridad.com/especialidades-tic/proteccion-de-datos/la-importancia-y-la-necesidad-de-proteger-la-informacion-sensible

GUAPACHA DÍAZ, Jenny. Un estudio comparado entre España y Colombia sobre el Ciberbullying como un posible tipo penal para Colombia. [En línea]. 2014. Disponible en: https://repository.ucatolica.edu.co/handle/10983/2233

FRANCO REYES, Aura. Las redes sociales y los delitos de injuria y calumnia en Colombia. [En línea]. 2017. Disponible en: https://repository.ucatolica.edu.co/handle/10983/14511

GONZÁLEZ GONZÁLEZ, Yaneth. Análisis de los delitos informáticos fijados por la ley 1273 de 2009 en relación con las redes sociales en Colombia. [En línea]. 2016. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/3608/5/Modelo_RAE_Facultades.pdf

MEZA ARDILA, Jenny. Los delitos sexuales en contra de los niños, niñas y adolescentes en las redes sociales: beneficios de los mecanismos de protección y prevención judicial. [En línea]. 2015. Disponible en: https://repository.ucatolica.edu.co/handle/10983/2621

CASTRO JARAMILLO, Ángela. Derecho a la intimidad en las redes sociales de internet en Colombia. [En línea]. 2016. Disponible en: https://repository.ucatolica.edu.co/handle/10983/16407

CATALÁN ALEGRE, David. Desarrollo y ciberseguridad en una red social de contenido multimedia. [En línea]. 2016. Disponible en: http://repositori.uji.es/xmlui/handle/10234/167041

CRC. Identificación de las posibles acciones regulatorias a implementar en materia de Ciberseguridad. [En línea]. Disponible en: https://www.crcom.gov.co/recursos_user/Documentos_CRC_2015/Actividades_regulatorias/Ciberseguridad/Doc_Ciberseguridad28_07_15.pdf

MONSALVE, Jaime. Ciberseguridad: principales amenazas en Colombia (ingeniería social, phishing y dos). [En línea]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4663/00004883.pdf?sequence=1&isAllowed=y

ENDARA DAZA, Francisco y PASMAY, Fausto. Análisis de redes sociales riesgos y beneficios. [En línea]. 2012. Disponible en: http://repositorio.usfq.edu.ec/handle/23000/4358

INCIBE. El centro de seguridad en internet para menores ayudará a niños y adolescentes a prevenir riesgos en la red. [En línea]. 2017. Disponible en: https://www.incibe.es/sala-prensa/notas-prensa/el-centro-seguridad-internet-menores-ayudara-ninos-y-adolescentes-prevenir

EL HERALDO. El Instituto Nacional de Ciberseguridad apuesta por enseñar a niños y adolescentes a protegerse en las redes sociales. [En línea]. 2017. Disponible en: https://www.heraldo.es/noticias/sociedad/2017/12/05/el-instituto-nacional-ciberseguridad-apuesta-por-ensenar-ninos-adolescentes-protegerse-las-redes-sociales-1212260-310.html

ESET. Guía de Seguridad en Redes Sociales. [En línea]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_redes_sociales_baja.pdf

TREND MICRO. Seguridad en Internet para niños y familias. [En línea]. Disponible en: https://www.trendmicro.com/es_es/initiative-education/internet-safety-kids-families.html

PINILLOS HERNÁNDEZ, Ricardo. Ciberseguridad para menores, asunto de todos. [En línea]. 2018. Disponible en: https://www.elcolombiano.com/opinion/columnistas/ciberseguridad-para-menores-asunto-de-todos-NA8727719

PANDA SEGURITY. Enseñando ciberseguridad desde el colegio. [En línea]. 2014. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/ensenar-ciberseguridad-colegio/

GUZMÁN FLÓREZ, Camilo y ANGARITA PINZÓN Cristian. Protocolos para la mitigación de ciberataques en el hogar. Caso de estudio: estratos 3 y 4 de la ciudad de Bogotá. [En línea]. 2017. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/15321/1/Cibersecurity%20Home.pdf

