CONSTRUCCIÓN DE UN DOCUMENTO DE RECOMENDACIONES DE CIBERSEGURIDAD PARA EL ENTORNO FAMILIAR

MAURICIO MORALES PINEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LÍBANO
2022

CONSTRUCCIÓN DE UN DOCUMENTO DE RECOMENDACIONES DE CIBERSEGURIDAD PARA EL ENTORNO FAMILIAR

MAURICIO MORALES PINEDA

Proyecto de Grado - Monografía presentada para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Ing. MIGUEL ANDRÉS AVILA
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LÍBANO
2022

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Líbano, 23 de diciembre de 2022

DEDICATORIA

“Con profundo amor, dedico este trabajo a mis padres Gonzalo y María Leidy, quienes desde mis primeros pasos orientaron mi camino hacia la búsqueda del conocimiento sin distinguir imposibilidades; de igual manera, a todas aquellas personas y familiares que a lo largo de mi vida han apostado y contribuido desde sus esquinas desinteresadamente en mi evolución académica y de aprendizaje constante”.

AGRADECIMIENTOS

“Agradezco profundamente a mis familiares, amigos y compañeros quienes con su apoyo desde diferentes frentes han hecho posible el desarrollo y culminación de este proceso académico. De igual manera, agradezco también al equipo docente de la Universidad Nacional Abierta y a Distancia UNAD quienes me han orientado pacientemente a lo largo del proceso con el cual es posible la entrega de este resultado académico”.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

ANDROID: sistema operativo *open source* soportado por Google y que, aunque inicialmente estaba presente solamente en *smartphones*, ahora puede encontrarse también en televisores denominados *Smart Tv*.

ANONYMOUS: grupo de *hacktivistas* conocidos púbicamente desde el año 2008.

ARPANET: se denominó de esta manera a una red militar de computadores y precursora de lo que hoy se conoce como internet.

ATAQUE INFORMÁTICO: intento por acceder a equipos informáticos o servidores mediante virus, *malware* u otro tipo de técnica.

***BLACK HACKERS*:** se conoce de esta manera a hackers que realizan sus ataques con malas intenciones.

***BLOCKCHAIN*:** conocida como cadena de bloques, es una tecnología mediante la cual se pueden hacer transacciones seguras con la garantía de que la información y de la cadena no se puede modificar dado que implicaría romper completamente la cadena.

***HARDWARE*:** se conoce de esta manera a la parte física de un equipo de cómputo.

***MALWARES*:** se determina de esta manera a cualquier tipo de *software* malicioso.

***RANSOMWARE*:** se conoce de esta manera a un tipo de *malware* que secuestra la información del equipo que lo hospeda, encriptándola y solicitando habitualmente una compensación económica a la víctima para poder recuperar la información.

RED: en informática es un conjunto de dispositivos interconectados entre sí para intercambiar información y compartir recursos.

***SOFTWARE*:** se conoce de esta manera a la parte lógica de un computador, como el sistema operativo o las aplicaciones.

RESUMEN

La presente monografía se basa en el análisis del estado del arte relacionado con las amenazas más comunes de ciberseguridad, aplicado al entorno familiar, en el que se enuncian algunos de los riesgos informáticos a los que se exponen sus integrantes en la realización de sus actividades cotidianas, tales como: Trabajo en casa, estudio, visualización de contenido multimedia, uso de redes sociales, equipos de cómputo, dispositivos *IoT*, entre otros. A partir de ello, se presentarán una serie de recomendaciones básicas de ciberseguridad con un principio de usabilidad didáctica en el que se plasmen conceptos, ejemplos, autodiagnósticos y rutas para identificar y solicitar ayuda ante posibles incidentes que se puedan presentar.

Esta construcción se realiza mediante un enfoque cualitativo, a partir de la identificación y análisis de modelos numéricos representados en estudios del sector, encuestas, entrevistas y opiniones de líderes del área de la tecnología, midiendo los fenómenos a partir de estadísticas encontradas con el propósito de determinar si un análisis sobre ciberseguridad familiar puede contribuir a la reducción de los delitos cibernéticos en Colombia.

Palabras clave: Ciberseguridad, ciberdelitos, riesgos informáticos, entorno familiar, análisis de ciberseguridad.

ABSTRACT

This monograph is based on the analysis of the state of the art related to the most common cybersecurity threats, applied to the family environment, in which some of the computer risks to which its members are exposed in the performance of their daily activities are stated, such as: Work at home, study, visualization of multimedia content, use of social networks, computer equipment, IoT devices, among others. From this, a basic cybersecurity recomendations will be designed with a principle of didactic usability in which concepts, examples, self-diagnosis and routes are reflected to identify and request help in the event of possible incidents that may arise.

This construction is carried out through a qualitative approach, based on the identification and analysis of numerical models represented in studies of the sector, surveys, interviews and opinions of leaders in the area of technology, measuring the phenomena from statistics found with the purpose of determine if a guide on family cybersecurity can contribute to the reduction of cybercrime in Colombia.

Keywords: Cybersecurity, cybercrimes, computer risks, family environment, cybersecurity analysis.

INTRODUCCIÓN

El contenido del presente documento se enfoca en los riesgos de ciberseguridad que rodean el entorno familiar, realizando un recorrido a lo largo de literatura relacionada con afectaciones en grupos poblacionales como menores, adultos, adultos mayores y segmentaciones por género. En este análisis se aborda especialmente las vulnerabilidades a las que se encuentran expuestos los menores de edad a partir de su contexto social, la penetración tecnológica en el hogar y fortalecimiento progresivo del criterio individual.

De igual manera, se realiza una identificación de las principales modalidades de ciberdelitos, por medio del análisis de datos relacionados con denuncias reales efectuadas ante autoridades competentes y testimonios individuales entregados por víctimas de estos delitos, en los que se realiza un especial énfasis en las consecuencias relacionadas con la salud mental, el estatus familiar y posteriores dificultades económicas.

A partir de ello, se emiten una serie de recomendaciones de ciberseguridad orientadas al público en general, en donde se abordan conceptos como medio para la introducción a cada tema, riesgos asociados a los que se encuentra expuesto un individuo, ejemplos y técnicas de uso común y/o herramientas que le permitirán al lector fortalecer sus hábitos y su sentido común como mecanismo de defensa ante ataques cibernéticos de los que podría potencialmente ser víctima por diversos canales.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En años recientes la penetración de la conectividad a internet en Colombia ha presentado un crecimiento continuo. De acuerdo con el último Boletín Trimestral de las TIC (Tecnologías de la Información y la Comunicación) del MinTIC Colombia (Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia), el III trimestre 2018 cerró con 6,68 millones de accesos fijos a internet, creció luego a 7.01 al cierre del III trimestre de 2019 y llegó hasta los 7.67 millones en el III trimestre de 2020, denotando para 2020 un crecimiento del doble de lo esperado[1].

Igualmente, el DANE (Departamento Administrativo Nacional de Estadísticas de Colombia) confirma en su último corte (2018) relacionado con la Encuesta Nacional de Vida (ENV) que un 44.9% de la población colombiana mayor de 5 años utilizó un computador y que un 64.1% utilizaron internet por cualquier medio[2]. Aunque aún no se cuenta con las cifras consolidadas para los años 2019 y 2020, si se compara con los datos del Boletín Trimestral de las TIC, sugiere que presentarán un incremento considerable, derivado, al parecer por el aumento en los usuarios conectados a la red ocasionado por la situación de confinamiento nacional durante 2020[3].

Por otra parte, también los delitos cibernéticos crecieron considerablemente. Tan solo en 2020 se registró un aumento del 84% en el que se incrementaron las estafas vía *WhatsApp* por medio de suplantación de identidad, suplantación de sitios web, secuestro de información y pornografía infantil a través de la red[4]. Igualmente, el CCIT (Cámara Colombiana de Informática y Telecomunicaciones) en su informe *"Tendencias del Cibercrimen Colombia 2019-2020"* se refiere a futuros ataques que estarán centrados en inteligencia artificial, *botnets* y masificación de perfiles falsos en redes sociales para

[1] COLOMBIA. MINTIC, Boletín Trimestral de Las TIC Tercer Trimestre De 2020. [en línea]. Estadísticas. 2021. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://colombiatic.mintic.gov.co/679/articles-161478_presentacion_cifras.pdf>

[2] COLOMBIA. DANE, Indicadores Básicos de TIC Hogares. [en línea]. Tic. 2019. [Citado en 20 de Marco de 2021]. Disponible en internet: <https://www.dane.gov.co/index.php/estadisticas-por-tema/tecnologia-e-innovacion/tecnologias-de-la-informacion-y-las-comunicaciones-tic/indicadores-basicos-de-tic-en-hogares#regional>

[3] COLOMBIA. MINTIC, Ministra de TIC Hace Balance De La Conectividad Durante La Pandemia. [en línea]. Mintic En Los Medios. 2020. [Citado en 15 de Marzo de 2021]. Disponible en internet: <https://webcache.googleusercontent.com/search?q=cache:BYeClyJvTRUJ:https://www.mintic.gov.co/portal/604/w3-article-145946.html>

[4] EL ESPECTADOR, En 2020 Se Profesionalizaron los Delitos en la Web Y Crecieron En Un 84%. [en línea]. Judicial. 2020. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.elespectador.com/noticias/judicial/los-ciberdelitos-aumentaron-un-84-durante-2020-policia/>

difusión de malware[5].

Para expertos como ESET, casa desarrolladora del popular software antivirus NOD32, es fundamental la formación sobre seguridad informática y debería incluirse en la educación formal[6]. Esta convergencia entre la problemática creciente por delitos informáticos y la necesidad de brindar información a las familias a través de material de consulta confiable y en lenguaje claro, abre la brecha que denota la necesidad que tiene la sociedad colombiana de contar con material de aprendizaje que le permita entender y sobre todo saber cómo afrontar las amenazas cibernéticas.

1.2 FORMULACIÓN DEL PROBLEMA

Teniendo en cuenta lo anteriormente expuesto, surge la siguiente pregunta problema:

¿Qué recomendaciones de ciberseguridad debería contener un documento para el entorno familiar, con el fin de generar conciencia en la sociedad acerca de las amenazas y riesgos presentes en el ciberespacio, así como, las medidas de protección para la prevención de incidentes cibernéticos?

[5] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACION CCIT, Tendencias Del Cibercrimen En Colombia 2019-2020. [en línea]. Estudios. 2019. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/>

[6] HARÁN, Juan Manuel. Educación en Seguridad Informática: ¿Debería Incluirse en la Educación Formal?. [en línea]. We Live Security. 2019. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.welivesecurity.com/la-es/2019/11/18/educacion-seguridad-informatica-deberia-incluirse-educacion-formal/>

2 JUSTIFICACIÓN

Los seres humanos hacen uso de las tecnologías de la información para socializar, estudiar, trabajar, ocio, comunicarse con sus semejantes y demás[7]. Con la llegada del confinamiento global por COVID-19, este uso se incrementó dado que las TIC se convirtieron en el medio apto para estudiar, trabajar, comunicarse, informarse, entretenerse[8], acelerando la penetración de estas tecnologías y consolidándose, así como una transformación digital sin precedentes para la humanidad[9].

De la mano con ello, también aumentaron los riesgos de ciberseguridad[10], en donde las personas de todas las edades del núcleo familiar realizan sus actividades en medio de riesgos latentes como suplantación de identidad, fraudes*, sexting, grooming*, ciberacoso, *vishing*, sin ser conscientes de la cantidad de datos que se comparten y como podrían ser contraproducentes para su seguridad[11].

Para algunos sectores, la ciberseguridad genera un impacto social directo en las sociedades y debe ser considerada como un bien común en el que interactúan todos los actores vinculados en la transformación digital[12] dado que fortalece la confianza y disminuye la posibilidad de posibles ciberdelitos.

Esta monografía tiene como propósito la realización de un análisis básico de la ciberseguridad familiar en donde se abordarán conceptos, tipos de riesgos y ataques, recomendaciones, control parental, rutas para solicitar ayuda ante incidencias, y autodiagnósticos que permitan concienciar a la sociedad sobre la importancia de adoptar hábitos para fortalecer la seguridad cibernética a partir de la familia como base.

---

[7] EN TIC CONFÍO, ¿Qué Son y Para Qué Sirven Las TIC ?. [en línea]. Pedagoría. 2015. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.enticconfio.gov.co/que-son-y-para-que-sirven-las-tic->

[8] REVISTA SEMANA, ¿Colapsará el Internet en Colombia por la Avalancha del Teletrabajo? . [en línea]. Tecnología. 2020. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.semana.com/economia/articulo/capacidad-de-conexion-a-internet-de-colombia-para-facilitar-el-teletrabajo/657315/>

[9] PNUD, Cómo La Covid-19 Ha Acelerado la Transformación Digital. [en línea]. Blog. 2020. [Citado en 10 de Marzo de 2021]. Disponible en internet: <https://www.undp.org/content/undp/es/home/blog/2020/how-covid-19-has-sped-up-digital-transformation.html>

[10] MÍNGUEZ, Cristina. Ciberseguridad, Más Prioritaria Que Nunca en Tiempos ee Pandemia. [en línea]. Tic. 2020. [Citado en 20 de Marzo de 2021]. Disponible en internet: <Ciberseguridad, más prioritaria que nunca en tiempos de pandemia>

[11] EL TIEMPO, Los Riesgos de Exponer Datos Personales en Internet. [en línea]. Tecnósfera. 2020. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/riesgos-de-exponer-datos-personales-en-internet-557397>

[12] DE PEDRO, Sandra. La Ciberseguridad Como Responsabilidad Social. [en línea]. Blog. 2019. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://gaptain.com/blog/la-ciberseguridad-como-responsabilidad-social/>

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Construir un documento de recomendaciones de ciberseguridad para el entorno familiar, que permita la generación de conciencia acerca de las amenazas y vulnerabilidades presentes en el ciberespacio, así como, las medidas de protección para la prevención de incidentes cibernéticos.

3.2 OBJETIVOS ESPECÍFICOS

Recopilar información acerca del estado del arte en materia de ciberseguridad para la identificación de las amenazas y riesgos actuales, conceptos, herramientas y recomendaciones de seguridad para el entorno familiar.

Establecer riesgos de ciberseguridad a las que se encuentra expuesta una persona, así como, la afectación para su entorno familiar.

Analizar las principales modalidades de ciberdelitos a través de casos reales y sus repercusiones en el entorno familiar.

Proponer recomendaciones de seguridad, buenas prácticas de higiene cibernética y herramientas para la prevención de incidentes cibernéticos en el entorno familiar.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La sociedad colombiana y las empresas cada día viven un proceso de transformación digital en el que internet se convierte en el nuevo medio de transporte de información. De acuerdo con Víctor Díaz, country mánager de Lenovo Colombia, las empresas colombianas están adoptando más tecnologías en busca de la productividad, obligándose a realizar un cambio cultural hacia la transformación digital[13]. De acuerdo con la Encuesta de Transformación Digital de la ANDI (Asociación Nacional de Industriales de Colombia), con corte a 2018 el 88.2% de las empresas conocen que es la llamada "Cuarta Revolución Industrial"[14].

Esta transformación tiene sus ventajas en las que participan todos los sectores de la sociedad: Para organizaciones como Bancolombia, hay menos filas, los trámites son más sencillos "a tan solo un clic" y se puede comprar y vender a través de este medio[15]. Para otros autores, en cuanto a la comunicación familiar, se puede enviar mensajes al instante sin importar la distancia, acortando esa percepción de lejanía[16] y se percibe esa sensación de que ahora todo está más conectado con todo.

Estas ventajas han llevado a la sociedad colombiana a convertirse en el 4 país del mundo en donde las personas se dedican más tiempo a navegar en internet, con un promedio de 9 horas diarias por persona[17] (cifra emitida por el *Global Web Index*, encargado de emitir los rankings mundiales de tiempo de uso de internet).

De acuerdo con la Universidad de Palermo, la conectividad a la red ofrece innumerables oportunidades competitivas para empresas y gobiernos, tanto para comercializar como para desarrollar sus operaciones[18]. Por su parte, en cuanto a las familias, plataformas

[13] EL TIEMPO, Panorama de Colombia Frente a la Transformación Digital. [en línea]. Transformación Digital. 2020. [Citado en 15 de Marzo de 2021]. Disponible en internet: <https://www.eltiempo.com/mas-contenido/panorama-de-colombia-frente-a-la-transformacion-digital-550807>

[14] ANDI, ANDI Presentó Los Resultados de la Encuesta de Transformación Digital . [en línea]. Noticias. 2019. [Citado en 15 de Marzo de 2021]. Disponible en internet: <http://www.andi.com.co/Home/Noticia/15609-andi-presento-los-resultados-de-la-encu>

[15] BANCOLOMBIA, Guía Para Entender La Transformación Digital En Colombia. [en línea]. Reset. 2020. [Citado en 15 de Marzo de 2021]. Disponible en internet: <https://resetmarketingdigital.com/guia-transformacion-digital-en-colombia>

[16] ÁLVAREZ TABARES, Omar Julián. y RODRÍGUEZ GUERRA, Elquis. El Uso De La Internet Y La Influencia En La Comunicación Familiar. Diciembre, 2012. Vol. 7. No. 7., p.11-21.

[17] GLOBAL WEB INDEX, 5 Things to Know about Internet Users in Colombia. [en línea]. Transformación Digital. 2018. [Citado en 15 de Marzo de 2021]. Disponible en internet: <https://blog.globalwebindex.com/trends/internet-users-colombia/>

[18] UNIVERSIDAD DE PALERMO, Internet, ¿Oportunidad O Amenaza Para Los Negocios?. [en línea]. Escritos En La Facultad 97. 2014. [Citado en 15 de Marzo de 2021]. Disponible en internet:

como *Qustodio* (plataforma líder en control parental), señala importantes ventajas del internet para las familias como el uso con fines académicos, de ocio, oportunidades para reducir el papel, aceleración de aprendizaje y favorecimiento de la comunicación[19]. Este tipo de tendencias permiten inferir que tanto las organizaciones como las personas están cada vez más conectadas a la red, lo cual se convierte en una oportunidad excelente para los ciberdelincuentes y es que de acuerdo con la revista Semana, "el cibercrimen es un delito más rentable que el narcotráfico"[20], por lo cual es fácil inferir que los delincuentes están dispuestos a aprovechar ese "mercado".

En este contexto, es factible que se presenten ataques cibernéticos en todos los niveles de la sociedad y es que, de acuerdo con Avast, desarrolladora del conocido antivirus Avast, existen amenazas como la ingeniería social, en la que un usuario puede entregar sus accesos a un estafador, dado que resulta más fácil engañar a alguien para que revele una contraseña que lograr vulnerarla por otros medios[21].

Conscientes de ello, entidades como el Gobierno de Colombia invierten frecuentemente importantes cantidades de recursos para desarrollar programas como En TIC Confío con el que buscan sensibilizar a la sociedad sobre el uso seguro de las TIC[22], con metas ambiciosas como la más reciente para 2021 en la que buscó llegar a 1.8 millones de personas[23], correspondiente al 3,52% de la población colombiana, si se tiene en cuenta que de acuerdo con el DANE la proyección de habitantes en Colombia para 2021 fue de 51.049.498[24].