LINTI. Ciberseguridad ¿De qué hablamos cuando hablamos de "Ciberseguridad"?. [En línea]. Disponible en: https://www.linti.unlp.edu.ar/ciberseguridad

MOSQUERA GENDE, Ingrid. Día Internacional de la Seguridad Informática: uso de internet y buenas prácticas docentes. [En línea]. 2018. Disponible en: https://www.unir.net/educacion/revista/noticias/dia-internacional-de-la-seguridad-informatica-uso-de-internet-y-buenas-practicas-docentes/549203661296/

KASPERSKY. Ciberseguridad con garantía de future. [En línea]. 2016. Disponible en: https://www.kaspersky.es/blog/dublin-forum-2016/9086/

POLICÍA NACIONAL. Ciberseguridad en Colombia. [En línea]. 2014. Disponible en: https://www.policia.gov.co/noticia/ciberseguridad-en-colombia

EJÉRCITO NACIONAL. Seguridad de la Información y tendencias estratégicas de ciberseguridad. [En línea]. 2017. Disponible en: https://www.esmic.edu.co/sala_prensa/articulos/seguridad_informacion_tendencias_2508

INCIBE CERT. Defensa activa e inteligencia: de la teoría a la práctica. [En línea]. 2018. Disponible en: https://www.incibe-cert.es/blog/defensa-activa-e-inteligencia-teoria-practica

REVISTA KUBERNETICA. El hombre y la tecnología: del hombre moderno al hombre primitivo. [En línea]. 2010. Disponible en: http://www.santiagokoval.com/2011/04/27/el-hombre-y-la-tecnologia-del-hombre-moderno-al-hombreprimitivo/

CALDERÓN CARRILLO, Daniel. Los niños como sujetos sociales. Notas sobre la antropología de la infancia. [En línea]. 2015. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-06362015000100007

VUANELLO, Graciela. Los niños frente a Internet: seguridad, educación y tecnología. [En línea]. 2015. Recuperado de: https://www.redalyc.org/articulo.oa?id=60741185005

MONTES AGUDELO, Carolina y VARGAS FORERO, Viviana. Problemas de ingeniería social y su implicación en la adolescencia de Colombia. [En línea]. 2018. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/22583/41946700.pdf?sequence=1&isAllowed=y

INCIBE. NCIBE acerca la ciberseguridad a niños de 5 a 8 años mediante un nuevo recurso. [En línea]. 2019. Disponible en:https://www.incibe.es/sala-prensa/notas-prensa/incibe-acerca-ciberseguridad-ninos-5-8-anos-mediante-nuevo-recurso

MINISTERIO DE EDUCACIÓN. Ley 1620 de 2013. [En línea]. Disponible en: https://www.mineducacion.gov.co/1759/articles-327397_archivo_pdf_proyecto_decreto.pdf

SECRETARIA SENADO. Ley 1273 de 2009. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

INFORMÁTICA JURÍDICA. Legislación Informática de Colombia. [En línea]. Disponible en: http://www.informatica-juridica.com/legislacion/colombia/

MINISTERIO DE LA TIC. Ley 1336 del 2009. [En línea]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3706_documento.pdf

PRESIDENCIA. Ley 1928 de 2018. [En línea]. Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

ANDRADE ORTIZ, Hamilton. Cuestionario sobre Ciberseguridad - UNAD. [En línea]. Neiva, 2020. Disponible en: https://docs.google.com/forms/d/e/1FAIpQLSe-V57CAppZ4najKuOJca6GFFg_o8GjRvutAll3yyl3YKtixQ/viewform

ANEXOS

ANEXO A

Respuesta del instituto colombiano de bienestar familiar - ICBF sobre delitos informáticos de los últimos 5 años que haya afectado a los niños, niñas y adolescentes del Huila.

Gmail

Hamilton Andrade <ing.hamilton.andrade@gmail.com>

Derecho de Petición Información y Orientación SIM No. 1762120551 (EMAIL CERTIFICADO de RespuestasPQRS@icbf.gov.co)
1 mensaje

EMAIL CERTIFICADO de RespuestasPQRS@icbf.gov.co <402666@certificado.4-72.com.co> 15 de septiembre de 2020 a las 07:39
Responder a: RespuestasPQRS@icbf.gov.co
Para: ing.hamilton.andrade@gmail.com

AVISO IMPORTANTE: Esta dirección de correo electrónico** RespuestasPQRS@icbf.gov.co **es de uso único y exclusivo de envío de notificaciones, todo mensaje que se reciba no será leído y automáticamente se eliminará de nuestros servidores.

Señor ciudadano por favor no responda este correo, si desea comunicarse con ICBF debe hacerlo a través del correo atencionalciudadano@icbf.gov.co

Instituto Colombiano de Bienestar Familiar
Cecilia De la Fuente de Lleras
Dirección de Servicios y Atención

El futuro es de todos

12600/SIM 1762120561

Bogotá D.C.,

Señor:

HAMILTON ANDRADE

Dirección física o electrónica: ing.hamilton.andrade@gmail.com

ASUNTO: Derecho de Petición Información y Orientación SIM No. 1762120551 (Para consultas cite este número)

Respetado señor:

Con toda atención nos permitimos informarle que hemos recibido su solicitud de fecha 12 de septiembre de 2020, en los siguientes términos: "(...) Solicitud de información para investigación (...)"

En respuesta a su solicitud es conveniente indicarle que, con el fin de adelantar el oportuno y efectivo direccionamiento de su petición al área competente, le agradecemos remitirnos su solicitud acompañada de los siguientes documentos, los cuales se encuentran publicados en la página web del ICBF, en el siguiente link: https://www.icbf.gov.co/evaluacion/monitoreo-y-seguimiento-la-gestion

Allí podrá descargar: el formato para la presentación de los proyectos de investigación externos y diligenciarlo completamente, formato acta de compromiso de confidencialidad para particulares o instituciones, diligenciado, con firma y huella, y carta de aval de la institución de educación superior o entidad solicitante

Cabe resaltar que dentro de los documentos que adjunta no se encuentra la carta de aval de la institución de educación superior o entidad solicitante, es necesaria para darle trámite a su solicitud.

Si requiere información sobre programas, trámites y servicios del ICBF, consulte nuestro portafolio de servicios en la página web, ingresando al enlace: https://www.icbf.gov.co/portafolio-de-servicios-icbf. También podrá solicitar asesoría en Derecho en Familia, y/o presentar quejas, reclamos o sugerencias las 24 horas del día a través de nuestros canales de atención, Línea Gratuita Nacional: 01-8000-91-8080, correo electrónico: atencionalciudadano@icbf.gov.co y en la página web www.icbf.gov.co, opciones: Solicitudes PQRS, Chat ICBF, Videollamada o Llamada en Línea.

Recuerde que, si desea reportar un caso por presunta vulneración de derechos de los niños, niñas y adolescentes, lo podrá realizar a través de la Línea 141, de las líneas de WhatsApp: 320 239 16 85 – 320 239 13 20 - 320 865 54 50 o por cualquiera de nuestros canales de atención.

Cordialmente,

Dirección de Servicios y Atención
BIENESTAR FAMILIAR
Línea gratuita nacional ICBF:
01 8000 91 80 80
www.icbf.gov.co

Cordial saludo,

Envío documento solicitados por ICBF para obtener información de los últimos 5 años de ciberdelitos que han afectado a los niños, niñas y adolescentes del Huila para realizar monografía con el título: ESTUDIO DE CIBERSEGURIDAD DE LOS ÚLTIMOS 5 AÑOS EN EL TEMA DE DELITOS INFORMÁTICOS DIRIGIDO A LOS NIÑOS, NIÑAS Y ADOLESCENTES EN EL DEPARTAMENTO DEL HUILA.