De acuerdo con Emma W., líder del equipo de seguridad centrado en las personas en el Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC), percibir a la gente como el factor más débil en la ciberseguridad es injusto dado siempre se ha tratado de

<http://fido.palermo.edu/servicios_dyc/publicacionesdc/vista/detalle_articulo.php?id_libro=501&id_articulo=10417>

[19] DIARIO ABC, Internet No Es El Enemigo: 7 Beneficios Del Uso De Las Nuevas Tecnologías Que Evitamos Admitir. [en línea]. Educación. 2020. [Citado en 15 de Marzo de 2021]. Disponible en internet: <https://www.abc.es/familia/educacion/abci-internet-no-enemigo-7-beneficios-nuevas-tecnologias-evitamos-admitir-202001301416_noticia.html>

[20] REVISTA SEMANA, El Cibercrimen Es Un Delito Más Rentable Que El Narcotráfico . [en línea]. Cibercrimen. 2015. [Citado en 15 de Marzo de 2021]. Disponible en internet: <https://www.semana.com/internacional/articulo/principales-cifras-del-cibercrimen-mundo-colombia/213988/>

[21] AVAST, Ingeniería Social . [en línea]. Otras Amenazas. 2020. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.avast.com/es-es/c-social-engineering>

[22] COLOMBIA. MINTIC, En TIC Confío + . [en línea]. Otras Amenazas. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.enticconfio.gov.co/quienes-somos>

[23] COLOMBIA. MINTIC, Min Tic Capacitará A 1,8 Millones De Colombianos En Habilidades Digitales. [en línea]. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/161930:Min-TIC-capacitara-a-1-8-millones-de-colombianos-en-habilidades-digitales>

[24] COLOMBIA. DANE, Proyecciones De Población. [en línea]. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/proyecciones-de-poblacion>

trasladar la responsabilidad a los mismos sin tener en cuenta el contexto y las motivaciones[25].

Al profundizar sobre el alcance de los problemas de ciberseguridad, se encuentra que no solamente afecta a empresas y gobiernos, sino que las personas comunes también están expuestas a numerosos riesgos, en medio de una pensamiento recurrente centrado en el *"yo no tengo nada que esconder",* el cual es calificado por el portal *datosprotegidos.org* como la falacia de la privacidad[26], dado que la información de cada individuo, como el lugar donde guarda su dinero, sus hábitos, sus allegados y sus pensamientos y actividades más íntimas propias de cada personalidad deben ser protegidas.

En cuanto a la problemática de la ciberseguridad, se encuentran entonces muchos factores en común relacionados los riesgos para una empresa o para una familia. La diferencia es que la familia desconoce en mayor medida el riesgo al que se exponen sus integrantes y por ello le resta importancia ya que no considera que pueda ser objeto de ataque y a su vez extiende ese hábito de despreocupación a sus demás actividades externas al hogar como el trabajo o su comportamiento social. De acuerdo con autores como Javier Jiménez de *RedesZone*, la cantidad de datos expuestos en redes sociales son alarmantes, representando un agujero enorme para la privacidad dado que cualquier atacante puede obtenerlos para planear estafas u otros delitos[27].

4.2 MARCO CONCEPTUAL

El presente marco conceptual pretende esclarecer una serie de términos relacionados con ciberseguridad.

Internet es una red de redes y dispositivos interconectados con alcance global, en donde es posible encontrar todo tipo de información sobre todos los temas como cultura, arte, música, audiovisual, literatura, política, y es posible además realizar transacciones como trámites, servicios y actividades de esparcimiento[28].

---

[25] TECH TARGET, La Gente Puede Ser El Eslabón Más Fuerte En La Ciberseguridad, Dice Ncsc. [en línea]. 2017. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://searchdatacenter.techtarget.com/es/cronica/La-gente-puede-ser-el-eslabon-mas-fuerte-en-la-ciberseguridad-dice-NCSC>

[26] DATOS PROTEGIDOS, No Tengo Nada Que Ocultar: La Falacia De La Privacidad. [en línea]. 2015. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://datosprotegidos.org/no-tengo-nada-que-ocultar-la-falacia-de-la-privacidad/>

[27] JIMÉNEZ, Javier. ¿expones Demasiados Datos En Redes Sociales? . [en línea]. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.redeszone.net/noticias/seguridad/datos-expuestos-usuarios-redes-sociales/>

[28] COLOMBIA. MINTIC, Internet, ¿Qué Es? ¿Para Qué Sirve?. [en línea]. 2020. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.enticconfio.gov.co/internet-que-es-para-que-sirve>

La conectividad, según su contexto se refiere a la capacidad de un equipo de cómputo para comunicarse con otro en distintos puntos geográficos[29].

Ciberseguridad es la práctica de defender los datos, servidores, computadoras, dispositivos electrónicos y móviles de los ataques maliciosos. De acuerdo con su contexto se puede dividir en categorías como seguridad de la red, seguridad de aplicaciones, seguridad operativa, seguridad de la información, y depende considerablemente de la capacidad de recuperación ante desastres y de la capacitación de los usuarios finales, el cual se convierte en el factor más impredecible dada la naturaleza del comportamiento humano[30].

Un riesgo informático es cualquier tipo de vulnerabilidad en un sistema que pueda terminar en pérdidas de datos, infiltraciones de usuarios no autorizados, caídas de un sistema o rupturas de la integridad[31].

Un delito cibernético es aquel en el que delincuentes utilizan medios informáticos para cometer delitos como suplantación de sitios web, estafas, implantación de virus, piratería, violación de derechos de autor, entre otros[32].

Un computador es una máquina electrónica diseñada para facilitarle la vida al ser humano y que puede realizar tareas diversas como de ofimática, navegación en internet, tratamiento de datos, ocio, trabajo y demás[33].

Las TIC son el conjunto de herramientas, redes, programas informáticos, equipos, recursos, medios y aplicaciones que permiten el procesamiento, compilación, transmisión y almacenamiento de información como datos, voz, imágenes, texto y video[34].

La transformación digital se define como la integración de la tecnología digital en todas las áreas de una organización, modificando su operación en relación a la aplicación de capacidades digitales a activos, productos y procesos para mejorar su valor para el

[29] HOSTDIME, Que Es La Conectividad , Origen Del Término, Lo Que Significa, Definición; Ejemplos. [en línea]. 2017. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://blog.hostdime.com.co/que-es-conectividad-orige-termino-significa-definicion-ejemplos/>

[30] KASPERSKY, ¿Qué Es La Ciberseguridad?. [en línea]. 2020. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>

[31] HACKNOID, ¿qué Son Los Riesgos En Informática?. [en línea]. 2018. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://hacknoid.com/hacknoid/importancia-de-la-gestion-de-riesgos-informaticos/>

[32] POLICÍA NACIONAL DE COLOMBIA, Denunciar Delitos Informáticos. [en línea]. Virtual. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.policia.gov.co/denuncia-virtual/delitos-informaticos>

[33] CCF GLOBAL, ¿Qué Es Un Computador?. [en línea]. 2020. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://edu.gcfglobal.org/es/informatica-basica/que-es-un-computador/1/>

[34] COLOMBIA. MINTIC, Tecnologías De La Información y Las Comunicaciones (TIC). [en línea]. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.mintic.gov.co/portal/inicio/5755:Tecnolog-as-de-la-Informaci-n-y-las-Comunicaciones-TIC>

cliente, incrementar su eficiencia, gestionar riesgos y descubrir nuevas maneras de optimizar procesos, estrategias y generar ingresos[35].

4.3 MARCO HISTÓRICO

Los delitos informáticos a través de las TIC surgen con el nacimiento mismo de este tipo de tecnologías, en la época del telégrafo por ejemplo, eran conocidos casos en los que delincuentes lograban intervenir las líneas físicas de la red con el propósito de conocer el contenido de los mensajes privados enviados por este medio[36], en su momento la forma de resolver el problema fue comenzar a utilizar un sistema simple para cifrar los mensajes basado en referencias como por ejemplo, en vez de decir “nos vemos en la torre del reloj” se podría decir “nos vemos en el lugar en donde te caíste la segunda vez que hablamos”.

Posteriormente, con el nacimiento del teléfono también lograron presentarse interceptaciones similares al caso del telégrafo, sin embargo la novedad de poderse comunicar en tiempo real abrió la brecha para que delincuentes comenzaran a realizar estafas con engaños como anuncios de premios, inversiones fraudulentas, accesos a datos de tarjetas de créditos y un sinfín de intentos de estafas de toda índole que se extienden hasta la actualidad y que se basan en la ingeniería social para hacer que la víctima haga lo que el atacante desea[37]. Estos perpetradores han sido denominados como “*phreakers*”.

Luego del teléfono la humanidad inicia su revolución a través de la computación, que cambió la forma en la que se organizaba la información y que abrió nuevamente una brecha para nuevos delitos informáticos. El primer indicio antes de la red de redes fue el conocido caso de un cajero de banco que en los años 70 en New York logró desviar 2 millones de dólares por medio de una computadora[38].

Para los años 80, se presenta un caso de una condena por un delito cibernético real en el que Ian Murphy conocido como “Capitán Zap”, *hackeo* la computadora de otra persona

[35] POWER DATA, ¿Qué Es La Transformación Digital?. [en línea]. 2019. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.powerdata.es/transformacion-digital>

[36] KASPERSKY DAILY, El Telégrafo, El Abuelo De Internet: El Principio De La Era De La Información. [en línea]. Cifrado. 2015. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.kaspersky.es/blog/telegraph-grandpa-of-internet/6273/>

[37] COMISION FEDERAL DE COMERCIO DE LOS ESTADOS UNIDOS, Estafas Por Teléfono. [en línea]. Estafas. 2019. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.consumidor.ftc.gov/articulos/s0076-estafas-por-telefono>

[38] HERJAVEC, Robert. Cybersecurity CEO: The History Of Cybercrime, From 1834 To Present. [en línea]. Estafas. 2019. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.herjavecgroup.com/history-of-cybercrime/>

para buscar, copiar y manipular datos con el fin de cambiar las políticas de llamadas de una compañía telefónica para poder realizar llamadas telefónicas gratuitas[39].

Durante esta misma década se conoce el caso de Rich Skrenta, un niño de 15 años que programa el primer virus informático conocido que tuvo una expansión real denominado *Elk Cloner*[40]*.* Algunos años después nace la ley de fraude y abuso informático en estados y unidos y casi a la par se presenta el caso de Robert T. Morris jr., un estudiante que lanzó un gusano con capacidades auto-replicantes en la *ARPANET* (precursora de la internet actual), perdiendo el control de esta e infectando alrededor de 600.000 computadoras[41].

Finalizando esta misma década se reporta el primer caso a gran escala de *ransomware*, en el que las víctimas descargaban un formulario de encuesta relacionado con el *SIDA* por medio de un *disquette* y una vez descargado, secuestraba los datos almacenados en la computadora y exigía 500 dólares como pago para poderlos recuperar[42].

Durante los años 90, con el lanzamiento de la *World Wide Web* los *black hackers* se mueven hacia este lugar y comienzan a conocerse casos de ataques cibernéticos hacia objetivos como la *NASA*, el programa nuclear de Corea y otras organizaciones. Estos ataques comienzan a ser documentados como ejecutados por personas desde computadores comunes utilizando programas encontrados en línea.

Para mediados de esta década comienzan a conocerse los denominados *macro-virus*, los cuales son virus integrados en aplicaciones que se ejecutan cuando se abre determinada aplicación, convirtiéndose en una amenaza de fácil transmisión y que continúa propagándose de esa misma manera hasta la actualidad[43]. Luego el FBI da a conocer que más del 80% de empresas estadounidenses habrían sido hackeadas sin saberlo y paralelamente nace el virus Melissa AD WM97, el cual se apodera de las

[39] OBSERVATORIO GUATEMALTECO DE DELITOS INFORMÁTICOS, Historia Del Cibercrimen. [en línea]. 2017. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://ogdi.org/historia-del-cibercrimen>

[40] ESET, Elk Cloner: La Cápsula Del Tiempo. [en línea]. 2009. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.welivesecurity.com/la-es/2009/08/11/elk-cloner-capsula-tiempo/>

[41] MÁRQUEZ RIVERA, Jesús Manuel . El Gusano De Morris. [en línea]. 2011. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://blog.utp.edu.co/alejandropinto/files/2011/04/El-Gusano-de-Morris-El-D%c3%ada-Que-Internet-Se-Detuvo.pdf>

[42] SÁNCHEZ, Cristina . Así Fue El Primer 'ransomware' Del Mundo: Disquetes Con Sida Que Secuestraban Tu Pc. [en línea]. 2017. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.elconfidencial.com/tecnologia/2017-05-27/primer-ransomware-diskete-panama_1389351/>

[43] ESET, ¿Qué Es Un Macro Virus Y Cómo Funciona?. [en línea]. 2014. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.welivesecurity.com/la-es/2014/06/13/que-es-macro-virus-como-funciona/>

cuentas de correo electrónico cuando el usuario abre un archivo contaminado y envía automáticamente un mensaje a su libreta de contactos replicando el virus[44].

Ya en la primera década de los 2000 comienzan a conocerse casos de robos masivos de números de tarjetas de crédito y de ataques de Denegación de Servicio (DDoS) contra plataformas populares en ese momento como Yahoo y AOL[45], y se presenta un incremento considerable en casos de hackeo doméstico como robo de datos, *ransomware* y máquinas infectadas, casos específicos en los que se pudo documentar que 134 millones de tarjetas de crédito habrían quedado expuestas mediante un ataque de *SQL Injection*[46]. A finales de esta década el mundo conoce al grupo de *hackers* denominado *Anonymous,* el cual se atribuye un ataque de *DDoS* como parte de acciones activistas políticas.

En la nueva década de los 2010, se conocen virus como *Stuxnet* que es considerado la primera arma digital del mundo, utilizada para espionaje industrial y que en su momento ordenó autodestruirse a plantas de energía nuclear en Irán[47]. Posteriormente durante esta década los ataques y casos de robo de información de clientes de organizaciones se multiplica, generando cuestionamientos sobre toda la información que los usuarios comparten en la red.

Igualmente, durante esta década comienzan a identificarse amenazas cada vez más sofisticadas con casos de *ransomware* que secuestraba equipos de cómputo domésticos con malwares como *Reveton*, *CryptoLocker* y *CriptoWall*. De la misma manera, comienzan a presentarse amenazas de este tipo orientadas a smartphones *Android* con *malwares* como *LockerPin*, quienes exigían un pago de $500 dólares para poder recuperar el acceso al dispositivo[48].

A finales de la década se conocen casos como el famoso *WannaCry*, que se convierte en el primer *ransomware* conocido capaz de replicarse a si mismo como un gusano y que

---

[44] PANDA SECURITY, ¿Qué Es Un Macro Virus Y Cómo Funciona?. [en línea]. 2017. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.pandasecurity.com/es/mediacenter/malware/virus-melissa/>

[45] ESET, Mafiaboy: 20 Años De Uno De Los Primeros Ataques Documentados Del Tipo DOS. [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.welivesecurity.com/la-es/2020/02/10/mafiaboy-20-anos-primeros-ataques-denegacion-servicio/>

[46] RINALDI, Paola. ¿de Dónde Viene El Delito Cibernético? Origen Y Evolución Del Delito Cibernético. [en línea]. 2017. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/>

[47] BBC NEWS, El Virus Que Tomó Control De Mil Máquinas Y Les Ordenó Autodestruirse. [en línea]. 2015. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet>

[48] VANDERBURG, Eric. The Evolution of a Cybercrime: A Timeline of Ransomware Advances. [en línea]. 2017. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.carbonite.com/blog/article/2017/08/the-evolution-of-a-cybercrime-a-timeline-of-ransomware-advances>

en cuestión de días se expandió por más de 150 países exigiendo a cada usuario infectado pagar la suma de $300 dólares para recuperar el acceso a su información[49].

4.4 ESTADO ACTUAL

En la actualidad, existen varios tipos de delitos informáticos entre los que se destacan las estafas informáticas, por medio de las cuales el atacante engaña a la víctima con promesas falsas a cambio de dinero o por medio de ingeniería social principalmente vía telefónica o *email* para obtener datos de cuentas bancarias o similares. Esta práctica conocida como *phishing* se enfoca en atacar mediante estos engaños directamente a la víctima. Igualmente existe dentro de este grupo el denominado *carding,* el cual es caracterizado por la realización fraudulenta de copias de datos de tarjetas de crédito para realizar adquisiciones con ellas[50].

Por otra parte, otro de los grandes grupos de ataques son los delitos informáticos de daños, cuyo caso más conocido es el particular *ransomware WannaCry*, el cual se empeña en borrar, dañar, deteriorar, modificar o hacer inaccesibles los datos informáticos de la víctima y cobrando un monto de dinero determinado para que esta pueda recuperar el acceso a sus equipos o información.

También existen en la actualidad los ciberdelitos contra la intimidad, cuyos casos más reconocidos es cuando alguna persona instala algún tipo de software espía en los dispositivos de otra, permitiéndole acceder a la información confidencial y privada de su víctima sin su consentimiento.

Al cierre de 2020, en Colombia, la Asociación Colombiana de Ingenieros de Sistemas ACIS, estima que se incrementaron en un 600% los ciberdelitos en medio de la crisis de salud y confinamiento nacional por Covid-19[51].

4.5 MARCO TECNOLÓGICO

[49] OBSERVATORIO GUATEMALTECO DE DELITOS INFORMÁTICOS, Historia Del Cibercrimen. [en línea]. 2017. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://ogdi.org/historia-del-cibercrimen>

[50] ESPARÍS FIGUEIRA, Martín. Ciberdelincuencia: Los Delitos Informáticos Más Comunes. [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.sistemius.com/ciberdelincuencia-4-tipos-de-delitos-informaticos/>

[51] ACIS, Un 600% Ha Aumentado Los Ciberdelitos En Pandemia, ¡asegúrese Para Iniciar El 2021! . [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://acis.org.co/portal/content/noticiasdelsector/un-600-ha-aumentado-los-ciberdelitos-en-pandemia-%C2%A1aseg%C3%BArese-para-iniciar-el-2021>

El crecimiento en el uso de dispositivos conectados a internet y la exposición de información y los riesgos a los que se enfrentan los usuarios de los mismos se realiza por medio de una serie de tecnologías que es conveniente relacionar para el desarrollo del proyecto.

Un computador es una máquina diseñada por los seres humanos con el propósito de facilitar la vida y automatizar procesos. Estas máquinas se componen en *software* y *hardware* y también se les conoce en algunos países como "ordenadores"[52]. Igualmente, existe internet, que es denominada una red de redes con alcance global, por medio de la cual se puede transportar todo tipo de información digital y sobre la que funcionan diversos servicios como correo electrónico, redes sociales, plataformas gubernamentales, servicios financieros digitales, entretenimiento, *e-commerce*- entre otros. Funciona a través de un protocolo llamado TCP/IP lo que permite la conexión y transporte de paquetes de datos entre dispositivos como ordenadores, *smartphones, smart tv*, servidores, internet de las cosas (IoT), entre otros[53].

Un dispositivo móvil, en tecnología es un aparato con características como las de un computador, pero menores en tamaño y funcionales bajo la premisa de que deben poderse transportar fácilmente y ser utilizados durante su transporte[54].

Un teléfono es un dispositivo que permite transmitir sonidos a distancia haciendo uso de señales eléctricas. Sus primeras versiones utilizaban circuitos de conversación para el transporte de la voz y circuitos de marcación para la vinculación de las llamadas. Actualmente existen teléfonos móviles que hacen uso de señales GSM, 3G, 4G y 5G y otros servicios de teléfono mediante internet denominados *VoIP*[55].

Un pago a través de internet es una modalidad de envío de dinero normalmente asociada al comercio electrónico en la que no se requiere la entrega física de las divisas, sino que estas se realizan de manera computarizada en la moneda seleccionada. Estos pagos electrónicos se pueden realizar debitando dinero de una cuenta bancaria, con tarjetas de crédito o utilizando sistemas de monedas basados en *blockchain*[56].

---

[52] GCF APRENDE, ¿Qué Es Un Computador?. [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://edu.gcfglobal.org/es/informatica-basica/que-es-un-computador/1/>

[53] NIC, ¿Qué Es Internet?. [en línea]. 2018. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://nic.ar/es/enterate/novedades/que-es-internet>

[54] UNIVERSIDAD AUTÓNOMA DE MÉXICO, ¿Qué Es Un Dispositivo Móvil?. [en línea]. 2018. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://revista.seguridad.unam.mx/numero-07/dispositivos-moviles>

[55] DEFINICIÓN.DE, Definición De Teléfono. [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://definicion.de/telefono/>

[56] DEBITOOR, Pago Online. [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://debitoor.es/glosario/pago-online>

4.6 MARCO LEGAL

Además de los aspectos técnicos, existen aspectos legales que deben tenerse en cuenta para el desarrollo del proyecto, por lo que todas las actividades relacionadas con el *software* deben acogerse a las leyes colombianas y los tratados internacionales vigentes que los regulan:

Ley 1273 de 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley Estatutaria 1581 De 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Esta ley es conocida como la ley estatutaria de Habeas Data y limita el alcance y tratamiento de bases de datos realizadas por terceros, otorgándole a cualquier colombiano el derecho constitucional de conocer, actualizar, rectificar o autorizar que borren sus datos en cualquier momento y ante cualquier entidad que posea una base de datos y/o archivos que contenga su nombre.