Agradezco la atención a la presente y en espera de una pronta respuesta.

Hamilton Andrade O.

Cel: 3143739574

Candidato al título de Especialista en Seguridad Informática de la UNAD

---------- Forwarded message ----------
De: <RespuestasPQRS@icbf.gov.co>
Date: vie., 28 de ago. de 2020 a la(s) 07:03
Subject: Derecho de Petición - Información y Orientación SIM No. 1762085251
To: <ing.hamilton.andrade@gmail.com>
Cc: <correo@certificado.4-72.com.co>

Instituto Colombiano de Bienestar Familiar
Cecilia De la Fuente de Lleras
Dirección de Servicios y Atención

El futuro es de todos

12600/SIM 1762085251

Bogotá D.C.,

Señor:

HAMILTON ANDRADE O.

Dirección física o electrónica: ing.hamilton.andrade@gmail.com

ASUNTO: Derecho de Petición - Información y Orientación SIM No. 1762085251 (Para consultas cite este número)

Respetado Señor,

En atención a la solicitud de fecha 21 de agosto de 2020, registrada con el número del asunto, mediante la cual indica "(…) Soy estudiante de la UNAD en la Especialización de Seguridad Informática y me encuentro desarrollando la monografía con el título: estudio de ciberseguridad de los últimos 5 años en el tema de delitos informáticos dirigido a los niños, niñas y adolescentes en el departamento del huila, por esta razón, solicito su colaboración para obtener información de los últimos 5 años en cuanto a los delitos informáticos que han afectado a los niños, niñas y adolescentes del Huila. (…)", con el presente nos permitimos informarle que:

En respuesta a su solicitud es conveniente indicarle que, con el fin de adelantar el oportuno y efectivo direccionamiento de su petición al área competente, le agradecemos remitirnos su solicitud acompañada de los siguientes documentos, los cuales se encuentran publicados en la página web del ICBF, en el siguiente link: https://www.icbf.gov.co/evaluacion/monitoreo-y-seguimiento-la-gestion

Allí podrá descargar: el formato para la presentación de los proyectos de investigación externos y diligenciarlo completamente, formato acta de compromiso de confidencialidad para particulares o instituciones, diligenciado, con firma y huella, y carta de aval de la institución de educación superior o entidad solicitante.

Si requiere información sobre programas, trámites y servicios del ICBF, consulte nuestro portafolio de servicios en la página web, ingresando al enlace: https://www.icbf.gov.co/portafolio-de-servicios-icbf. También podrá solicitar asesoría en Derecho en Familia, y/o presentar quejas, reclamos o sugerencias las 24 horas del día a través de nuestros canales de atención, Línea Gratuita Nacional: 01-8000-91-8080, correo electrónico: atencionalciudadano@icbf.gov.co y en la página web www.icbf.gov.co, opciones: Solicitudes PQRS, Chat ICBF, Videollamada o Llamada en Línea.

Recuerde que, si desea reportar un caso por presunta vulneración de derechos de los niños, niñas y adolescentes, lo podrá realizar a través de la Línea 141, de las líneas de WhatsApp: 320 239 16 65 – 320 239 13 20 - 320 865 54 50 o por cualquiera de nuestros canales de atención.

Cordialmente,

Dirección de Servicios y Atención

ICBF Sede de la Dirección General

Avenida carrera 68 No. 64 C– 75
atencionalciudadano@icbf.gov.co

INFORMACIÓN CLASIFICADA

Description :

Cordial saludo,

Soy estudiante de la UNAD en la Especialización de Seguridad Informática y me encuentro desarrollando la monografía con el el título: ESTUDIO DE CIBERSEGURIDAD DE LOS ÚLTIMOS 5 AÑOS EN EL TEMA DE DELITOS INFORMÁTICOS DIRIGIDO A LOS NIÑOS, NIÑAS Y ADOLESCENTES EN EL DEPARTAMENTO DEL HUILA.
Por esta razón, solicito su colaboración para obtener información de los últimos 5 años en cuanto a los delitos informáticos que han afectado a los niños, niñas y adolescentes del Huila.