Decreto Número 1317 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Ley estatutaria 1266 de 2008, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Organización de Cooperación y Desarrollo Económico (OECD), el 22 de octubre de 2010, el gobierno encabezado por el presidente Santos, solicitó formalmente a la OECD el ingreso de Colombia como miembro de la organización. La solicitud fue aceptada para su estudio al ser Colombia clasificada como un país de Renta Media Alta. (Mintic, 2014)

La Unión Internacional de Telecomunicaciones –UIT. es la organización más importante de las Naciones Unidas en lo que concierne a las Tecnologías de la Información y las Comunicaciones. Es un organismo que se encarga de la reglamentación, la normalización y el desarrollo de las TIC en todo el mundo, incluyendo la gestión internacional del espectro radioeléctrico y de las órbitas de los satélites. (Mintic, 2014)

5 DESARROLLO DE LOS OBJETIVOS

5.1 RECOPILACIÓN DE INFORMACIÓN ACERCA DEL ESTADO DEL ARTE EN MATERIA DE CIBERSEGURIDAD RELACIONADO CON EL ENTORNO FAMILIAR.

5.1.1 Estado del Arte. El análisis del estado del arte que aquí se realiza se enfoca en los tipos de prevención de delitos cibernéticos iniciando con un enfoque internacional y luego con un enfoque nacional.

5.1.1.1 Investigación y Prueba del Ciberdelito.

- Título: Investigación y Prueba del Ciberdelito
- Autor: Josefina Quevedo González.
- Categoría: Internacional
- Referencia: QUEVEDO GONZÁLEZ, Josefina. Investigación Y Prueba Del Ciberdelito. Programa De Doctorado En Derecho Y Ciencia Política. Barcelona.: Universitat De Barcelona. 2017. 505p.
- Resumen: Aborda teóricamente el origen y evolución de internet, los factores que favorecen la comisión de delitos, los cambios, conceptos y técnicas.
- Aporte: Discusión teórica sobre el origen y evolución de internet y de los delitos vinculados a través de etapas como la militar, la académica, la comercial y la social.

5.1.1.2 La Investigación de la Policía en los Ciberdelitos: Un Estudio Comparativo entre México y España.

- Título: La Investigación de la Policía en los Ciberdelitos: Un Estudio Comparativo entre México y España
- Autor: Citlalli Munguia Zuñiga
- Categoría: Internacional
- Referencia: MUNGUIA ZUÑIGA, Citlalli. La Investigación De La Policía En Los Ciberdelitos: Un Estudio Comparado Entre México Y España. Tesis Para Obtener El Grade De Maestría En Derecho. Puebla.: Benemérita Universidad Autónoma De Puebla. 2014. 154p.
- Resumen: Aporta estudio sobre el desarrollo de las nuevas tecnologías de la información y su impacto en las sociedades en relación con los ciberdelitos.
- Aporte: Desglosa una serie de condicionantes necesarias en México en cuanto a normatividad, tipificación, capacitación de la Policía y señala un comparativo con el estado en España.

5.1.1.3 Estudio exhaustivo sobre el delito cibernético.

- Título: Estudio exhaustivo sobre el delito cibernético.
- Autor: Oficina de las Naciones Unidas contra la Droga y el Delito
- Categoría: Internacional
- Referencia: OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO, Estudio Exhaustivo Sobre el Delito Cibernético. [en línea]. 2013. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf>
- Resumen: Aborda las temáticas de conectividad y delitos cibernéticos, la perspectiva global, la legislación y marcos, tipificación de delitos, evidencias electrónicas y justicia y estrategias de prevención.
- Aporte: Entrega un panorama generalizado de la problemática de delitos cibernéticos y en particular sobre la prevención como estrategia aplicada a naciones, academia y el sector privado.

5.1.1.4 Artículo 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad

- Título: Artículo 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad.
- Autor: Manuel Ángel Tevenet Gutiérrez
- Categoría: Internacional
- Referencia: TEVENET GUTIÉRREZ, Manuel ángel. Artículo 197 Bis Y Recomendaciones Para La Prevención De Los Ciberdelitos Contra La Intimidad. Máster Universitario En Seguridad De Las Tecnologías De La Información Y De Las Comunicaciones. Catalunya.: Universitat Oberta De Catalunya (UOC). 2019. 72p.
- Resumen: Pretende entregar una visión general del estado de la legislación española en ciberdelitos, desglosando las amenazas más comunes, que engloban en el artículo 197 Bis. Como problema objetivo plantea el creciente nivel de importancia que le otorga la sociedad al mundo cibernético y el grado de exposición derivado que tiene la ciudadanía en este espacio.
- Aporte: Entrega un panorama global sobre los tipos de sujetos, las conductas típicas, tipos de amenazas, vulneraciones, hacking, interceptación de datos, el rol de las compañías en el cibercrimen, prácticas de gestión de la información (ISO27001) y una serie de recomendaciones.

5.1.1.5 Las menores víctimas de la ciberdelincuencia, medidas preventivas en el ámbito internacional

- Título: Las menores víctimas de la ciberdelincuencia, medidas preventivas en el ámbito internacional.
- Autor: Juan Manuel Ávila Silva
- Categoría: Nacional

- Referencia: AVILA SILVA, Juan Manuel. Los Menores Víctimas De La Ciberdelincuencia, Medidas Preventivas En El ámbito Internacional. Barranquilla.: Universidad Libre. 2018. 12p.
- Resumen: Se centra en las medidas preventivas adoptadas internacionalmente para la protección de los menores de edad víctimas de ciberdelitos. Presenta un enfoque cualitativo, presenta estadísticas de ciberdelitos a nivel mundial y aborda un análisis jurídico deductivo por medio de la reflexión sobre la adopción de dichas medidas.
- Aporte: Aborda los menores de edad a partir de los derechos del niño y su relación con víctimas del cibercrimen. Igualmente plantea una serie de medidas preventivas ejecutadas en el ámbito internacional y su aplicabilidad, con conceptos de Naciones Unidas, Organización Internacional de Telecomunicaciones y conceptos emitidos durante cumbres mundiales. Concluye el rol fundamental de los padres y la importancia de las actividades de prevención.

5.1.1.6 Modelo Ontológico de los Ciberdelitos: Caso de estudio Colombia

- Título: Modelo Ontológico de los Ciberdelitos: Caso de estudio Colombia.
- Autor: Jhon Marin, Yuri Nieto, Freddy Huertas, Carlos Montenegro
- Categoría: Nacional
- Referencia: MARIN, Jhon. NIETO, Yuri. HUERTAS, Freddy. y MONTENEGRO, Carlos. Modelo Ontológico De Los Ciberdelitos: Caso De Estudio Colombia. *Revista Ibérica De Sistemas E Tecnologias De Informação.* Bogotá.: *Iberian Journal Of Information Systems And Technologies.* 2018. 12p..
- Resumen: Presenta un modelo Ontológico de los ciberdelitos a partir de casos de estudio en Colombia. Tiene en cuenta distintos aspectos como son jurisprudencia, clasificación, nivel de impacto y se identifican las nuevas modalidades que se están presentando.
- Aporte: Entrega una segregación de tipos de delitos informáticos y sus formas de ataque a través de mecanismos lógicos y físicos. Aborda igualmente las cifras y estrategias realizadas por el Gobierno de Colombia para prevenir este tipo de delitos.

5.1.1.7 La Práctica de Delitos Informáticos en Colombia

- Título: La Práctica de Delitos Informáticos en Colombia.
- Autor: Edison Raúl Serrano Buitrago.
- Categoría: Nacional
- Referencia: SERRANO BUITRAGO, Edison Raúl. La Práctica De Delitos Informáticos En Colombia. Especialización En Administración De La Seguridad. Bogotá.: Universidad Militar Nueva Granada. 2014. 26p.
- Resumen: Destaca la importancia del origen, evolución, métodos y tipos de personas que intervienen en un hecho delictivo informático en Colombia. Aborda la necesidad de proteger la información y de contar con los controles adecuados. También resalta la ruta para denunciar estos delitos oportunamente ante las autoridades para reducir impunidad.

- Aporte: Entrega un informe con cifras de delitos en la región, controles a realizar, buenas prácticas y el rol de la ciudadanía.

5.1.2 Amenazas, riesgos, conceptos herramientas y recomendaciones. A través del análisis del estado del arte se identifican riesgos y amenazas como la adicción a internet, riesgos emocionales, *sexting*, *sextorsión*, ciberacoso, *grooming*, *malware*, riesgos de aplicaciones y red, riesgos de interceptación de información, ingeniería social, *scam*, suplantación de identidad, *vishing*, *smishing* riesgos de extorsión, riesgos de explotación sexual, estafas informáticas comunes, herramientas y hábitos sugeridos para la gestión de contraseñas, control parental, navegación segura en internet, uso de herramientas para proteger los datos que se intercambian a través de las redes y herramientas de software antivirus. Estos conceptos son abordados detalladamente en la sección 5.4 RECOMENDACIONES DE SEGURIDAD PARA EL ENTORNO FAMILIAR, que podrá ser encontrada más adelante en este documento.

5.2 DEFINICIÓN DE RIESGOS DE CIBERSEGURIDAD PARA UNA PERSONA Y SU FAMILIA.

De acuerdo con portales como ABC Datos, los menores de edad presentan un grado de vulnerabilidad importante ante ataques cibernéticos dada la falta de contexto que pueden tener sobre el mundo debido a su corta edad y las limitadas aún experiencias que han vivido y conocido. Por ello destaca que este grupo poblacional puede ser afectado por aspectos como ciberacoso o *ciberbullying*, dado que un atacante puede presionar e incluso valerse del anonimato para engañar o realizar algún tipo de presión para que el menor haga algo que el atacante desea.

Por otra parte, también se presenta un importante grado de vulnerabilidad ante amenazas como el malware, esto debido a que este grupo poblacional suele sentirse atraído en mayor nivel hacia portales de juegos de toda índole que pueden tener el virus e infectar los equipos[57].

Entidades como el Instituto Colombiano de Bienestar Familiar (*ICBF*), destacan además riesgos cibernéticos como la ciber-dependencia, en la que niños, niñas o adolescentes hagan un uso excesivo de internet y plataformas digitales que lleguen a un punto en el que no logren desconectarse a por cuenta propia de dichos servicios[58]. De igual manera, la misma entidad alerta sobre el auge de los denominados *challenges* o retos virales en

[57] ABC DATOS, Riesgos De Ciberseguridad Para Los Menores De Edad. [en línea]. Ciberseguridad. 2021. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.abcdatos.com/blog/riesgos-de-ciberseguridad-para-los-menores-de-edad/>

[58] ICBF COLOMBIA, Conoce Los Riesgos Cibernéticos A Los Que Se Enfrentan Los Niños Y Niñas Y Cómo Prevenirlos. [en línea]. 2022. [Citado en 10 de Marzo de 2022]. Disponible en internet: <https://www.icbf.gov.co/mis-manos-te-ensenan/conoce-los-riesgos-ciberneticos-los-que-se-enfrentan-los-ninos-y-ninas-y-como>

los que les piden a los menores realizar distintos retos que les permitan obtener recompensas o premios[59] En este mismo sentido, la Policía Nacional de Colombia alerta sobre el riesgo derivado de estos retos virales, en los que un atacante podría inducir al menor a causarse a sí mismo o a otra persona algún tipo de daño, derivado de una ciber-inducción al daño físico[60].

Portales como Gaptain presentan una estadística enfocada en menores de edad en la que detalla comportamientos y peligros de acuerdo con su rango específico de edad, tal como se presenta en la Figura 1, en la que se puede evidenciar que en el primer rango de edad de 2 a 5 años los niños normalmente comienzan a tener contacto con plataformas de videos como *YouTube* y esto puede generar riesgos por presentación de contenido inapropiado para su edad. De hecho, aunque durante 2015, esta plataforma de Google lanzó su servicio *YouTube Kids* con el propósito de mostrar contenido apropiado para los menores y herramientas como configuraciones de búsquedas, temporizadores, control del historial y personalización de contenidos[61], también se ha visto inmersa en demandas por contenido inapropiado dentro de este servicio por el contenido de la publicidad que se muestra a los menores[62].

[59] ICBF COLOMBIA, Riesgos Digitales, ¿Cómo Proteger A Niñas, Niños Y Adolescentes Cuando Navegan En Internet?. [en línea]. 2019. [Citado en 10 de Marzo de 2022]. Disponible en internet: <https://www.icbf.gov.co/ser-papas/riesgos-digitales-los-que-se-exponen-los-ninos-y-como-prevenirlos>

[60] POLICÍA NACIONAL DE COLOMBIA, ¿Sabe Cómo Prevenir Que Niños, Niñas Y Adolescentes Sean Víctimas De La Ciberinducción Al Daño Físico?. [en línea]. 2018. [Citado en 10 de Marzo de 2022]. Disponible en internet: <https://www.policia.gov.co/noticia/sabe-como-prevenir-que-ninos-ninas-y-adolescentes-sean-victimas-ciberinduccion-al-dano>

[61] ASIÁN, Arantxa. 5 Trucos Para Sacarle El Máximo Provecho A Youtube Kids. [en línea]. Tu Experto Apps. 2019. [Citado en 15 de Mayo de 2021]. Disponible en internet: <https://www.tuexpertoapps.com/2019/02/07/5-trucos-para-sacarle-el-maximo-provecho-a-youtube-kids/>

[62] DIARIO LA VANGUARDIA, Denuncian A Google Por Contenido Inapropiado En Youtube Kids. [en línea]. Tecnología. 2015. [Citado en 15 de Mayo de 2021]. Disponible en internet: <https://www.lavanguardia.com/tecnologia/redes-sociales/youtube/20150407/54429717715/denuncia-google-youtube-kids.html>

Figura 1. Comportamiento y peligros para menores en internet por rango de edad

Fuente: GAPTAIN, Riesgos De Ciberseguridad Para Los Menores De Edad. [en línea]. 2021. [Citado en 25 de Abril de 2020]. Disponible en internet: <https://gaptain.com/riesgos-de-internet-y-moviles/>

De acuerdo con este mismo informe, los menores entre 6 a 9 años comienzan a tener contacto con redes sociales y eso supone una vulnerabilidad que puede ser aprovechada por pederastas u otros delincuentes que pongan en riesgo los datos privados de los menores. De igual manera, en los rangos de 10 a 14 años se encuentra que estos menores suelen obtener su primer teléfono móvil con el cual pueden presentarse situaciones de *ciberbullying* o adicción al internet, hecho que puede agudizarse en las edades de entre 15 y 17 años en donde además incrementan los riesgos por *sexting, grooming* y/o chantajes sexuales.

En cuanto a los adultos, de acuerdo con el *FBI* de Estados Unidos, para 2020 las denuncias por fraudes cibernéticos llegaron a máximos históricos en su territorio de influencia, con pérdidas totales superiores a los $4200 millones de dólares, en donde se determinó que la mayor cantidad de casos se presentaron con mayores de 50 años excediendo los $1800 millones USD[63]. En relación al impacto emocional derivado de fraudes, el Instituto Nacional de Investigación y Prevención del Fraude de Colombia INIF, realiza un análisis derivado de un estudio denominado “Fraudes financieros, salud y

[63] FEDERAL BUREAU OF INVESTIGATION (FBI), Internet Crime Report 2020. [en línea]. 2021. [Citado en 11 de Marzo de 2022]. Disponible en internet: <https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf>

calidad de vida: un estudio cualitativo"[64], realizado en España durante 2020 con una muestra de 32 personas víctimas de fraudes financieros, en donde se encontraron efectos secundarios como afectaciones a la salud mental y física entre las personas afectadas, destacándose casos como alteraciones del sueño, cansancio, cambios en el estado ánimo y dolores de cabeza permanentes[65].

De acuerdo con Fernández de Marcos (Doctora en Derecho y socia en Davara & Davara Asesores Jurídicos (España), la sociedad actual tiene la necesidad de contar con formación en todos los niveles sobre tecnologías de información con un énfasis especial en internet, ciberseguridad, redes sociales, *big data*, entre otros. De acuerdo con su planteamiento, esta formación integral debe realizarse además en términos que se puedan entender y abarcando todos los sectores desde el colegio, la universidad y el entorno empresarial[66].

5.3 PRINCIPALES MODALIDADES DE CIBERDELITOS Y REPERCUSIONES A TRAVÉS DE CASOS REALES

5.3.1 Balance de denuncias relacionadas con modalidades de ciberdelitos. En la figura 2, según las métricas de estadísticas de víctimas publicadas por la Fiscalía General de la Nación de Colombia, desde enero de 2010 hasta el cierre de abril de 2021 se han presentado las siguientes cantidades de delitos informáticos segregadas de la siguiente por rango de edades[67], y en la que se puede evidenciar que las principales víctimas de estos delitos son personas adultas entre los 29 y 59 años de edad, seguidas por jóvenes entre los 18 y 28 años, luego adultos mayores de 60 años y finalmente los adolescentes, pre-adolescentes, infancia y primera infancia (en ese orden).

---

[64] INSTITUTO NACIONAL DE INVESTIGACIÓN Y PREVENCIÓN DEL FRAUDE DE COLOMBIA INIF, Conoce el Impacto Emocional del Fraude. [en línea]. 2021. [Citado en 11 de Marzo de 2022]. Disponible en internet: <https://inif.com.co/blog/2021/02/04/impacto-emocional-del-fraude/>

[65] RODRÍGUEZ, Vicente. y PÉREZ, Daniel. Fraudes Financieros, Salud y Calidad De Vida: Un Estudio Cualitativo. [en línea]. 2020. [Citado en 11 de Marzo de 2022]. Disponible en internet: <https://www.gacetasanitaria.org/es-fraudes-financieros-salud-calidad-vida-articulo-S0213911119302742>

[66] FERNÁNDEZ DE MARCOS, Laura Davara. Formación TIC (redes Sociales, Internet, Ciberseguridad, Big Data, Etc.) En Casa, En El Colegio, En La Universidad Y En La Empresa: Características, Razón De Ser Y Contenido . [en línea]. Revista Tecnología, Ciencia Y Educación N.º 12 Enero-abril 2019 . 2019. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.tecnologia-ciencia-educacion.com/index.php/TCE/article/view/243>

[67] FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 25 de Abril de 2020]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

Figura 2. Delitos informáticos en Colombia por grupo de edad de la víctima

GRUPO_DELITO	GRUPO_EDAD_VICTIMA	Count of Rows (Total de víctimas...
DELITOS INFORMATICOS	ADULTEZ 29 - 59	13,628
DELITOS INFORMATICOS	SIN DATO	9,720
DELITOS INFORMATICOS	JUVENTUD 18 - 28	7,196
DELITOS INFORMATICOS	ADULTO MAYOR DE 60	4,231
DELITOS INFORMATICOS	ADOLESCENTE 14 - 17	1,202
DELITOS INFORMATICOS	PRE-ADOLESCENTE 12 - 13	358
DELITOS INFORMATICOS	INFANCIA 6 - 11	166
DELITOS INFORMATICOS	PRIMERA INFANCIA 0 - 5	84

Fuente: FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 25 de Abril de 2020]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

De igual manera, en este mismo período de tiempo las víctimas de delitos informáticos fueron principalmente mujeres con 18.453 casos, seguida por los hombres con 16.224, tal como se evidencia en la figura 3:

Figura 3. Delitos informáticos en Colombia por género de la víctima

GRUPO_DELITO	SEXO_VICTIMA	Count of Rows (Total de víctimas...
DELITOS INFORMATICOS	FEMENINO	18,453
DELITOS INFORMATICOS	MASCULINO	16,224
DELITOS INFORMATICOS		1,908

Fuente: FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 25 de Abril de 2020]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

Por otra parte, como se evidencia en la figura 4, se pudo encontrar también que el principal delito por el que las víctimas presentan denuncias en cuanto a delitos informáticos, corresponde a hurtos por medios informáticos con 15.448 casos, el cual duplica al segundo tipo de delito, que es acceso abusivo a un sistema informático con 6.948 casos, seguido por violación de datos personales con 6.349, luego transferencia no consentida de activos con 2.239, suplantación de sitios web con 1.986, interceptación de datos informáticos con 595, daño informático con 563, uso de software malicioso con

549, obstaculización ilegítima del sistema con 201, acceso abusivo a un sistema de información con 201, suplantación de sitios web con 143.

Figura 4. Víctimas de delitos informáticos por delito

GRUPO_DELITO	DELITO	Count of Rows (Total de víctimas...
DELITOS INFORMATICOS	HURTO POR MEDIOS INFORMATICOS Y...	15,448
DELITOS INFORMATICOS	ACCESO ABUSIVO A UN SISTEMA INFO...	6,948
DELITOS INFORMATICOS	VIOLACION DE DATOS PERSONALES AR...	6,349
DELITOS INFORMATICOS	TRANSFERENCIA NO CONSENTIDA DE ...	2,239
DELITOS INFORMATICOS	SUPLANTACION DE SITIOS WEB PARA C...	1,986
DELITOS INFORMATICOS	INTERCEPTACION DE DATOS INFORMA...	595
DELITOS INFORMATICOS	DAÑO INFORMATICO ART 269D LEY 12...	563
DELITOS INFORMATICOS	USO DE SOFTWARE MALICIOSO ART 26...	549
DELITOS INFORMATICOS	OBSTACULIZACION ILEGITIMA DEL SIST...	201
DELITOS INFORMATICOS	ACCESO ABUSIVO A UN SISTEMA INFO...	193
DELITOS INFORMATICOS	VIOLACION DE DATOS PERSONALES AR...	158
DELITOS INFORMATICOS	SUPLANTACION DE SITIOS WEB PARA C...	143
DELITOS INFORMATICOS	ACCESO ABUSIVO A UN SISTEMA INFO...	137
DELITOS INFORMATICOS	VIOLACION DE DATOS PERSONALES AR...	136
DELITOS INFORMATICOS	ACCESO ABUSIVO A UN SISTEMA INFO...	117
DELITOS INFORMATICOS	VIOLACION DE DATOS PERSONALES AR...	114
DELITOS INFORMATICOS	ACCESO ABUSIVO A UN SISTEMA INFO...	103
DELITOS INFORMATICOS	VIOLACION DE DATOS PERSONALES AR...	94
DELITOS INFORMATICOS	DE LOS ATENTADOS INFORMATICOS Y ...	38
DELITOS INFORMATICOS	INTERCEPTACION DE DATOS INFORMA...	35
DELITOS INFORMATICOS	(Other)	37,024

Fuente: FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 25 de Abril de 2020]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

Al evaluar los delitos informáticos reportados de acuerdo con los grupos poblacionales presentados (adulto mayor de 60, adultez 29-59, juventud 18-28, adolescente 14-17, preadolescente 12-13, infancia 6-11 y primera infancia 0-5) se identificaron las principales modalidades de ataque en cada grupo de integrantes de una familia.

En la figura 5 se presentan los delitos informáticos listados de acuerdo al grupo de adultos entre los 29 y 59 años de edad, denotando que el hurto por medios informáticos y semejantes es el principal motivo de denuncia con el 41% de los casos reportados. Seguido continúan el acceso abusivo a un sistema informático y la violación de datos personales con un 16% cada una, luego la transferencia no consentida de activos con 8% y la suplantación de sitios web para capturar datos personales con el 7%.

Figura 1. Delitos informáticos por grupo de edades adultez 29-59

DELITO	Percent of Total
HURTO POR MEDIOS INFORMATICOS Y SEMEJANTES ART. 269I LEY …	41%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 127…	16%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009	16%
TRANSFERENCIA NO CONSENTIDA DE ACTIVOS VALIENDOSE DE AL…	8%
SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONA…	7%
(Other)	3%
INTERCEPTACION DE DATOS INFORMATICOS, ART 269C LEY 1273 D…	2%
USO DE SOFTWARE MALICIOSO ART 269E LEY 1273 DE 2009	2%
DAÑO INFORMATICO ART 269D LEY 1273 DE 2009	2%
OBSTACULIZACION ILEGITIMA DEL SISTEMA INFORMATICO O RED …	1%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 127…	1%
SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONA…	1%

Fuente: FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 21 de Agosto de 2022]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

Por otra parte, en la figura 6 se puede evidenciar que el grupo de jóvenes entre los 18 y 28 años presenta en primer lugar denuncias de hurto por medios informáticos y semejantes con el 29%, seguido por violación de datos personales con el 24%, luego acceso abusivo a un sistema informático con el 22%, posteriormente la suplantación de sitios web para capturar datos personales con el 8% de las denuncias y la transferencia no consentida de activos con un 6%.

Figura 2. Delitos informáticos por grupo de edades juventud 18 - 28

DELITO	Percent of Total
HURTO POR MEDIOS INFORMATICOS Y SEMEJANTES ART. 269I LEY 1273 ...	29%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009	24%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 2...	22%
SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES AR...	8%
TRANSFERENCIA NO CONSENTIDA DE ACTIVOS VALIENDOSE DE ALGUNA ...	6%
(Other)	4%
INTERCEPTACION DE DATOS INFORMATICOS, ART 269C LEY 1273 DE 2009	2%
USO DE SOFTWARE MALICIOSO ART 269E LEY 1273 DE 2009	1%
DAÑO INFORMATICO ART 269D LEY 1273 DE 2009	1%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 2...	1%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 2...	1%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009, AGRAVA...	1%

Fuente: FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 21 de Agosto de 2022]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

En la figura 7 por su parte, se aborda los tipos de denuncia realizadas por adultos mayores de 60 años, en donde se encuentra que el hurto por medios informáticos es por un amplio margen el principal motivo de denuncia con el 68% de los casos, seguido de la transferencia no consentida de datos y acceso abusivo a un sistema informático con el 8% cada una. Posteriormente, la violación de datos personales con el 7%, la suplantación de sitios web para capturar datos personales con el 4% y la interceptación de delitos informáticos con el 1%.

Figura 3. Delitos informáticos por grupo de edades adulto mayor de 60

DELITO	Percent of Total
HURTO POR MEDIOS INFORMATICOS Y SEMEJANTES ART. 269I LEY 1273 ...	68%
TRANSFERENCIA NO CONSENTIDA DE ACTIVOS VALIENDOSE DE ALGUNA ...	8%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 2...	8%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009	7%
SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES AR...	4%
INTERCEPTACION DE DATOS INFORMATICOS, ART 269C LEY 1273 DE 2009	1%
(Other)	1%
DAÑO INFORMATICO ART 269D LEY 1273 DE 2009	1%
USO DE SOFTWARE MALICIOSO ART 269E LEY 1273 DE 2009	1%
OBSTACULIZACION ILEGITIMA DEL SISTEMA INFORMATICO O RED DE TEL...	0%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 2...	0%
SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES AR...	0%

Fuente: FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 21 de Agosto de 2022]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

En cuanto al grupo poblacional de adolescentes entre los 14 y 17 años, el principal motivo de denuncia varía si se compara con los 3 grupos poblacionales anteriores como se aprecia en la figura 8, dado que el acceso abusivo a un sistema informático abarca el 42% de las denuncias, seguido por la violación de datos personales con el 36%, luego por el hurto por medios informáticos y la suplantación de sitios web con el 6% cada una.

Figura 4. Delitos informáticos por grupo de edades adolescente 14 - 17

DELITO	Percent of Total
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 20...	42%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009	36%
HURTO POR MEDIOS INFORMATICOS Y SEMEJANTES ART. 269I LEY 1273 D...	6%
SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES AR...	6%
(Other)	3%
DAÑO INFORMATICO ART 269D LEY 1273 DE 2009	1%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009, AGRAVA...	1%
INTERCEPTACION DE DATOS INFORMATICOS, ART 269C LEY 1273 DE 2009	1%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 20...	1%
TRANSFERENCIA NO CONSENTIDA DE ACTIVOS VALIENDOSE DE ALGUNA ...	1%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009, AGRAVA...	1%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 20...	1%

Fuente: FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 21 de Agosto de 2022]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

En este orden, como se presenta en la figura 9, entre el grupo de preadolescentes entre los 12 y 13 años el acceso abusivo a un sistema informático es el mayor motivo de denuncia con el 47% de los casos, seguido por la violación de datos personales con el 35%, luego por la suplantación de sitios web para capturar datos con el 6%, luego el hurto por medios informáticos con el 2% y el acceso abusivo a un sistema informático con el 1%.

Figura 5. Delitos informáticos por grupo de edades preadolescente 12-13

DELITO	Percent of Total
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 2...	47%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009	35%
SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES A...	6%
(Other)	3%
HURTO POR MEDIOS INFORMATICOS Y SEMEJANTES ART. 269I LEY 1273 ...	2%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 2...	1%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 2...	1%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 2...	1%
INTERCEPTACION DE DATOS INFORMATICOS, ART 269C LEY 1273 DE 2009	1%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009, AGRAV...	1%
DAÑO INFORMATICO ART 269D LEY 1273 DE 2009	0%
OBSTACULIZACION ILEGITIMA DEL SISTEMA INFORMATICO O RED DE TEL...	0%

Fuente: FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 21 de Agosto de 2022]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

Para el grupo poblacional de infantes entre los 6 y 11 años, como se evidencia en la figura 10, el acceso abusivo a un sistema informático es el principal motivo de denuncia con el 39% de los casos, seguido de la violación de datos personales con el 32%, luego el hurto por medios informáticos y semejantes con el 14%, posteriormente la suplantación de sitios web para capturar datos personales con el 6%, y el daño informático con el 2%. También se segmentan en este grupo la interceptación de datos informáticos, la transferencia no consentida de activos, el daño informático y la violación de datos personales con el 1% de los casos.

Figura 6. Delitos informáticos por grupo de edades infancia 6-11

DELITO	Percent of Total
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 20...	39%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009	32%
HURTO POR MEDIOS INFORMATICOS Y SEMEJANTES ART. 269I LEY 1273 D...	14%
SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES AR...	6%
DAÑO INFORMATICO ART 269D LEY 1273 DE 2009	2%
(Other)	2%
INTERCEPTACION DE DATOS INFORMATICOS, ART 269C LEY 1273 DE 2009	1%
TRANSFERENCIA NO CONSENTIDA DE ACTIVOS VALIENDOSE DE ALGUNA ...	1%
DAÑO INFORMATICO ART 269D LEY 1273 DE 2009, AGRAVADO POR APROV...	1%
USO DE SOFTWARE MALICIOSO ART 269E LEY 1273 DE 2009	1%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009, AGRAVA...	1%
OBSTACULIZACION ILEGITIMA DEL SISTEMA INFORMATICO O RED DE TEL...	1%

Fuente: FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 21 de Agosto de 2022]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

En la figura 11, se listan los delitos informáticos para el grupo de infantes entre los 0 a 5 años, cuyo principal motivo de denuncia son el hurto por medios informáticos con el 34%, luego la violación de datos personales con el 29%, seguidamente del acceso abusivo a un sistema informático con el 18%, la transferencia no consentida de activos con el 5%, la suplantación de sitios web para captura de datos personales con el 5%.

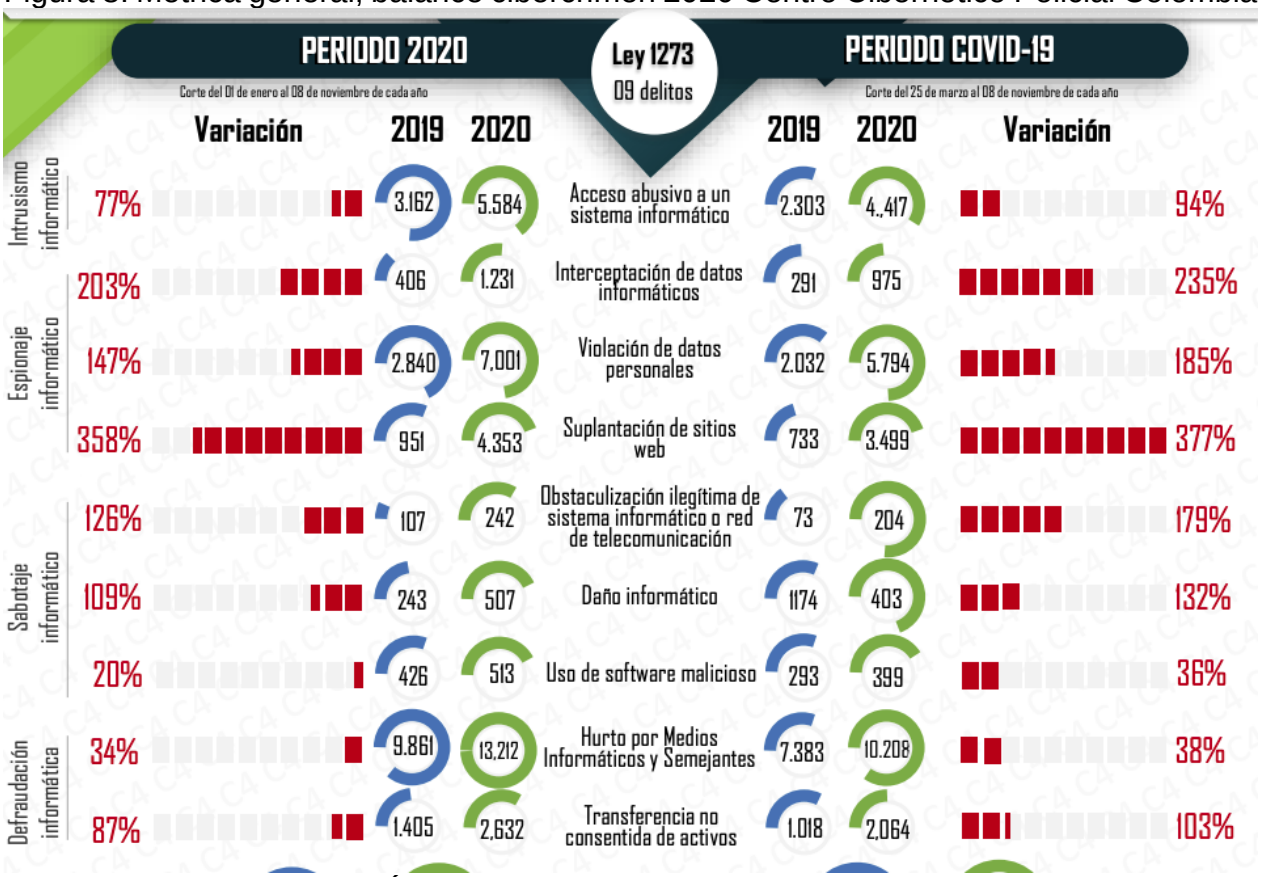
Figura 7. Delitos informáticos por grupo de edades primera infancia 0-5

DELITO	Percent of Total
HURTO POR MEDIOS INFORMATICOS Y SEMEJANTES ART. 269I LEY 1273 D...	34%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009	29%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 20...	18%
TRANSFERENCIA NO CONSENTIDA DE ACTIVOS VALIENDOSE DE ALGUNA ...	5%
SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES AR...	5%
DAÑO INFORMATICO ART 269D LEY 1273 DE 2009	3%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 20...	2%
OBSTACULIZACION ILEGITIMA DEL SISTEMA INFORMATICO O RED DE TEL...	1%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 20...	1%
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009, AGRAVA...	1%
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 20...	1%

Fuente: FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 21 de Agosto de 2022]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

Por su parte, el Centro Cibernético Policial de la Policía Nacional de Colombia, en su último informe publicado con corte a noviembre de 2020, presenta las métricas del resultado de la acción operativa de la entidad, en donde se destaca una variación del 377% en el delito de suplantación de sitios web en comparación con el período anterior (2019), seguido de la interceptación de datos informáticos con una variación del 235% en el mismo período. En la figura 12 se pueden evidenciar también los demás delitos de este informe, tales como violación de datos personales (185%), obstaculización ilegítima de sistema informático o red de telecomunicación (179%), daño informático (132%), transferencia no consentida de activos (103%), acceso abusivo a un sistema informático (94%), hurto por medios informáticos y semejantes (38%) y uso de software malicioso (36%).

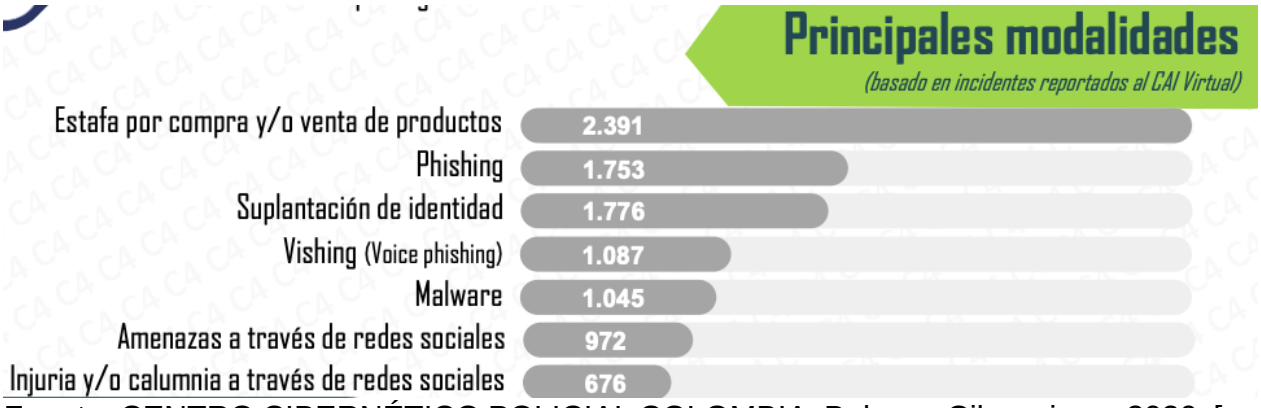
Figura 8. Métrica general, balance cibercrimen 2020 Centro Cibernético Policial Colombia



Fuente: CENTRO CIBERNÉTICO POLICIAL COLOMBIA, Balance Cibercrimen 2020. [en línea]. 2021. [Citado en 20 de Agosto de 2022]. Disponible en internet: <https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf>

Este mismo informe además, señala las principales modalidades de delitos cibernéticos reportadas a través de la herramienta *CAI Virtual* del Centro Cibernético Policial de Colombia en 2020, las cuales pueden ser evidenciadas en la figura 13, en donde por un amplio margen predomina la estafa por compra y/o venta de productos con 2392 casos, seguida por el *phishing* (1753 casos), suplantación de identidad (1776 casos), *vishing* (1087 casos), *malware* (1045 casos), amenazas a través de redes sociales (972 casos) e injuria y/o calumnia a través de redes sociales (676 casos.)

Figura 9. Principales modalidades de ciberdelitos reportadas a través de la herramienta *CAI VIRTUAL*



Fuente: CENTRO CIBERNÉTICO POLICIAL COLOMBIA, Balance Cibercrimen 2020. [en línea]. 2021. [Citado en 20 de Agosto de 2022]. Disponible en internet: <https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf>

Vale la pena resaltar, que estas estadísticas posiblemente se quedan cortas, dado que según el Departamento Nacional de Estadísticas de Colombia – DANE, durante 2020 un 69% de las personas no realizaron denuncias de delitos ante las autoridades. De acuerdo con el director de esta entidad, esto se debe a que la ciudadanía colombiana considera que las autoridades son ineficientes y las víctimas no confían en el desempeño de la administración de la justicia[68].