Estaré al tanto de su respuesta.

Gracias

Hamilton Andrade O.

Cel: 3143739574

Candidato al título de Especialista en Seguridad Informática de la UNAD

Gmail

Hamilton Andrade <ing.hamilton.andrade@gmail.com>

Derecho de Petición - Información y Orientación SIM No. 1762085251

2 mensajes

RespuestasPQRS@icbf.gov.co <RespuestasPQRS@icbf.gov.co>
Para: ing.hamilton.andrade@gmail.com
CC: correo@certificado.4-72.com.co

28 de agosto de 2020 a las 07:03

AVISO IMPORTANTE: Esta dirección de correo electrónico *RespuestasPQRS@icbf.gov.co* ***es de uso único y exclusivo de envío de notificaciones, todo mensaje que se reciba no será leído y automáticamente se eliminará de nuestros servidores.***

Señor ciudadano por favor no responda este correo, si desea comunicarse con ICBF debe hacerlo a través del correo atencionalciudadano@icbf.gov.co

Instituto Colombiano de Bienestar Familiar
Cecilia De la Fuente de Lleras
Dirección de Servicios y Atención

12500/SIM 1762085251

Bogotá D.C.,

Señor:

HAMILTON ANDRADE O.

Dirección física o electrónica: ing.hamilton.andrade@gmail.com

ASUNTO: Derecho de Petición - Información y Orientación SIM No. 1762085251 (Para consultas cite este número)

Respetado Señor,

En atención a la solicitud de fecha 21 de agosto de 2020, registrada con el número del asunto, mediante la cual indica "(…) Soy estudiante de la UNAD en la Especialización de Seguridad Informática y me encuentro desarrollando la monografía con el título: estudio de ciberseguridad de los últimos 5 años en el tema de delitos informáticos dirigido a los niños, niñas y adolescentes en el departamento del huila. por esta razón, solicito su colaboración para obtener información de los últimos 5 años en cuanto a los delitos informáticos que han afectado a los niños, niñas y adolescentes del Huila. (…)", con el presente nos permitimos informarle que:

En respuesta a su solicitud es conveniente indicarle que, con el fin de adelantar el oportuno y efectivo direccionamiento de su petición al área competente, le agradecemos remitirnos su solicitud acompañada de los siguientes documentos, los cuales se encuentran publicados en la página web del ICBF, en el siguiente link: https://www.icbf.gov.co/evaluacion/monitoreo-y-seguimiento-la-gestion

Allí podrá descargar: el formato para la presentación de los proyectos de investigación externos y diligenciarlo completamente, formato acta de compromiso de confidencialidad para particulares o instituciones, diligenciado, con firma y huella, y carta de aval de la institución de educación superior o entidad solicitante.

Si requiere información sobre programas, trámites y servicios del ICBF, consulte nuestro portafolio de servicios en la página web, ingresando al enlace: https://www.icbf.gov.co/portafolio-de-servicios-icbf. También podrá solicitar asesoría en Derecho en Familia, y/o presentar quejas, reclamos o sugerencias las 24 horas del día a través de nuestros canales de atención, Línea Gratuita Nacional: 01-8000-91-8080, correo electrónico: atencionalciudadano@icbf.gov.co y en la página web www.icbf.gov.co, opciones: Solicitudes PQRS, Chat ICBF, Videollamada o Llamada en Línea.

Recuerde que, si desea reportar un caso por presunta vulneración de derechos de los niños, niñas y adolescentes, lo podrá realizar a través de la Línea 141, de las líneas de WhatsApp: 320 239 16 86 – 320 239 13 20 - 320 865 54 50 o por cualquiera de nuestros canales de atención.