5.3.2 Testimonios relacionados con casos reales. Aunque son masivas las denuncias entregadas a las autoridades, muchas de las víctimas prefieren abstenerse de hablar al respecto en público ya sea por temor a algún tipo de futuras represalias o por vergüenza[69], este hecho también se motiva por algún tipo de desconfianza en el éxito que pueda tener la investigación[70]. Aun así, se encuentran casos reales en donde las víctimas abiertamente han contado su experiencia y el impacto que ha causado en su entorno.

Un primer caso difundido en la prensa durante 2021 presenta la historia de “Clara” (el nombre original se ha cambiado el nombre durante la redacción del artículo), quien fue

[68] ACOSTA ARGOTE, Cristian. Un 69,8% De Las Personas No Denuncia Los Delitos Ante Las Autoridades Según Informe Del DANE. [en línea]. Asuntos Legales Diario La República. 2021. [Citado en 15 de Mayo de 2021]. Disponible en internet: <https://www.asuntoslegales.com.co/actualidad/un-698-de-las-personas-no-denuncia-los-delitos-ante-las-autoridades-segun-el-dane-3131619>

[69] VILLALBA, Juan José. “Muchas Víctimas No Hablan Por Vergüenza”: El Perturbador Caso Del Hombre Que Sedujo Y Estafó A Más De Cincuenta Mujeres. [en línea]. 2021. [Citado en 12 de Marzo de 2022]. Disponible en internet: <https://elpais.com/icon/actualidad/2021-04-22/muchas-victimas-no-hablan-por-verguenza-el-perturbador-caso-del-hombre-que-sedujo-y-estafo-a-mas-de-cincuenta-mujeres.html>

[70] BBC MUNDO, ¿qué Hacer Si Publican Una Foto Tuya En Internet Sin Tu Permiso?. [en línea]. 2017. [Citado en 12 de Marzo de 2022]. Disponible en internet: <https://www.bbc.com/mundo/noticias-37896303>

víctima de un delito cibernético en Colombia por medio de diferentes llamadas telefónicas en las que le ofrecían una serie de beneficios por contar con una tarjeta de crédito. En este caso, los estafadores tenían todos sus datos, incluyendo los números de su tarjeta de crédito y hasta el cupo exacto que se la había asignado. Aunque ella no aceptó ninguna oferta, posteriormente evidenció los cargos a su tarjeta de crédito, los cuales, ante la negativa de ayuda por parte del banco emisor, le motivaron a denunciar, descubriendo durante la investigación que el estafador grabó la llamada y la editó de tal manera que se escuchara que ella aceptaba todo lo que le habían previamente ofrecido[71]. Contra este grupo de estafadores existen más de 6000 denuncias en Colombia, siendo una banda conformada por 51 delincuentes[72].

Otro tipo de casos como el de acceso abusivo a un sistema de información y suplantación de identidad se encuentra, de acuerdo con el diario El Heraldo de Colombia, en el caso de una mujer llamada Inés Navarro, quien interpone ante la Fiscalía de este país una denuncia por hackeo a sus redes sociales y correo electrónico. De acuerdo con la declaración pública que entrega la mujer al mencionado medio de comunicación con relativa angustia, los atacantes obtuvieron la lista de sus contactos a quienes estuvieron contactando, haciéndose pasar por ella para solicitarles dinero a su nombre. Incluso algunas personas estafadas por los atacantes la han buscado nuevamente a ella para cobrar el dinero que supuestamente les había prestado[73].

El impacto de los delitos informáticos también puede verse reflejado también en la estabilidad económica de una familia. Un caso conocido en Chile durante 2020 y difundido por medios de comunicación de ese país reflejó el drama de la reconocida chef Virginia de María a quien le hurtaron su cuenta de la popular red *Instagram*. De acuerdo con la profesional, el atacante la estuvo extorsionando, exigiéndole millonarias sumas de dinero para poder recuperar su cuenta, luego de ir poco a poco borrando todo su material de la mencionada plataforma. Esta situación generó una detenida en sus ingresos traduciéndose una serie de inconvenientes a nivel personal, laboral y económico como ella misma lo definió entre lágrimas públicamente[74].

---

[71] EL TIEMPO, El Testimonio De Una Víctima De Estafadores A Través De 'Call Center'. [en línea]. 2021. [Citado en 12 de Marzo de 2022]. Disponible en internet: <https://www.eltiempo.com/justicia/delitos/estafa-testimonio-de-victima-que-robaron-a-traves-de-call-center-595708>

[72] BLU RADIO, Cayeron Los Call Center: Estafaron A Más De 6.900 Personas Con Venta Ficticia De Servicios Bancarios. [en línea]. 2021. [Citado en 12 de Marzo de 2022]. Disponible en internet: <https://www.bluradio.com/judicial/cayeron-los-call-center-estafaron-a-mas-de-6-900-personas-con-venta-ficticia-de-servicios-bancarios>

[73] EL HERALDO, Alertan Aumento De Hackeo A Correos Y Redes Sociales. [en línea]. 2020. [Citado en 12 de Marzo de 2022]. Disponible en internet: <https://www.elheraldo.co/judicial/alertan-aumento-de-hackeo-correos-y-redes-sociales-738973>

[74] TELE13, La Terrible Pesadilla Que Vive Virginia De María Tras El Hackeo De Su Cuenta De Instagram. [en línea]. 2020. [Citado en 12 de Marzo de 2022]. Disponible en internet: <https://www.t13.cl/noticia/tendencias/terrible-pesadilla-virginia-maria-hackeo-instagram-extorsion-18-12-2020>

Escenarios como el robo de identidad digital también reflejan los ciberdelitos en sus diferentes modalidades. Uno de los casos más graves conocidos en México durante 2017, se dio a conocer luego que una joven estudiante originaria de Nayarit recibió una notificación del Servicio de Administración Tributaria (SAT) de ese país en la que le cobraban los impuestos correspondientes a la recepción de depósitos bancarios por más de 800 millones de pesos mexicanos (38 millones de dólares aproximadamente). Durante la investigación, se encontró que su identidad digital había sido robada y otras personas lograron crear y administrar una cuenta bancaria a su nombre para realizar la transacción de los dineros[75].

Otras víctimas, también en México han denunciado públicamente casos en los que fueron víctimas de hurtos por medios informáticos. Una mujer de 43 años, usuaria de tarjeta de crédito con un manejo excepcional en relación con los compromisos con su cuenta, recibió varios correos electrónicos de su banco en la que le alertaban sobre un bloqueo de la tarjeta por mal uso. Para reactivarla, le exigieron diligenciar un formulario aparentemente del banco con la información necesaria para dicho proceso. 30 minutos después, recibió una alerta relacionada con compras por valor de 30000 pesos mexicanos (1500 dólares aproximadamente). Al contactar a la entidad bancaria para denunciar el posible fraude, manifestó las dificultades que encontró para intentar demostrar que ella no hizo esa compra, dado que el banco se excusó trasladando la culpa a la usuaria por diligenciar dicho formulario[76].

5.4 RECOMENDACIONES DE SEGURIDAD PARA EL ENTORNO FAMILIAR

5.4.1 Conceptos básicos.

5.4.1.1 ¿Qué es la ciberseguridad? De acuerdo con Kaspersky, la ciberseguridad es una práctica que se enfoca en la defensa de las redes y sistemas electrónicos frente a ataques maliciosos. Se extiende a aspectos como la seguridad en aplicaciones, seguridad de la información, seguridad de redes, recuperación ante desastres y formación para la prevención[77].

[75] CAPITAL MÉXICO, Casos Más Graves Del Robo De Identidad. [en línea]. 2017. [Citado en 13 de Marzo de 2022]. Disponible en internet: <https://www.capitalmexico.com.mx/especial/casos-mas-graves-del-robo-de-identidad-sat-adeudos-fiscales/>

[76] DIARIO EL UNIVERSAL, Tres Historias, Misma Tragedia. [en línea]. 2017. [Citado en 13 de Marzo de 2022]. Disponible en internet: <https://www.eluniversal.com.mx/articulo/cartera/finanzas/2015/09/28/robo-de-identidad-tres-historias-misma-tragedia>

[77] KASPERSKY, ¿Qué es la Ciberseguridad?. [en línea]. 2021. [Citado en 13 de Marzo de 2022]. Disponible en internet: <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>

De igual manera, para Cisco, los aspectos fundamentales de la ciberseguridad deben atenderse a partir de la implementación de un sistema de gestión de amenazas en las que se pueda afrontar los riesgos a partir de diferentes frentes, como los procesos, la tecnología y principalmente sobre la atención en las personas, quienes finalmente suelen ser la parte frágil de la cadena en aspectos relacionados con la seguridad informática[78].

5.4.1.2 Ciberseguridad y la familia. De acuerdo con la corporación Hábitat para la Humanidad de México, la familia se define como la célula principal de la sociedad, siendo el lugar en donde se vive el aprendizaje de valores y los hábitos necesarios para el desarrollo y progreso de una sociedad[79]. En este orden de ideas, y de acuerdo con el Banco Mundial, los aprendizajes que se logran en el entorno familiar y escolar durante la primera infancia son fundamentales para la fuerza laboral y productiva de las naciones[80].

Enlazando estos dos conceptos en relación con los procesos de aprendizaje en familia, de acuerdo con la medicina familiar se puede determinar que existe una influencia importante entre los conocimientos y saberes que se crean en el hogar, los cuales se fortalecen a través del aprendizaje mutuo entre todos sus integrantes, lo cual podrá contribuir a la formación personal y académica de todos sus integrantes[81]. En este contexto, la oportunidad de formación en aspectos de ciberseguridad a partir de la familia toma un rol importante, y es que, de acuerdo con Microsoft México, 9 de cada 10 personas consideran que es necesaria una formación para que el entorno digital sea más seguro[82].

5.4.1.3 ¿Qué son las TIC?. Las TIC se definen como Tecnologías de la Información y la Comunicación. Específicamente son tecnologías que utilizan microelectrónica, informática y telecomunicaciones para ofrecer medios para comunicarse utilizando herramientas tecnológicas y comunicacionales[83]. En otras palabras, es un coctel de tecnologías para facilitar la comunicación.

---

[78] CISCO, ¿Qué es la Ciberseguridad?. [en línea]. 2021. [Citado en 13 de Marzo de 2022]. Disponible en internet: <https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~how-cybersecurity-works>

[79] CORPORACIÓN HÁBITAT PARA LA HUMANIDAD MÉXICO, La Familia Como Base de la Sociedad. [en línea]. 2021. [Citado en 13 de Marzo de 2022]. Disponible en internet: <https://www.habitatmexico.org/article/la-familia-como-base-de-la-sociedad>

[80] OZANUS, P. Scott. La Primera Infancia Como Base de la Fuerza Laboral del Futuro. [en línea]. 2017. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://blogs.worldbank.org/es/voices/la-primera-infancia-como-base-de-la-fuerza-laboral-del-futuro>

[81] FERNÁNDEZ DELGADO, Darío. Aprender en Familia, Una Experiencia Enriquecedora. [en línea]. 2020. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.linkedin.com/pulse/aprender-en-familia-una-experiencia-enriquecedora-mariposas-colombia/?originalSubdomain=es>

[82] MICROSOFT, ¿Cómo Proteger a Tus Niños y Adolescentes de los Riesgos en Línea?. [en línea]. 2022. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://news.microsoft.com/wp-content/uploads/prod/sites/41/2022/02/eBook-GuiaCiberseguridad-para-padres-de-familia-VF.pdf>

[83] CLARO, ¿Qué Son Las TIC? Y ¿Por Qué Son Tan Importantes?. [en línea]. 2019. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.claro.com.co/institucional/que-son-las-tic/>

Se clasifican en dos tipos: Por un lado, se encuentran las tecnologías de la comunicación (*TC*) tales como la telefonía, la radio y la televisión, y por otra, las tecnologías de la información (*TI*), que se enfocan en la digitalización, gestión y registro de contenidos. En conjunto, las *TC* y las *TI* constituyen las redes y plataformas necesarias con las cuales hoy es posible comunicarse mediante voz, texto, video y realizar innumerables tareas remotas como trabajar, estudiar, comerciar, entretenerse y demás[84].

5.4.1.4 Internet. De esta manera se conoce a la principal red de comunicación a nivel mundial. El significado de la palabra "internet" se refiere a los términos *inter* para referirse a enlaces y conexiones, y *net* para relacionarse con la interconexión de las redes. De esta manera, es fácil deducir que se refiere a una conexión integrada de redes interconectadas[85].

Más allá de su significado, las oportunidades que ofrece internet en la actualidad (2022) permiten trabajar desde cualquier lugar, comunicarse, estudiar, divertirse, vender, tomar citas médicas mediante telemedicina, comprar, vender, realizar inversiones, manipular aparatos mediante el llamado internet de las cosas, informarse y acceder a un sinfín de fuentes de información[86]. Por supuesto, esta enorme oferta, como en cualquier aspecto también representa una serie de riesgos y su protección ante ellos es el motivo por el cual se crea el presente análisis.

[84] IONET, Soporte TI Vs TIC ¿Cuál es la Diferencia?. [en línea]. 2020. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.ionet.cl/post/soporte-ti-vs-tic-cual-es-la-diferencia>

[85] COLEGIO DE MICHOACÁN, Internet. [en línea]. 2019. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.colmich.edu.mx/computo/files/internet.pdf>

[86] COLOMBIA. ESCUELA TIC FAMILIA, ¿Qué Actividades Puedo Realizar en Internet?. [en línea]. 2018. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.escuelaticfamilia.gov.co/648/w3-article-71538.html>

5.4.1.5 Redes Sociales. Se define de esta manera a las diferentes páginas web y/o aplicaciones que a través de diferentes metodologías y tecnologías sirven como herramientas de comunicación entre los usuarios que hacen uso de ellas. Principalmente, a través de ella se logra una comunicación compartiendo textos, imágenes, videos e incluso audios. Normalmente en estas plataformas y/o aplicaciones, un usuario ingresa para crear un perfil con información personal con el propósito de ser encontrado por otros usuarios. En dicho perfil, normalmente el usuario comparte contenido propio (imágenes, videos, audios, etc) para que sea visto por otras personas[87]. Esta característica de compartir contenido es el eje central sobre el cual se fundamentan las redes sociales. Por un lado, quien consume el contenido suele sentirse actualizado con información reciente de su interés generando un estado de gratificación inmediata en su cerebro, y por otro lado, quien genera el contenido y recibe reacciones de otros usuarios suele sentirse gratificado también al percibir que está obteniendo reacciones positivas de otros usuarios[88].

5.4.1.6 Huella digital y reputación en internet. Iniciaremos con un ejemplo sencillo: Cuando alguien camina en la arena va dejando un rastro de cada pisada a medida que avanza; eso es una huella. En internet, cada pisada es el registro de la actividad del usuario en la red, fotografías, publicaciones, registros de ingreso a plataformas, un *like* en alguna red social, compras, comentarios, gustos, amistades, operaciones bancarias, noticias, cada registro de cada sitio que visitas, suscripciones etc. La diferencia entre las huellas dejadas en la arena y las huellas dejadas en internet es sencilla: Las huellas en internet no se borran así el usuario crea que las borró[89], lo cual resulta sumamente atractivo para hackers malintencionados que a partir de esa información pueden construir un ataque.

Cada una de las huellas dejadas en internet están asociadas a la identidad digital de cada persona, por lo que una organización o persona potencialmente podría acceder a ella para obtener más información de lo que la persona cree relacionada con su manera de pensar, de actuar y en esencia de su ser[90]. Un ejercicio sencillo es escribir el nombre de la persona a consultar en el popular buscador de Google para descubrir como comienza a aparecer información y fotografías de dicha persona.

---

[87] GODADDY, ¿Qué Son Las Redes Sociales y Para Qué Sirven?. [en línea]. 2021. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://es.godaddy.com/blog/que-son-las-redes-sociales-y-para-que-sirven/>

[88] VELÁSQUEZ, Melissa. y MELO, Carolina. ¿Por Qué Son Tan Adictivas Las Redes Sociales?. [en línea]. 2021. [Citado en 14 de Marzo de 2022]. Disponible en internet: < https://cnnespanol.cnn.com/2021/10/29/redes-sociales-adictivas-facebook-instagram-twitter-orix/>

[89] GOBIERNO DE ARGENTINA, Huella Digital y Reputación Web. [en línea]. 2021. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.argentina.gob.ar/jefatura/innovacion-publica/gobierno-abierto-y-pais-digital/paisdigital/navegacion-segura/huella-digital-y-reputacion-web-1>

[90] GOBIERNO DE CANARIAS, ¿Qué es la Identidad Digital?. [en línea]. 2020. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/identidad-digital-profesorado/que-es-la-identidad-digital/>

5.4.1.6.1 Recomendaciones para controlar la identidad digital. De acuerdo con McAfee, es importante tomar una serie de medidas que permitan controlar la identidad digital. La primera medida es no utilizar redes *wifi* públicas tal como las que se encuentran en centros comerciales o aeropuertos; en caso que sea estrictamente necesario, sería fundamental contar un una red VPN para proteger la información que circule por dicha red. De igual manera, es importante no escribir ningún tipo de información en páginas web que no inicien con "https", el cual es un protocolo seguro de transferencia de hipertexto que garantiza que la información sea encriptada y entregada al punto sin poder ser interceptada en su ruta. Por otra parte, también es recomendable utilizar contraseñas seguras y modificarlas regularmente; en este sentido es importante que la contraseña cuente con al menos 16 caracteres que incluyan letras, números, mayúsculas, minúsculas y símbolos. En cuanto al software que se utiliza ya sea en el computador o *smartphone*, es importante que este se encuentre actualizado dado que frecuentemente los desarrolladores publican nuevas versiones o parches que incluyen mejoras o correcciones de seguridad; y finalmente, es importante revisar los términos y condiciones de las plataformas y/o software que utiliza, dado que es conocido que suele ser una práctica habitual que a veces dichos términos incluyan dentro de la "letra menuda" de los contratos algún tipo de cláusulas para explotar, vender y transferir (incluso a perpetuidad) los datos de los usuarios[91].

5.4.1.7 *Deep web.* Para comprender la denominada *deep web* simplemente es necesario aprender a diferenciarla de la *surface web*. En la figura 14 es posible hacerse una idea de la diferencia.

Figura 14. Surface Web vs. Deep Web

Fuente: WIKIDATA, Deep Web. [en línea]. 2017. [Citado en 14 de Marzo de 2022]. Disponible en internet:

[91] MCAFEE, ¿Qué es la Identidad Digital y Todo lo que Puedes Hacer para Protegerla?. [en línea]. 2021. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.mcafee.com/blogs/languages/espanol/que-es-la-identidad-digital-y-todo-lo-que-puedes-hacer-para-protegerla/>

<https://upload.wikimedia.org/wikipedia/commons/c/c9/Surface_Web_%26_Deep_Web.jpg>

A un nivel más técnico, de acuerdo con el portal web Hipertextual, la *deep web* es básicamente todo el contenido encontrado en internet que no se encuentra indexado en los buscadores *web* normales como Bing, Google, Yahoo, Baidu, Yandex etc. De cierta manera, hace parte de la internet profunda porque es invisible para estos buscadores los cuales son quienes generan la mayor parte del tráfico que ingresa a los sitios web[92]. Ahora bien, esta deep web no debe confundirse con la dark web, puesto que en esta última convergen todos los contenidos que tienen propósitos ilegales y/o delictivos, y sobre la cual se abordará el siguiente punto.

5.4.1.8 *Dark web*. Para acceder a la *dark web* es necesario utilizar redes propias que se conocen como *darknets*. Para ello existen tecnologías como *Freenet* o *Tor* con las cuales es posible crear y compartir contenido que se presente de manera oculta a los navegadores tradicionales y que solo puedan ser accesibles por medio de herramientas de software específicas, buscando como premisa mantener el anonimato

Aunque la utilidad inicial de la *dark web* se centra buscar evadir la censura y el rastreo realizado por los gobiernos, también es conocido que en esta red suelen circular ampliamente y sin restricción algunos contenidos que se considera no debería estar en línea por ir contra de las leyes; por ejemplo sitios que permitan comprar armas, drogas, medicamentos sin receta, estafas, contratar sicarios, etc[93].

[92] LÓPEZ, José María. Deep Web: Qué Es y Cómo Entrar en el Lado Más Oculto de Internet. [en línea]. 2017. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://hipertextual.com/2021/04/deep-web-como-entrar-que-es>

[93] KASPERSKY, ¿Qué es la Deep Web y la Dark Web?. [en línea]. 2020. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.kaspersky.es/resource-center/threats/deep-web>

5.4.1.8.1 Recomendaciones para acceder a la *dark web*. Si un usuario decide ingresar a la *dark web* ya conociendo el propósito de dicha red, lo mínimo que debería hacer es tomar al menos algunas precauciones, como separar su identidad en dicha red de su identidad real. Es decir, no utilizar su nombre real, ni las mismas imágenes, ni los mismos correos electrónicos, ni las mismas contraseñas, ni medios de pago que usa habitualmente. De igual manera, es importante no descargar archivos de dicha red ya que podrían estar contaminados por algún tipo de virus que podría poner al usuario en aprietos. También, es importante desactivar *Java* y *ActiveX* para evitar intrusiones remotas por este medio y sobre todo es fundamental que confíe en su intuición para protegerse de estafas o de atacantes que quieran obtener acceso a la información real del usuario[94].

5.4.1.9 *Hackers*. De acuerdo con ADSL Zone, un *hacker* es una persona con conocimientos relacionados con informática suficientes para lograr acceder a plataformas sin autorización por medio de la explotación de vulnerabilidades existentes. En pocas palabras, son personas capaces de descubrir los puntos débiles de un sistema y de explotarlos[95]. Existen distintos tipos de *hackers* tal como se describe a continuación[96].

5.4.1.9.1 *White-hat hackers.* A menudo este grupo de *hackers* trabaja para agencias de ciberseguridad, áreas de TI de las empresas o por motivación propia. Utilizan sus conocimientos con propósitos “blancos” como descubrir y reportar vulnerabilidades en el marco del respeto a las leyes aplicables.

5.4.1.9.2 *Black-hat hackers*. Este grupo de hackers generalmente actúan con propósitos delictivos como robar datos, realizar ataques de denegaciones de servicio (DDoS), distribuir software malicioso, comprar y vender *malware*, engañar a personas mediante ingeniería social, entre otras actividades informáticas que realizan con propósitos maliciosos.

[94] WELIVESECURITY, Cómo Configurar Tor Para Navegar en la Deep Web de Forma Segura. [en línea]. 2020. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.welivesecurity.com/la-es/2020/07/23/como-configurar-tor-navegar-deep-web-forma-segura/>

[95] LUENGO, Manuel. Te Contamos Qué es un Hacker y Cuántos Tipos Hay. [en línea]. 2021. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.adslzone.net/reportajes/seguridad/hacker-tipos/>

[96] KASPERSKY. Hackers de Sombrero Negro, Blanco y Gris: Definición y Explicación. [en línea]. 2022. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://latam.kaspersky.com/resource-center/definitions/hacker-hat-types>

5.4.1.9.3 *Gray-hat hackers.* Este grupo comprende aquellos *hackers* que combinan los dos anteriores. Por ello, es habitual que se encarguen de buscar vulnerabilidades en un sistema sin la autorización del propietario y en ocasiones se ofrecen a solucionar la vulnerabilidad por un pago. También se conocen porque suelen disfrutar alardear de sus conocimientos y sienten una profunda convicción por ingresar sin autorización a sistemas para demostrar a los propietarios que tienen razón. En este contexto, es común que a los propietarios de los sistemas no les guste el hecho de que estos *hackers* ingresen a sus sistemas sin autorización y por ende se consideran ilegales.

5.4.1 Riesgos.

5.4.1.1 ¿Qué es un riesgo? Un riesgo se define como la posibilidad latente de que se produzca algún tipo de contratiempo o desgracia de que algo o alguien sufra algún daño o perjuicio. De acuerdo con *Red Hat* (corporación desarrolladora del sistema operativo *Red Hat Enterprise Linux*), en el caso de las Tecnologías de la Información (TI), los riesgos pueden ser originados por diferentes causas, como desastres naturales, accidentes, errores de administración o amenazas latentes de ciberseguridad[97].

5.4.1.2 Adicción a internet. Para la Clínica Recal, especializada en el tratamiento de adicciones en España, la adicción a internet se define como un problema relacionado con la capacidad individual de controlar los impulsos, los cuales le impiden a una persona abstenerse o moderar el uso de internet. Esta incapacidad de control llega a afectar individualmente a la persona en sus relaciones de familia, amistades y/o de trabajo.

De acuerdo con un estudio denominado *"Internet addiction: When the positive emotions are not so positive"* (Adicción a internet: Cuando las emociones positivas no son tan positivas) dado a conocer en 2019 por la Universidad de Michigan en Estados Unidos, se pudo establecer que existen rasgos de la personalidad que se deterioran con el uso excesivo de internet tales como la amabilidad, la autoestima, la estabilidad emocional, la conciencia y la apertura a vivir nuevas experiencias. De acuerdo con este mismo estudio, concluye que la calidad de vida cae en picada cuando interviene un patrón de abuso en el uso de internet en las personas[98].

En este orden de ideas, otro estudio publicado en 2017 enfocado en los jóvenes encontró que algunos rasgos de la personalidad como el neuroticismo y la elevada extroversión aumentaban el uso abusivo de internet a lo largo del tiempo, comenzando a ser problemático con más de 2 horas diarias entre semana y más de 4 horas diarias a lo largo

[97] REDHAT, ¿Qué es la Gestión de Riesgos?. [en línea]. 2019. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.redhat.com/es/topics/management/what-is-risk-management>

[98] LONGSTREET, Phil. GONZÁLEZ, Esther. y BROOKS, Stoney. Internet Addiction: When The Positive Emotions Are Not So Positive. [en línea]. 2019. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.sciencedirect.com/science/article/abs/pii/S0160791X18300290>

del fin de semana, sugiriendo que exceder este tiempo de consumo constituye un factor de riesgo[99].

5.4.1.3 Riesgos emocionales y físicos. Los problemas de ciberseguridad no afectan únicamente a empresas y grandes corporaciones con vulneraciones, robos y/o secuestros de información. Existen amenazas que se enfocan explícitamente sobre las personas de todas las edades, abriendo la posibilidad de afectar significativamente la estabilidad emocional y física de un entorno familiar completo.

5.4.1.3.1 *Sexting* – Sextorsión. Se conoce de esta manera a la práctica de enviar fotos y/o videos de carácter sexual de sí mismo a otra persona mediante medios electrónicos. Aunque parezca difícil de creer, de acuerdo con UNICEF, tan solo en México un 65% de los usuarios de internet entre los 15 y 19 años ha realizado al menos una vez alguna práctica de *sexting*, siendo principalmente los hombres quienes la realizan. De este balance, el 50% lo han practicado con su pareja del momento, mientras que el 30% con un amigo o amiga. Algunas de las causales expuestas en el informa atribuyen a posibles presiones de la pareja y adrenalina por vivir la experiencia con una persona conocida o desconocida[100].

5.4.1.3.1.1 Recomendaciones en casos de *sexting*. En este análisis ya se abordó el concepto de huella digital en internet (una vez se publica algo en la red, difícilmente se puede eliminar aunque se intente), sin embargo, y aunque en este material no se recomienda hacerlo bajo ninguna circunstancia, si un usuario decidió hacerlo siendo consciente de ello y bajo su propio riesgo, es posible entregar al menos algunas recomendaciones para atender una eventual crisis originada por filtraciones de este material íntimo y privado de acuerdo con la organización IS4K[101]:

- Responder con calma. Si un menor o alguien cercano resulta afectado por un caso de filtrado de material íntimo ayude a resolver el problema y evite reacciones fuertes.
- Contactar a los difusores: Si se tiene la posibilidad de contactar a quien está difundiendo los contenidos debe realizarse el contacto y solicitar la eliminación.
- Reportar ante proveedores de servicios: Si el contenido se publica en alguna plataforma como Facebook, Instagram, Twitter, TikTok, etc, es fundamental que reporte ante la plataforma correspondiente el contenido. Esto no es garantía de que dicho contenido desaparecerá, pero ayudará a limitar su difusión.

[99] ANDERSON, Emma Louise. y STEEN, Eloisa. Internet Use And Problematic Internet Use: A Systematic Review Of Longitudinal Research Trends In Adolescence And Emergent Adulthood. [en línea]. 2017. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.tandfonline.com/doi/full/10.1080/02673843.2016.1227716>

[100] UNICEF, Ciberseguridad. [en línea]. 2020. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.unicef.org/mexico/ciberseguridad>

[101] INTERNET SEGURA FOR KIDS, Sexting. [en línea]. 2020. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.is4k.es/necesitas-saber/sexting>

- Denunciar: Si el usuario tiene un modo para obtener pruebas de la situación, es importante recopilar estas pruebas y denunciar ante las autoridades correspondientes de cada país.
- Apoyo psicológico: Solicitar apoyo psicológico de profesionales es fundamental para orientar emocionalmente a la persona víctima.

5.4.1.3.2 Ciberacoso (*cyberbullying*). De acuerdo con el portal especializado *StopBullying* del Gobierno de los Estados Unidos, la práctica del ciberacoso se centra en el uso de medios digitales con el propósito de acosar psicológicamente a otras personas, mediante prácticas como amenazas, hostigamientos o humillaciones a través de la difusión de contenidos perjudiciales, negativos, crueles o falsos de la víctima.

Los medios más utilizados para las actividades de ciberacoso suelen ser las redes sociales como *Instagram, Facebook y TikTok*, los mensajes de texto, herramientas de chat como *WhatsApp* y *Messenger*, foros en internet, correo electrónico y comunidades de videojuegos en la red[102].

5.4.1.3.2.1 Recomendaciones para prevenir el ciberacoso. De acuerdo con stopbullying.gov, en el caso de los menores de edad es fundamental que los padres estén al tanto de la actividad de sus hijos en la red. Esto derivado del hecho de que sin saberlo el menor podría ser víctima o acosador. Por otra parte, algunas señales comunes que suelen presentar los menores que estén padeciendo ciberacoso van desde un aumento o disminución notable en el uso de dispositivos electrónicos, que el menor trate de ocultar la pantalla cuando otras personas están cerca, hábitos de crear nuevas y eliminar frecuentemente las cuentas en redes sociales, la reducción en el interés en participar en situaciones sociales y casos de depresión[103].

Ante un caso de ciberacoso, es importante seguir algunas recomendaciones:

- Prestar atención: Identificar cambios de humor o comportamiento en el menor.
- Hablar: Preguntar al menor para conocer de primera mano que puede estar sucediendo y desde que momento se está presentando si es el caso.
- Documentar: Llevar un registro de lo que está ocurriendo y en dónde. Obtener capturas de pantalla de publicaciones y demás evidencias.
- Denunciar: Denunciar casos ante las plataformas y ante las autoridades correspondientes si es el caso.
- Apoyo: Brinde apoyo emocional al menor y busque ayuda psicológica de profesionales si es el caso.

---

[102] GOBIERNO DE ESTADOS UNIDOS, Qué es el Ciberacoso. [en línea]. 2021. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://espanol.stopbullying.gov/acoso-por-internet-1yqc/qu%C3%A9-es>

[103] GOBIERNO DE ESTADOS UNIDOS, Prevenir el Ciberacoso. [en línea]. 2021. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://espanol.stopbullying.gov/acoso-por-internet-1zqb/prevenci%C3%B3n>

5.4.1.3.3 *Grooming*. De esta manera se conoce la manera en la que personas se acercan a jóvenes y niños con el propósito de ganar su confianza, a través de la creación de lazos emocionales para poder abusar sexualmente de ellos. Puede ocurrir a través de internet o en persona y para lograrlo, normalmente el *groomer* invierte importantes cantidades de tiempo para lograr obtenerla confianza de los menores y de sus familias. Habitualmente, el atacante finge ser quien no es realmente, ofrece una falsa comprensión y consejos, entrega regalos, brinda atención y se vale de su posición económica y profesional.

El atacante normalmente suele también utilizar varios perfiles falsos en redes sociales para hacerse pasar por niños o adolescentes para generar una relación de amistad y confianza con el menor que quiere acosar[104].

5.4.1.3.3.1 Recomendaciones para prevenir el *grooming*. De acuerdo con la Fundación Red Contra el Abuso Sexual, algunas recomendaciones que en familia pueden seguirse para prevenir el *grooming* son[105]:

- No utilizar la tecnología como un medio para generar paz emocional. En vez de ello, es importante que el menor aprenda como controlar sus emociones mediante técnicas de respiración o conversaciones de confianza en familia.
- Incitar al menor a realizar actividades al aire libre.
- Establecer límites de tiempo en el uso de pantallas.
- No utilizar dispositivos electrónicos al menos una hora antes de irse a dormir para garantizar descansos eficientes.
- Involucrarse en el entorno digital del menor para conocer con quien está teniendo contacto habitualmente.
- Si se requiere, buscar ayuda de profesionales como psicólogos quienes contribuirán a determinar causas de problemas relacionados con la red.
- No permitir el uso de plataformas como Instagram, *WhatsApp, Tumblr, TikTok, Twitter, Facebook* y similares a menores de 13 años.

[104] GOBIERNO DE ARGENTINA, Grooming. [en línea]. 2021. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.argentina.gob.ar/grooming>

[105] FUNDACIÓN RED CONTRA EL ABUSO SEXUAL, Tips para Prevenir el Grooming en Casa. [en línea]. 2021. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://redcontraelabusosexual.org/tips-para-prevenir-el-grooming-en-casa/>

5.4.1.4 Riesgos de aplicaciones y red. En el uso del día a día existen amenazas que también se enfocan en las herramientas de *software* y de *hardware* que pueden potencialmente representar una vulnerabilidad para la información tanto familiar como la de una organización. En este orden de ideas, diferentes tipos de virus podrían afectar el funcionamiento o la integridad de la información presente en los equipos y dar lugar a robos de información, robos de contraseñas y generar además comportamientos anormales en los sistemas.

5.4.1.4.1 *Malware*. De acuerdo con Avast, el *malware* se refiere a cualquier tipo de software malicioso ("***mal****icious soft****ware***"), diseñado con el propósito de infiltrar los dispositivos sin autorización. Habitualmente trabaja en segundo plano y es difícil de detectar, pudiendo afectar los sistemas desde aspectos simples como generar malfuncionamientos y ralentizaciones, hasta captar datos para robo de identidad o secuestro de información.

En cuanto a su alcance, no existen dispositivos inmunes al *malware*. *Smartphones Android*, o *iOS*, computadoras *Windows, Linux o Mac* o en general cualquier dispositivo que contenga piezas de *software* pueden ser infiltrados potencialmente por este tipo de *software* malicioso. Para saber si un dispositivo está infectado, es posible detectar ocasionalmente síntomas como funcionamientos más lentos de lo habitual, falta injustificada de espacio de almacenamiento, presencia de ventanas emergentes y programas no deseados, entre otros[106].

Existen diferentes tipos de malware que se pueden separar en varias categorías de acuerdo con su funcionamiento.

- *Ransomware*: Es posiblemente uno de los más terribles tipos de malware ya que se enfocan en secuestrar la información de un equipo encriptándola y mostrando en pantalla un mensaje al usuario con una nota de rescate en la que normalmente solicitan el pago de alguna compensación económica para recuperar la información. En estos casos, normalmente, cuando un usuario se decide a pagar lo que va a ocurrir es que va a perder su dinero dado que el atacante no está interesado en devolver la información[107].

- *Spyware* (*software* espía): Se encarga de capturar información sobre una red o un dispositivo para enviársela al atacante. Información como datos personales, contraseñas, datos financieros, números de tarjetas de crédito suelen resultar atractivas para cometer fraudes o robar la identidad de las personas[108].

[106] AVAST, ¿Qué es el Malware?. [en línea]. 2022. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.avast.com/es-es/c-malware>
[107] AVAST, Guía Esencial Sobre el Ransomware. [en línea]. 2022. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.avast.com/es-es/c-what-is-ransomware>
[108] PANDA SECURITY, Spyware. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.pandasecurity.com/es/security-info/spyware/>

- Gusanos: Uno de los primeros tipos de virus conocidos y que se encarga básicamente de infectar a más equipos y de auto replicarse. Normalmente los gusanos se encargan de llevar otros tipos de *malware* a las máquinas infectadas[109].

- *Adware*: Este tipo de *malware* se encarga de instalar herramientas que muestran publicidad no deseada para el usuario en los navegadores con el propósito de generar ingresos para el atacante. De igual manera, suelen también capturar datos de los usuarios para mostrar más publicidad y la principal forma de instalarse es mediante engaños al usuario haciéndole creer que está instalando otras herramientas[110].

- Troyanos: Es un tipo de *malware* que engaña al usuario haciéndole creer que está instalando un software legítimo. Una vez instalado el *software* aparentemente legítimo, el *malware* se activa y puede realizar tareas como descargar más paquetes de virus, robar datos, etc. Puede llegar por lugares como correos electrónicos, descargas y páginas clon aparentemente legítimas. Por ello, si alguna vez un usuario recibe correos electrónicos con archivos adjuntos con extensiones .exe, .vbs o .bat, seguramente se trate de este tipo de programas maliciosos[111].

- *Botnets* (redes de robots): Mediante los *botnets*, los atacantes se encargan de capturar equipos para poder controlarlos de manera remota. De esta manera, el atacante puede realizar acciones como enviar *spam*, robar datos a terceros, coordinar ataques de denegación de servicio (DDos) y demás[112].

5.4.1.4.2 Interceptación de datos. Este tipo de ataques se conocen también como *"man in the middle"* (hombre en medio), y se basa en interceptar la comunicación que se realiza entre 2 o más interlocutores, ya sea suplantando la identidad de uno de ellos o a través de dispositivos técnicos que capturen la información que circula por una red. Este tipo de ataques es habitual encontrarlos en redes wifi-públicas como las que se suministran en aeropuertos y centros comerciales, o incluso a un nivel más sofisticado con la instalación de dispositivos en un punto de una red cableada[113].

5.4.1.5 Riesgos sociales

---

[109] AVAST, ¿Qué es un Gusano Informático?. [en línea]. 2022. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.avast.com/es-es/c-computer-worm>

[110] MALWAREBYTES, Adware. [en línea]. 2022. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://es.malwarebytes.com/adware/>

[111] KASPERSKY, ¿Qué es un Troyano y Qué Daño Puede Causar?. [en línea]. 2022. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://latam.kaspersky.com/resource-center/threats/trojans>

[112] AVG ANTIVIRUS, ¿Qué es una Botnet y Cómo Puede Proteger Su Ordenador?. [en línea]. 2022. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.avg.com/es/signal/what-is-botnet>

[113] INSTITUTO NACIONAL DE CIBERSEGURIDAD, El Ataque Del "Man In The Middle" en la Empresa, Riesgos y Formas de Evitarlo. [en línea]. 2020. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo>

5.4.1.5.1 Ingeniería social. Un popular adagio reza que una cadena es tan fuerte como su punto más débil. En este sentido y en cuanto a ciberseguridad, el punto más débil son precisamente los usuarios. Es por ello, que la ingeniería social es la técnica más utilizada por los atacantes para engañar a los usuarios para lograr que les brinden accesos, o que les entreguen datos confidenciales para lograr infectar sus equipos de cómputo con *malware*. Una de las maneras principales con las que se logra acceder a una red corporativa suele ser contactar a alguno de los empleados de la organización haciéndose pasar por algún técnico de soporte o similar y aprovechar la buena fe del empleado para lograr su cometido. De igual modo, en las familias también es posible lograr este tipo de ataques a través de la identificación del flanco más débil[114].