Cordialmente,

Dirección de Servicios y Atención

ICBF Sede de la Dirección General

Avenida carrera 68 No. 64 C– 75
atencionalciudadano@icbf.gov.co

INFORMACIÓN CLASIFICADA

ANEXO B

Respuesta de la gobernación del Huila y la secretaria de educación departamental sobre delitos informáticos de los últimos 5 años que haya afectado a los niños, niñas y adolescentes.

GOBERNACION DEL HUILA
Secretaría de Educación

Neiva, 18 de agosto de 2020

Señor
HAMILTON ANDRADE ORTIZ
Ing.hamilton.andrade@gmail.com
Neiva, Huila

Asunto: Respuesta a su solicitud

Respetado señor Andrade.

Una vez recibida su solicitud hemos leído atentamente el contenido de la misma y procedido a revisar en las diferentes dependencias de la Secretaría de Educación si existen denuncias, comunicados o algún tipo de registro relacionado con el tema de delitos informáticos, procedentes de las Instituciones Educativas, profesores o comunidad educativa en general, concluyendo que no hay registros en la Secretaría de Educación del Huila, con denuncias referentes al tema.

Por lo anterior, solo nos resta desearle éxitos en su investigación y sobre todo en los frutos positivos que pueda generar la misma en los niños, niñas y adolescentes de nuestro departamento.

Cordialmente,

Atentamente,

SONIA CRISTINA RAMIREZ PEREZ
PROFESIONAL UNIVERSITARIO
GESTION DE RECURSOS EDUCATIVOS

Anexos:

Proyectó: SONIA CRISTINA RAMIREZ PEREZ
Revisó: SONIA CRISTINA RAMIREZ PEREZ

Edificio Gobernación, Calle 8 Cra. 4 esquina, Neiva – Huila – Colombia. PBX: (57+8) 8671300
www.huila.gov.co -Twitter: @HuilaGob - Facebook: Gobernación del Huila

ANEXO C

Respuesta de la policía nacional del Huila sobre delitos informáticos de los últimos 5 años que haya afectado a los niños, niñas y adolescentes.

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN DE PROTECCIÓN Y SERVICIOS ESPECIALES
SECCIONAL HUILA

N° - S-2020- 047823 **-DEUIL - / - SEPRO-GINAD – 1.10**

Palermo, 23 JUL 2020

Señor
HAMILTON ANDRADE O.
Estudiante de Especialidad en Seguridad Informática de la UNA
Neiva-Huila

Asunto: Respuesta solicitud información para trabajo de grado UNAD

En atención a su petición radicada el día 20 de Julio de la presente anualidad mediante correo electrónico, me permito informarle que la Policía Nacional ha dispuesto a través de la página www.policia.gov.co un enlace de estadística delictiva, en el cual podrá encontrar información relacionada con las diferentes conductas que afectan la convivencia y seguridad ciudadana, dicha información se encuentra desagregada por variables de tiempo, modo y lugar, así mismo, para información estadística adicional puede elevar una solicitud al correo dijin.aicri-jef@policia.gov.co y su respuesta se dará en 10 días hábiles al recibo de la comunicación. De igual manera, para más información relacionada a años anteriores, puede remitirse al link https://www.policia.gov.co/revistacriminalidad, esta fuente de búsqueda pertenece al sistema de Información Estadística Delincuencia Contravencional y Operativa de la Policía Nacional SIEDCO, siendo estos los únicos canales que brindan información detallada.

De antemano agradecemos su atención a la presente y lo motivamos a continuar realizando procesos de investigación que contribuyen al mejoramiento de la convivencia y seguridad ciudadana.