5.4.1.5.2 *Scam* – Estafas. Las estafas se basan en técnicas de ingeniería social y engaños más que en habilidades de delincuentes. Normalmente, el atacante contacta a la víctima ya sea por teléfono o por correo electrónico con el propósito de presentarle un beneficio. El pretexto puede ser que ganó un premio o que es beneficiario de algún programa exclusivo. Una vez la víctima accede o solicita más información, comienzan a solicitarle algunos datos para hacer parecer que todo es real, finalmente, cuando ya está todo listo, suelen solicitar algún tipo de remuneración para "los trámites", la cual evidentemente es hurtada[115].

5.4.1.5.3 Suplantación de identidad – *Phishing*. De acuerdo con Microsoft, se trata de un tipo de ataque en el que la víctima recibe un correo electrónico que contiene enlaces que redireccionan hacia un sitio web clonado de uno verdadero, este clon parece ser legítimo y habitualmente allí se solicita información como números de tarjetas de crédito, contraseñas, datos bancarios, entre otros.

Una forma de detectar este tipo de ataques es que habitualmente tienen un sentido de "urgencia", por lo que muchas veces indican a la persona que su cuenta bancaria fue bloqueada, o que ha sido notificado de una sanción por temas de tránsito y que para ver el monto debe descargar un archivo. Como se podrá notar, cualquier correo electrónico no esperado en el que soliciten que haga clic en algún lugar para realizar una acción, inmediatamente debe ser interpretado como sospechoso. Del mismo modo, cuando se reciben correos no esperados de remitentes poco frecuentes o por primera vez se debe desconfiar, incluso, en algunos casos temas como la mala ortografía delata a los delincuentes. Finalmente, debe revisarse cuidadosamente el dominio desde el cual se remite el correo electrónico, por ejemplo un banco enviaría una comunicación desde un correo similar a este: usuario@nombredemibanco.com, lo cual indicaría que al parecer es legítimo, sin embargo, si el correo viene desde una dirección que cualquiera puede crear como usuario_nombredemibanco@gmail.com, el hecho que termine en una

[114] KASPERSKY, Ingeniería Social: Definición. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering>

[115] PANDA SECURITY, Scam. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.pandasecurity.com/es/security-info/scam/>

dirección genérica como @gmail.com puede indicar que se trata de un atacante tratando de simular desde una cuenta convencional de Gmail que es un representante del banco[116].

5.4.1.5.4 *Vishing*. Este tipo de ataques es uno de los más conocidos en Latinoamérica. Simplemente se trata de una llamada telefónica sospechosa en donde un supuesto operador se identifica como empleado de una organización o empresa reconocida. Dado que habitualmente este tipo de atacantes ya han adquirido previamente de manera ilegal la información de los usuarios solo resta plantear al usuario una aparente situación difícil que requiere la cooperación de este último. Cuando el usuario percibe que efectivamente del otro lado de la línea tienen su información completa, suele entregar la información restante que le permita al atacante concretar su ataque.

Para enfrentar este tipo de ataques quizá la recomendación es muy simple: Cuando llamen al usuario, de organizaciones aparentemente legítimas conocidas por el o no a ofrecerle algo, simplemente debe preguntar de que se trata, si le piden como condición que suministre datos, o que digite claves a través del teclado del teléfono para poderle entregar la información, entonces simplemente el usuario debe manifestar que no está interesado y que si es tan urgente se dirigirá personalmente a las instalaciones de la empresa o que el mismo usuario marcará a los teléfonos oficiales[117].

5.4.1.5.5 *Smishing*. Al igual que en el caso del *Vishing*, se trata de un tipo de estafa. La diferencia radica en que esta se ejecuta normalmente a través de mensajes de texto. Aunque parezca increíble, una víctima puede recibir un mensaje en el que le indican que ingrese a alguna URL en internet, o más simple que ello, le pueden indicar que ganó un premio para un concurso en el que probablemente no se inscribió y que debe contactarse a una línea telefónica de un supuesto *call center.* Cuando la víctima se comunica, ya el resto es historia y puede remitirse al punto anterior (*vishing*) en donde el atacante por medio de la llamada ejecutará su ataque[118].

---

[116] MICROSOFT, Protéjase Del Phishing. [en línea]. 2022. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44#:~:text=El%20phishing%20es%20un%20ataque,que%20fingen%20ser%20sitios%20leg%C3%ADtimos.>

[117] OFICINA DE SEGURIDAD DEL INTERNAUTA, ¿Qué es el Vishing?. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-vishing#:~:text=Es%20un%20tipo%20de%20fraude,informaci%C3%B3n%20personal%20de%20sus%20v%C3%ADctimas.>

[118] TREND MICRO, ¿Qué es el Smishing?. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.trendmicro.com/es_es/what-is/phishing/smishing.html>

5.4.1.6 Riesgos de extorsión y explotación sexual. Muchos padres de familia suelen considerar que sus hijos están a salvo con el solo hecho de estar en casa todo el tiempo. Sin embargo, los tiempos han evolucionado y la penetración de internet en los hogares, aunque ofrece enormes ventajas para el desarrollo de la sociedad, también trae consigo la oportunidad para atacantes de entrar a los hogares haciendo uso de medios cibernéticos.

En este sentido, un atacante, simulando ser otra persona a través de perfiles falsos en redes sociales, podría llegar a entablar comunicación con los menores de edad de un hogar y a través de engaños hacer que crean tener una relación de confianza con el atacante quien podría pedirles realizar actividades ilícitas como solicitarles que se tomen fotografías de carácter pornográfico y se las envíen. Posteriormente, el atacante podría comenzar a chantajear a su víctima con ese material para obtener dinero o para intentar lograr que haga algo ilegal.

Para ello, una medida importante que los padres de familia deben considerar es mantenerse al tanto de quienes son las personas con las que tiene contacto sus hijos a través de redes sociales y verificar que esas personas existan en realidad[119].

5.4.2 Top estafas famosas comunes.

5.4.2.1 Tío – Tía - Primito. Este tipo de estafa resulta muy común y ya es bastante conocida en países latinos como Colombia. La modalidad es muy simple: Un día una persona recibe una llamada de un número desconocido en la que al azar una persona que dice ser su sobrino la quiere saludar. Para entablar confianza, el atacante le saluda y le cuestiona porque no se acuerda de el, de su sobrino favorito. Cuando la víctima avergonzada empieza a arrojar nombres el atacante solo debe seleccionar uno y seguir la conversación. Posteriormente, realiza otras llamadas para reafirmar el lazo emocional generado, y más adelante, hace una llamada final en la que le cuenta que está en problemas porque fue capturado en alguna carretera por la Policía por algo que no sabía y que debe sobornar al agente de turno. Es en ese momento en que el atacante le ruega a su víctima que le preste el dinero y que se lo regresa pronto, muchas veces las víctimas deciden transferir el dinero y es allí donde se concreta la estafa[120].

Para evitar caer en este tipo de estafas cibernéticas, cuando un usuario reciba una llamada de un supuesto sobrino simplemente debe arrojar un nombre al azar que no corresponda a su familia y allí se dará cuenta del timo. Por lo demás, aunque parezca

[119] FUNDACIÓN RED CONTRA EL ABUSO SEXUAL, Delitos Virtuales Contra Niños, Niñas y Adolescentes Aspectos Jurídicos. [en línea]. 2018. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://redcontraelabusosexual.org/delitos-virtuales-contra-ninos-ninas-y-adolescentes-aspectos-juridicos/>

[120] ALCALDÍA DE BOGOTÁ, No Caigas En Las Redes De Delincuentes, Conoce La Modalidad De Estafa 'tío-tía'. [en línea]. 2018. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://bogota.gov.co/mi-ciudad/seguridad/modalidad-de-estafa-tio-tia-en-bogota>

muy verdadero el contacto familiar, el usuario no se debe prestar para hacer transferencias de dinero.

5.4.2.2 Sorteos y becas. De acuerdo con la Comisión Federal de Comercio de Estados Unidos, este tipo de estafas cibernéticas comienzan con llamadas, correos electrónicos o mensajes de texto en los que le indican a la víctima que ha ganado un sorteo o una beca para estudiar en una prestigiosa universidad. Cuando la víctima intenta cobrar el premio, el estafador le va a indicar que debe pagar algún dinero por temas de trámites necesarios para poder realizar el cobro.

Para identificar este tipo de estafas, el usuario debe ser consciente que es imposible ganar un concurso de un sorteo en el que no está participando. Por otra parte, nadie debe pagar para obtener un premio y finalmente, en ningún concurso le van a pedir al ganador su información financiera para poder entregar el premio[121].

5.4.2.3 Herencias. También conocida como la "carta nigeriana", suele ser un correo electrónico enviado al azar en el que el atacante simula ser una persona con una enfermedad terminal que quiere donar todo su dinero a causas sociales en el país en el que usted se encuentra. Para ello le solicita simplemente que envíe sus datos como nombres, dirección, país, edad, teléfono. Cuando la víctima envía sus datos, el atacante solicita la información bancaria y le pide a la víctima que consigne simplemente los valores necesarios para realizar el trámite. Aunque no parezca, muchas personas consignan los montos solicitados creyendo ingenuamente que en verdad van a recibir esos dineros prometidos[122].

5.4.3 Herramientas.

5.4.3.1 Gestión de contraseñas. Gestionar contraseñas diferentes para tantas plataformas que los usuarios manejan en la actualidad suele ser difícil. Por ello, una práctica fácil tomada por muchos es utilizar la misma contraseña para todos los servicios. Esta, se considera una práctica terrible, ya que, si se presenta una fuga de información en alguno de los servicios registrados, la contraseña será visible para cualquier atacante. Para realizar una mejor gestión de contraseñas, existen herramientas capaces de custodiar las diferentes credenciales de inicio de sesión para todos los servicios de manera segura, de esta manera el usuario no tendrá que recordar las diferentes contraseñas creadas para cada servicio.

[121] ESTADOS UNIDOS. COMISIÓN FEDERAL DE COMERCIO, Estafas De Premios, Sorteos Y Loterías Falsas. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://consumidor.ftc.gov/articulos/estafas-de-premios-sorteos-y-loterias-falsas>

[122] POLICÍA NACIONAL DE COLOMBIA, Carta Nigeriana Herencia. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://caivirtual.policia.gov.co/contenido/carta-nigeriana-herencia>

En este caso, servicios gratuitos y de pago como *1Password, LastPass, Dashlane, KeePass, Enpass, Keeper, Bitwarden,* entre otros le permitirán al usuario administrar sus contraseñas de manera sencilla y segura[123].

5.4.3.2 Control parental. Supervisar y controlar la actividad realizada por los menores en la red y en los dispositivos electrónicos como computadores y *smartphones* es fundamental para garantizar que están a salvo de peligros cibernéticos.

Para ello, existen herramientas reconocidas a nivel mundial tanto gratuitas como de pago que le permitirán a un padre de familia controlar la actividad de sus hijos en la red. Es el caso de plataformas como *Qustodio, Secure Kids, Norton Family, Microsoft Family Safety, ESET Parental Control, Panda Dome Family, Google Family Link, Kidoz* entre otras[124].

5.4.3.3 Hábitos de Protección de datos. Descargar la responsabilidad de protección de la información en herramientas informáticas únicamente no es una buena opción, de hecho, en este mismo análisis se ha comentado que es a través de los usuarios principalmente en donde se presentan los mayores problemas de seguridad. Por ello, hábitos como actualizar regularmente el *software* de los dispositivos, revisar los permisos que solicitan las aplicaciones al instalarlas, estar atento a los cambios en las políticas de privacidad de las aplicaciones, utilizar las herramientas de doble factor de autenticación cuando se encuentren disponibles, verificar antes de reenviar contenidos engañosos, modificar regularmente las contraseñas, contar con copias de seguridad de la información y ser desconfiado con las solicitudes recibidas se convierten en buenos hábitos para limitar la posibilidad de ser *hackeado*[125].

5.4.3.4 Navegación segura *HTTPS*. Anteriormente, los sitios web utilizaban el protocolo *HTTP* para comunicar la información en los sitios web. Con el pasar del tiempo, se encontró que este protocolo por sí mismo no era completamente seguro, ya que la información no se encriptaba de ninguna manera. Es de esta manera que nace el protocolo *HTTPS* el cual se encarga de resolver este inconveniente. Para asegurarse de estar navegando en internet a través de *HTTPS*, simplemente, el usuario debe verificar que el acceso al sitio web inicia con *https://*[126].

---

[123] FERNÁNDEZ, Yubal. Gestores De Contraseñas: Qué Son, Cuáles Son Los Más Importantes Y Cómo Utilizarlos. [en línea]. 2020. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.xataka.com/basics/gestores-contrasenas-que-cuales-populares-como-utilizarlos>

[124] ETAPA INFANTIL, 10 Herramientas De Control Parental Para Mantener A Salvo A Tu Hijo En Internet. [en línea]. 2020. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.etapainfantil.com/herramientas-control-parental-internet>

[125] EL TIEMPO, Hábitos Simples Para Proteger Su Información En Internet. [en línea]. 2019. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/8-habitos-simples-para-proteger-su-informacion-en-internet-317734>

[126] ESPINOZA, Oscar. Descubre Cómo Funciona HTTPS Con Esta Infografía. [en línea]. 2019. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.redeszone.net/tutoriales/internet/como-funciona-https/>

5.4.3.5 *VPN*. Conocida como Red Privada Virtual (*Virtual Private Network* en inglés), es una tecnología que se encarga de permitir que una o varias computadoras se conecten a una red de manera privada por medio de internet. Un ejemplo sencillo de comprender es el caso en el que el usuario debe conectarse a una red *wifi* pública en un aeropuerto o centro comercial. En ese lugar tan concurrido es altamente posible que un atacante este capturando toda la información que circula a través del aire y que en muchos casos no tiene un proceso de cifrado. Es en ese momento en el que realizar una conexión a través de una red *VPN* fortalece la seguridad de las comunicaciones dado que dicha información ahora va a circular encriptada y va a ser ilegible para el atacante.

Al momento de adquirir un servicio de *VPN*, lo mejor es asegurarse de utilizar uno que sea de pago, para garantizar que la información efectivamente va a ser privada. En el mercado existen varias soluciones como *ExpressVPN, NordVPN, CyberGhost* o incluso realizar una implementación propia en un servidor administrado por el usuario con *Outline*[127].

5.4.3.6 Antivirus. Un *software* antivirus es un programa enfocado en escanear, detectar y eliminar virus informáticos. En este caso, es muy importante comprender que el software antivirus gratuitos tienen una muy baja o incluso nula efectividad, por lo que siempre se recomienda utilizar software antivirus de pago. En este orden de ideas, existen herramientas como *McAfee Total Protection, Kaspersky Total Security, Norton 360, Nod32*, entre otras[128].

[127] VPN OVERVIEW, Los Mejores Proveedores De VPN Del Año 2022. [en línea]. 2022. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://vpnoverview.com/es/mejores-proveedores-vpn/mejores-servicios-vpn/>

[128] CONTRERAS, Manuel. Estos Son Los Mejores Antivirus De Pago Que Puedes Comprar Para Tu Ordenador. [en línea]. 2020. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://computerhoy.com/listas/tecnologia/estos-son-mejores-antivirus-pago-puedes-comprar-ordenador-windows-591171>

6 CONCLUSIONES

La consulta de distintas fuentes de información mediante el estado del arte en materia de ciberseguridad determinó que en el contexto familiar los menores de edad se encuentran mayormente expuestos a riesgos de ciberseguridad como el ciberacoso, *grooming* y situaciones en las que podrían autoinfligirse daño a causa de retos (*challenges*) debido a la corta experiencia y limitado sentido común ante las amenazas derivado de su corta edad.

Con la revisión de los riesgos de ciberseguridad a los que se encuentra expuesta una persona y sus afectaciones, se encontró la existencia de efectos secundarios relacionados con algunas personas adultas, quienes luego de sufrir situaciones como estafas a través de medios digitales, han presentado casos de dolores severos de cabeza, alteraciones del sueño, cambios del estado de ánimo y cansancio, irradiando una sensación de intranquilidad hacia su entorno cercano.

Con la realización de esta revisión documental se determinó que la actividad que realizan los usuarios en internet deja rastros digitales que se consideran prácticamente imposibles de eliminar. Opiniones publicadas, imágenes, videos, *clicks* en botones “me gusta” de diferentes plataformas, dispositivos utilizados y tiempos de uso dejan registros en las plataformas sobre los cuales ningún usuario tiene garantía de poder eliminarlo si lo solicita. Además de ello, mucha de esta información es capaz de ser obtenida de manera legal o ilegal y ser difundida en la *dark web*, desde donde podría ser obtenida por un potencial atacante para planear y ejecutar un ataque contra el usuario, por lo cual, es importante limitar tanto como sea posible el uso y difusión de información personal a través de todo tipo de plataformas en internet.

Durante el análisis de casos reales relacionados con ciberdelitos, se revisó el consolidado de denuncias por delitos cibernéticos presentadas ante la Fiscalía General de Colombia, en donde se identificó que la mayor cantidad de casos presentados fueron en personas entre los 29 a 59 años de edad, con una predominancia en casos presentados entre las mujeres, siendo el hurto por medios informáticos, accesos abusivos a sistemas de información, violación de datos personales y la transferencia no consentida de información los principales puntos de dolor entre los denunciantes.

Se identificó que existen tipos de delitos cibernéticos que se enfocan en atacar el círculo social y familiar de las víctimas como el *phising*, en donde los atacantes suelen simular situaciones como detenciones policiales, favores con falsos inconvenientes con entidades gubernamentales y suplantaciones de identidad. El objetivo de este tipo de ataques es solicitar algún tipo de compensación económica al mencionado círculo familiar y social de una persona mediante engaños.

Durante la formulación de las recomendaciones de ciberseguridad y buenas prácticas, se encontró que es importante que los padres de familia estén al tanto de la actividad que

realizan sus hijos menores de edad en internet a través de todas las plataformas disponibles, así como del círculo social frecuentado por los menores en las mismas y de los temas tratados. Esto para prevenir situaciones como *sexting* y *grooming* en donde los menores podrían enviar material explícito atendiendo a retos o para detectar tempranamente situaciones de ciberacoso.

Se determinó que, aunque todas las edades están expuestas a casos de *sexting* y ciberacoso, los principales puntos de dolor entre los adultos están relacionados con las estafas, las cuales suelen darse principalmente a través de ingeniería social en donde una persona puede ser engañada a través de correo electrónico, mensajes de texto o llamadas telefónicas ya sea para que entregue credenciales de accesos a sistemas o para que simplemente realice transferencias de dinero a los atacantes.

7 RECOMENDACIONES

Ampliar el análisis del estado del arte en materia de ciberseguridad con el que se permita actualizar la lista de riesgos, tendencias cibernéticas y la legislación vigente tanto para la protección de los usuarios como para los castigos a quienes cometan delitos relacionados con los mismos.

Actualizar periódicamente la lista de riesgos de ciberseguridad con los que se permita incluir los nuevos peligros que naturalmente van naciendo o que van evolucionando en proporción a la creación de nuevas tecnologías, haciendo un especial énfasis en aquellos que podían irradiarse hacia el entorno social y/o familiar cercano de las potenciales víctimas.

Realizar actividades que permitan fomentar las denuncias realizadas por víctimas de delitos cibernéticos ante las autoridades competentes para que se puedan obtener datos aún más precisos de casos reales que puedan ser utilizados como insumos para la realización de estudios y creación de leyes de protección de los usuarios. De la misma manera, es fundamental la creación de un canal de apoyo psicosocial desde el que se pueda apoyar emocionalmente a las víctimas de delitos cibernéticos y su entorno familiar.

Difundir este análisis con sus recomendaciones de seguridad, buenas prácticas y herramientas, como un medio enfocado en la prevención para fortalecer la ciberseguridad en sus aspectos más destacados dentro del entorno familiar y social del lector.

8 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de CONSTRUCCIÓN DE UN DOCUMENTO DE RECOMENDACIONES DE CIBERSEGURIDAD PARA EL ENTORNO FAMILIAR, puedan acceder al documento.