Atentamente,

Intendente **CARLOS ALFONSO CUBILLOS ACOSTA**
Jefe Grupo de Protección a la Infancia y Adolescencia DEUIL

Elaborado Por: PT Andres Peña
Revisado Por: IT. Carlos Cubillos
Fecha de Elaboración: 23/07/2020
Ubicación: D:\Webmail\BACKUP\GINAD 2020

Kilómetro 2 Lote G12 Parque Industrial Palermo
Teléfono: 318-4795023
deuil.sepro@policia.gov.co
www.policia.gov.co

ANEXO D

Respuesta de la DIJIN CECIP-JEF sobre delitos informáticos de los últimos 5 años que haya afectado a los niños, niñas y adolescentes del Huila.

Gmail — Hamjlton Arrdrade <ing.hamilton.andrade@gmail.com>

Respuesta solicitud SOSPECHOSO Envío Formulario desde: Contáctenos EP174
1 mensaje

DIJIN CECIP-JEF <dijin.cecip-jef@policia.gov.co> — 21 de julio de 2020 a las 15:12
Responder a: DIJIN CECIP-JEF <dijin.cecip-jef@policia.gov.co>
Para: "ing.hamilton.andrade@gmail.com" <ing.hamilton.andrade@gmail.com>

Policía Nacional Dios y Patria

Buenas Tardes,

Respetuosamente me permito enviar a usted, respuesta a su solicitud así:

DESCRIPCIÓN CONDUCTA	01/01/2016 31/12/2016	01/01/2017 31/12/2017	01/01/2018 31/12/2018	01/01/2019 31/12/2019	01/01/2020 19/07/2020
ARTÍCULO 218. PORNOGRAFÍA CON MENORES	12	38	9	7	5
ARTÍCULO 219 A. UTILIZACIÓN O FACILITACIÓN DE MEDIOS DE COMUNICACIÓN PARA OFRECER SERVICIOS SEXUALES DE MENORES	7	8	4	1	2
TOTAL	19	46	13	8	7

Atentamente,

Jefatura **Centro Cibernético Policial**
Dirección de Investigación Criminal e INTERPOL
Carrera 62 No. 19-04 Puente Aranda
dijin.cecip-jef@policia.gov.co
Tel: 5159700 Ext 30428

Mensaje Importante

La información contenida en este mensaje, incluidos los archivos adjuntos al mismo, son para el uso exclusivo del destinatario y puede contener información que no es de carácter público, en caso de haber recibido este mensaje por error, comuníquese de forma inmediata con el emisor y proceda a su eliminación; recuerde que cualquier uso, difusión, distribución, copiado o divulgación de esta comunicación está estrictamente prohibido.

Para: DIJIN CECIP-JEF <dijin.cecip-jef@policia.gov.co>
Asunto: Fwd: SOSPECHOSO Envio Formulario desde: Contáctenos EP174

Cordial saludo,

Soy estudiante de la UNAD en la Especialización de Seguridad Informática y me encuentro desarrollando el trabajo de grado con el el título: ESTUDIO DE CIBERSEGURIDAD DE LOS ÚLTIMOS 5 AÑOS EN EL TEMA DE DELITOS INFORMÁTICOS DIRIGIDO A LOS NIÑOS, NIÑAS Y ADOLESCENTES EN EL DEPARTAMENTO DEL HUILA.
Por esta razón, solicito su colaboración para obtener información de los últimos 5 años en cuanto a los delitos informáticos que han afectado a los niños, niñas y adolescentes del Huila.

Estaré al tanto de su respuesta.

Gracias

Hamilton Andrade O.

Cel: 3143739574

Candidato al título de Especialista en Seguridad Informática de la UNAD

-------- Forwarded message --------
De: **DIJIN CAI-VIRTUAL** <caivirtual@policia.gov.co>
Date: lun., 20 de jul. de 2020 a la(s) 17:32
Subject: RE: SOSPECHOSO Envio Formulario desde: Contáctenos EP174
To: ing.hamilton.andrade@gmail.com <ing.hamilton.andrade@gmail.com>

Policía Nacional Dios y Patria, buen día,

Señor
Hamilton Andrade

Estimado usuario de acuerdo a su información emitida a esta unidad se le informa lo siguiente: Remita su requerimiento a nuestra jefatura con la finalidad de otorgarle el requerimiento.
Dijin.cecip-jef@policia.gov.co

Gracias por contactarnos, esperamos que la orientación suministrada haya sido de gran ayuda, si tiene dudas referentes a lo que debe realizar, puede contactarnos al número de teléfono en la ciudad de Bogotá 5159727 Ext. 30661, recuerde que estamos disponibles las 24 horas del día.

Atentamente,

-----Mensaje original-----
De: caivirtual@correo.policia.gov.co [mailto:caivirtual@correo.policia.gov.co]
Enviado el: lunes, 20 de julio de 2020 5:11 p. m.
Para: caivirtual@correo.policia.gov.co
Asunto: SOSPECHOSO Envio Formulario desde: Contáctenos

Enviado el Lunes, Julio 20, 2020 - 17:10 Enviado por usuario anónimo: 192.168.1.152 Los valores enviados son:

--Datos--
Nombres y Apellidos: Hamilton Andrade
Empresa: UNAD
E-mail: ing.hamilton.andrade@gmail.com
Móvil o Fijo: 3143739574
E-mail Centro: [ccp:email_centro]

Mensaje:
Cordial saludo,

Soy estudiante de la UNAD en la Especialización de Seguridad Informática y me encuentro desarrollando el trabajo de grado con el el título: ESTUDIO DE CIBERSEGURIDAD DE LOS ÚLTIMOS 5 AÑOS EN EL TEMA DE DELITOS INFORMÁTICOS DIRIGIDO A LOS NIÑOS, NIÑAS Y ADOLESCENTES EN EL DEPARTAMENTO DEL HUILA.
Por esta razón, solicito su colaboración para obtener información de los últimos 5 años en cuanto a los delitos informáticos que han afectado a los niños, niñas y adolescentes del Huila.

divulgacion de esta comunicacion esta estrictamente prohibido.

—Para evitar que su cuenta de correo personal institucional, sea víctima de suplantación, atacada por malware o phishing tenga presente no hacer click en links desconocidos, ya que a traves de estos se solicita datos personales como contraseña, número de cédula y correo electrónico entre otros. Por tal motivo deben abstenerse de suministrar información personal, institucional y bancaria.
–Se requiere difusión a la comunidad policial

CONFIDENCIALIDAD: Al recibir el acuse recibido por parte de esta dependencia se entendera como aceptado y se recepcionara como documento prueba de la entrega del usurario (Ley 527 del 18-08-1999).

—Para evitar que su cuenta de correo personal institucional, sea víctima de suplantación, atacada por malware o phishing tenga presente no hacer click en links desconocidos, ya que a traves de estos se solicita datos personales como contraseña, número de cédula y correo electrónico entre otros. Por tal motivo deben abstenerse de suministrar información personal, institucional y bancaria.
–Se requiere difusión a la comunidad policial

CONFIDENCIALIDAD: Al recibir el acuse recibido por parte de esta dependencia se entendera como aceptado y se recepcionara como documento prueba de la entrega del usurario (Ley 527 del 18-08-1999).

—Para evitar que su cuenta de correo personal institucional, sea víctima de suplantación, atacada por malware o phishing tenga presente no hacer click en links desconocidos, ya que a traves de estos se solicita datos personales como contraseña, número de cédula y correo electrónico entre otros. Por tal motivo deben abstenerse de suministrar información personal, institucional y bancaria.
–Se requiere difusión a la comunidad policial

CONFIDENCIALIDAD: Al recibir el acuse recibido por parte de esta dependencia se entendera como aceptado y se recepcionara como documento prueba de la entrega del usurario (Ley 527 del 18-08-1999).