BIBLIOGRAFÍA

ABC DATOS, Riesgos De Ciberseguridad Para Los Menores De Edad. [en línea]. Ciberseguridad. 2021. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.abcdatos.com/blog/riesgos-de-ciberseguridad-para-los-menores-de-edad/>

ACIS, Un 600% Ha Aumentado Los Ciberdelitos En Pandemia, ¡asegúrese Para Iniciar El 2021! . [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://acis.org.co/portal/content/noticiasdelsector/un-600-ha-aumentado-los-ciberdelitos-en-pandemia-%C2%A1aseg%C3%BArese-para-iniciar-el-2021>

ACOSTA ARGOTE, Cristian. Un 69,8% De Las Personas No Denuncia Los Delitos Ante Las Autoridades Según Informe Del DANE. [en línea]. Asuntos Legales Diario La República. 2021. [Citado en 15 de Mayo de 2021]. Disponible en internet: <https://www.asuntoslegales.com.co/actualidad/un-698-de-las-personas-no-denuncia-los-delitos-ante-las-autoridades-segun-el-dane-3131619>

ALCALDÍA DE BOGOTÁ, No Caigas En Las Redes De Delincuentes, Conoce La Modalidad De Estafa 'tío-tía'. [en línea]. 2018. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://bogota.gov.co/mi-ciudad/seguridad/modalidad-de-estafa-tio-tia-en-bogota>

ÁLVAREZ TABARES, Omar Julián. y RODRÍGUEZ GUERRA, Elquis. El Uso De La Internet Y La Influencia En La Comunicación Familiar. Diciembre, 2012. Vol. 7. No. 7., p.11-21.

ANDI, ANDI Presentó Los Resultados De La Encuesta De Transformación Digital . [en línea]. Noticias. 2019. [Citado en 15 de Marzo de 2021]. Disponible en internet: <http://www.andi.com.co/Home/Noticia/15609-andi-presento-los-resultados-de-la-encu>

ANDERSON, Emma Louise. y STEEN, Eloisa. Internet Use And Problematic Internet Use: A Systematic Review Of Longitudinal Research Trends In Adolescence And Emergent Adulthood. [en línea]. 2017. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.tandfonline.com/doi/full/10.1080/02673843.2016.1227716>

ASIÁN, Arantxa. 5 Trucos Para Sacarle El Máximo Provecho A Youtube Kids. [en línea]. Tu Experto Apps. 2019. [Citado en 15 de Mayo de 2021]. Disponible en internet: <https://www.tuexpertoapps.com/2019/02/07/5-trucos-para-sacarle-el-maximo-provecho-a-youtube-kids/>

AVAST, ¿Qué es el Malware?. [en línea]. 2022. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.avast.com/es-es/c-malware>

AVAST, ¿Qué es un Gusano Informático?. [en línea]. 2022. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.avast.com/es-es/c-computer-worm>
AVAST, Ingeniería Social . [en línea]. Otras Amenazas. 2020. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.avast.com/es-es/c-social-engineering>

AVG ANTIVIRUS, ¿Qué es una Botnet y Cómo Puede Proteger Su Ordenador?. [en línea]. 2022. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.avg.com/es/signal/what-is-botnet>

BANCOLOMBIA, Guía Para Entender La Transformación Digital En Colombia. [en línea]. Reset. 2020. [Citado en 15 de Marzo de 2021]. Disponible en internet: <https://resetmarketingdigital.com/guia-transformacion-digital-en-colombia>

BBC NEWS, El Virus Que Tomó Control De Mil Máquinas Y Les Ordenó Autodestruirse. [en línea]. 2015. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet>

BBC MUNDO, ¿Qué Hacer Si Publican Una Foto Tuya En Internet Sin Tu Permiso?. [en línea]. 2017. [Citado en 12 de Marzo de 2022]. Disponible en internet: <https://www.bbc.com/mundo/noticias-37896303>

BLU RADIO, Cayeron Los Call Center: Estafaron A Más De 6.900 Personas Con Venta Ficticia De Servicios Bancarios. [en línea]. 2021. [Citado en 12 de Marzo de 2022]. Disponible en internet: <https://www.bluradio.com/judicial/cayeron-los-call-center-estafaron-a-mas-de-6-900-personas-con-venta-ficticia-de-servicios-bancarios>

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACION CCIT, Tendencias Del Cibercrimen En Colombia 2019-2020. [en línea]. Estudios. 2019. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/>

CAPITAL MÉXICO, Casos Más Graves Del Robo De Identidad. [en línea]. 2017. [Citado en 13 de Marzo de 2022]. Disponible en internet: <https://www.capitalmexico.com.mx/especial/casos-mas-graves-del-robo-de-identidad-sat-adeudos-fiscales/>

CENTRO CIBERNÉTICO POLICIAL COLOMBIA, Balance Cibercrimen 2020. [en línea]. 2021. [Citado en 20 de Agosto de 2022]. Disponible en internet: <https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf>

CISCO, ¿Qué es la Ciberseguridad?. [en línea]. 2021. [Citado en 13 de Marzo de 2022]. Disponible en internet: <https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~how-cybersecurity-works>

CCF GLOBAL, ¿Qué Es Un Computador?. [en línea]. 2020. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://edu.gcfglobal.org/es/informatica-basica/que-es-un-computador/1/>

CLARO, ¿Qué Son Las TIC? Y ¿Por Qué Son Tan Importantes?. [en línea]. 2019. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.claro.com.co/institucional/que-son-las-tic/>

COLEGIO DE MICHOACÁN, Internet. [en línea]. 2019. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.colmich.edu.mx/computo/files/internet.pdf>

COLOMBIA. DANE, Indicadores Básicos De Tic Hogares. [en línea]. Tic. 2019. [Citado en 20 de Marco de 2021]. Disponible en internet: <https://www.dane.gov.co/index.php/estadisticas-por-tema/tecnologia-e-innovacion/tecnologias-de-la-informacion-y-las-comunicaciones-tic/indicadores-basicos-de-tic-en-hogares#regional>

COLOMBIA. DANE, Proyecciones De Población. [en línea]. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/proyecciones-de-poblacion>

COLOMBIA. ESCUELA TIC FAMILIA, ¿Qué Actividades Puedo Realizar en Internet?. [en línea]. 2018. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.escuelaticfamilia.gov.co/648/w3-article-71538.html>

COLOMBIA. MINTIC, Boletín Trimestral De Las TIC Tercer Trimestre De 2020. [en línea]. Estadísticas. 2021. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://colombiatic.mintic.gov.co/679/articles-161478_presentacion_cifras.pdf>

COLOMBIA. MINTIC, En TIC Confío + . [en línea]. Otras Amenazas. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.enticconfio.gov.co/quienes-somos>

COLOMBIA. MINTIC, Internet, ¿Qué Es? ¿para Qué Sirve?. [en línea]. 2020. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.enticconfio.gov.co/internet-que-es-para-que-sirve>

COLOMBIA. MINTIC, Ministra De TIC Hace Balance De La Conectividad Durante La Pandemia. [en línea]. Mintic En Los Medios. 2020. [Citado en 15 de Marzo de 2021]. Disponible en internet: <https://webcache.googleusercontent.com/search?q=cache:BYeClyJvTRUJ:https://www.mintic.gov.co/portal/604/w3-article-145946.html>

COLOMBIA. MINTIC, Min TIC Capacitará A 1,8 Millones De Colombianos En Habilidades Digitales. [en línea]. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/161930:Min-TIC-capacitara-a-1-8-millones-de-colombianos-en-habilidades-digitales>

COLOMBIA. MINTIC, Tecnologías De La Información Y Las Comunicaciones (tic). [en línea]. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.mintic.gov.co/portal/inicio/5755:Tecnolog-as-de-la-Informaci-n-y-las-Comunicaciones-TIC>

COMISION FEDERAL DE COMERCIO DE LOS ESTADOS UNIDOS, Estafas Por Teléfono. [en línea]. Estafas. 2019. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.consumidor.ftc.gov/articulos/s0076-estafas-por-telefono>

CONTRERAS, Manuel. Estos Son Los Mejores Antivirus De Pago Que Puedes Comprar Para Tu Ordenador. [en línea]. 2020. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://computerhoy.com/listas/tecnologia/estos-son-mejores-antivirus-pago-puedes-comprar-ordenador-windows-591171>

CORPORACIÓN HÁBITAT PARA LA HUMANIDAD MÉXICO, La Familia Como Base De La Sociedad. [en línea]. 2021. [Citado en 13 de Marzo de 2022]. Disponible en internet: <https://www.habitatmexico.org/article/la-familia-como-base-de-la-sociedad>

DATOS PROTEGIDOS, No Tengo Nada Que Ocultar: La Falacia De La Privacidad. [en línea]. 2015. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://datosprotegidos.org/no-tengo-nada-que-ocultar-la-falacia-de-la-privacidad/>

DEBITOOR, Pago Online. [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://debitoor.es/glosario/pago-online>

DEFINICIÓN.DE, Definición De Teléfono. [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://definicion.de/telefono/>

DE PEDRO, Sandra. La Ciberseguridad Como Responsabilidad Social. [en línea]. Blog. 2019. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://gaptain.com/blog/la-ciberseguridad-como-responsabilidad-social/>

DIARIO ABC, Internet No Es El Enemigo: 7 Beneficios Del Uso De Las Nuevas Tecnologías Que Evitamos Admitir. [en línea]. Educación. 2020. [Citado en 15 de Marzo de 2021]. Disponible en internet: <https://www.abc.es/familia/educacion/abci-internet-no-enemigo-7-beneficios-nuevas-tecnologias-evitamos-admitir-202001301416_noticia.html>

DIARIO EL UNIVERSAL, Tres Historias, Misma Tragedia. [en línea]. 2017. [Citado en 13 de Marzo de 2022]. Disponible en internet:

<https://www.eluniversal.com.mx/articulo/cartera/finanzas/2015/09/28/robo-de-identidad-tres-historias-misma-tragedia>

DIARIO LA VANGUARDIA, Denuncian A Google Por Contenido Inapropiado En Youtube Kids. [en línea]. Tecnología. 2015. [Citado en 15 de Mayo de 2021]. Disponible en internet: <https://www.lavanguardia.com/tecnologia/redes-sociales/youtube/20150407/54429717715/denuncia-google-youtube-kids.html>

EL ESPECTADOR, En 2020 Se Profesionalizaron Los Delitos En La Web Y Crecieron En Un 84%. [en línea]. Judicial. 2020. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.elespectador.com/noticias/judicial/los-ciberdelitos-aumentaron-un-84-durante-2020-policia/>

EL HERALDO, Alertan Aumento De Hackeo A Correos Y Redes Sociales. [en línea]. 2020. [Citado en 12 de Marzo de 2022]. Disponible en internet: <https://www.elheraldo.co/judicial/alertan-aumento-de-hackeo-correos-y-redes-sociales-738973>

EL TIEMPO, El Testimonio De Una Víctima De Estafadores A Través De 'call Center'. [en línea]. 2021. [Citado en 12 de Marzo de 2022]. Disponible en internet: <https://www.eltiempo.com/justicia/delitos/estafa-testimonio-de-victima-que-robaron-a-traves-de-call-center-595708>

EL TIEMPO, Hábitos Simples Para Proteger Su Información En Internet. [en línea]. 2019. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/8-habitos-simples-para-proteger-su-informacion-en-internet-317734>

EL TIEMPO, Los Riesgos De Exponer Datos Personales En Internet. [en línea]. Tecnósfera. 2020. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/riesgos-de-exponer-datos-personales-en-internet-557397>

EL TIEMPO, Panorama De Colombia Frente A La Transformación Digital. [en línea]. Transformación Digital. 2020. [Citado en 15 de Marzo de 2021]. Disponible en internet: <https://www.eltiempo.com/mas-contenido/panorama-de-colombia-frente-a-la-transformacion-digital-550807>

EN TIC CONFÍO, ¿Qué Son Y Para Qué Sirven Las Tic ?. [en línea]. Pedagoría. 2015. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.enticconfio.gov.co/que-son-y-para-que-sirven-las-tic->

ESET, ¿Qué Es Un Macro Virus Y Cómo Funciona?. [en línea]. 2014. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.welivesecurity.com/la-es/2014/06/13/que-es-macro-virus-como-funciona/>

ESET, Elk Cloner: La Cápsula Del Tiempo. [en línea]. 2009. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.welivesecurity.com/la-es/2009/08/11/elk-cloner-capsula-tiempo/>

ESET, Mafiaboy: 20 Años De Uno De Los Primeros Ataques Documentados Del Tipo Dos. [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.welivesecurity.com/la-es/2020/02/10/mafiaboy-20-anos-primeros-ataques-denegacion-servicio/>

ESPARÍS FIGUEIRA, Martín. Ciberdelincuencia: Los Delitos Informáticos Más Comunes. [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.sistemius.com/ciberdelincuencia-4-tipos-de-delitos-informaticos/>

ESPINOZA, Oscar. Descubre Cómo Funciona HTTPS Con Esta Infografía. [en línea]. 2019. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.redeszone.net/tutoriales/internet/como-funciona-https/>

ESTADOS UNIDOS. COMISIÓN FEDERAL DE COMERCIO, Estafas De Premios, Sorteos Y Loterías Falsas. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://consumidor.ftc.gov/articulos/estafas-de-premios-sorteos-y-loterias-falsas>

ETAPA INFANTIL, 10 Herramientas De Control Parental Para Mantener A Salvo A Tu Hijo En Internet. [en línea]. 2020. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.etapainfantil.com/herramientas-control-parental-internet>

FEDERAL BUREAU OF INVESTIGATION (FBI), Internet Crime Report 2020. [en línea]. 2021. [Citado en 11 de Marzo de 2022]. Disponible en internet: <https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf>

FERNÁNDEZ DE MARCOS, Laura Davara. Formación TIC (redes Sociales, Internet, Ciberseguridad, Big Data, Etc.) En Casa, En El Colegio, En La Universidad Y En La Empresa: Características, Razón De Ser Y Contenido . [en línea]. Revista Tecnología, Ciencia Y Educación N.º 12 Enero-abril 2019 . 2019. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.tecnologia-ciencia-educacion.com/index.php/TCE/article/view/243>

FERNÁNDEZ DELGADO, Darío. Aprender en Familia, Una Experiencia Enriquecedora. [en línea]. 2020. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.linkedin.com/pulse/aprender-en-familia-una-experiencia-enriquecedora-mariposas-colombia/?originalSubdomain=es>

FERNÁNDEZ, Yubal. Gestores De Contraseñas: Qué Son, Cuáles Son Los Más Importantes Y Cómo Utilizarlos. [en línea]. 2020. [Citado en 16 de Marzo de 2022].

Disponible en internet: <https://www.xataka.com/basics/gestores-contrasenas-que-cuales-populares-como-utilizarlos>

FISCALÍA COLOMBIA, Conteo De Víctimas. [en línea]. Datos Abiertos. 2021. [Citado en 25 de Abril de 2020]. Disponible en internet: <https://www.datos.gov.co/Justicia-y-Derecho/Conteo-de-V-ctimas/sft7-9im5>

FUNDACIÓN RED CONTRA EL ABUSO SEXUAL, Delitos Virtuales Contra Niños, Niñas y Adolescentes Aspectos Jurídicos. [en línea]. 2018. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://redcontraelabusosexual.org/delitos-virtuales-contra-ninos-ninas-y-adolescentes-aspectos-juridicos/>

FUNDACIÓN RED CONTRA EL ABUSO SEXUAL, Tips para Prevenir el Grooming en Casa. [en línea]. 2021. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://redcontraelabusosexual.org/tips-para-prevenir-el-grooming-en-casa/>

GAPTAIN, Riesgos De Ciberseguridad Para Los Menores De Edad. [en línea]. 2021. [Citado en 25 de Abril de 2020]. Disponible en internet: <https://gaptain.com/riesgos-de-internet-y-moviles/>

GCF APRENDE, ¿Qué Es Un Computador?. [en línea]. 2020. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://edu.gcfglobal.org/es/informatica-basica/que-es-un-computador/1/>

GLOBAL WEB INDEX, 5 Things to Know about Internet Users in Colombia. [en línea]. Transformación Digital. 2018. [Citado en 15 de Marzo de 2021]. Disponible en internet: <https://blog.globalwebindex.com/trends/internet-users-colombia/>

GOBIERNO DE ARGENTINA, Grooming. [en línea]. 2021. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.argentina.gob.ar/grooming>

GOBIERNO DE ARGENTINA, Huella Digital y Reputación Web. [en línea]. 2021. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.argentina.gob.ar/jefatura/innovacion-publica/gobierno-abierto-y-pais-digital/paisdigital/navegacion-segura/huella-digital-y-reputacion-web-1>

GOBIERNO DE CANARIAS, ¿Qué es la Identidad Digital?. [en línea]. 2020. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/identidad-digital-profesorado/que-es-la-identidad-digital/>

GOBIERNO DE ESTADOS UNIDOS, Prevenir el Ciberacoso. [en línea]. 2021. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://espanol.stopbullying.gov/acoso-por-internet-1zqb/prevenci%C3%B3n>

GOBIERNO DE ESTADOS UNIDOS, Qué es el Ciberacoso. [en línea]. 2021. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://espanol.stopbullying.gov/acoso-por-internet-1yqc/qu%C3%A9-es>

GODADDY, ¿Qué Son Las Redes Sociales y Para Qué Sirven?. [en línea]. 2021. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://es.godaddy.com/blog/que-son-las-redes-sociales-y-para-que-sirven/>

AVAST, Guía Esencial Sobre el Ransomware. [en línea]. 2022. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.avast.com/es-es/c-what-is-ransomware>

HACKNOID, ¿Qué Son Los Riesgos En Informática?. [en línea]. 2018. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://hacknoid.com/hacknoid/importancia-de-la-gestion-de-riesgos-informaticos/>

HARÁN, Juan Manuel. Educación En Seguridad Informática: ¿Debería Incluirse En La Educación Formal?. [en línea]. We Live Security. 2019. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.welivesecurity.com/la-es/2019/11/18/educacion-seguridad-informatica-deberia-incluirse-educacion-formal/>

HERJAVEC, Robert. Cybersecurity CEO: The History Of Cybercrime, From 1834 To Present. [en línea]. Estafas. 2019. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.herjavecgroup.com/history-of-cybercrime/>

HOSTDIME, Que Es La Conectividad , Origen Del Término, Lo Que Significa, Definición; Ejemplos. [en línea]. 2017. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://blog.hostdime.com.co/que-es-conectividad-orige-termino-significa-definicion-ejemplos/>

ICBF COLOMBIA, Conoce Los Riesgos Cibernéticos A Los Que Se Enfrentan Los Niños Y Niñas Y Cómo Prevenirlos. [en línea]. 2022. [Citado en 10 de Marzo de 2022]. Disponible en internet: <https://www.icbf.gov.co/mis-manos-te-ensenan/conoce-los-riesgos-ciberneticos-los-que-se-enfrentan-los-ninos-y-ninas-y-como>

ICBF COLOMBIA, Riesgos Digitales, ¿Cómo Proteger A Niñas, Niños Y Adolescentes Cuando Navegan En Internet?. [en línea]. 2019. [Citado en 10 de Marzo de 2022]. Disponible en internet: <https://www.icbf.gov.co/ser-papas/riesgos-digitales-los-que-se-exponen-los-ninos-y-como-prevenirlos>

INSTITUTO NACIONAL DE CIBERSEGURIDAD, El Ataque Del “Man In The Middle” en la Empresa, Riesgos y Formas de Evitarlo. [en línea]. 2020. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo>

INSTITUTO NACIONAL DE INVESTIGACIÓN Y PREVENCIÓN DEL FRAUDE DE COLOMBIA INIF, Conoce el Impacto Emocional del Fraude. [en línea]. 2021. [Citado en 11 de Marzo de 2022]. Disponible en internet: <https://inif.com.co/blog/2021/02/04/impacto-emocional-del-fraude/>

INTERNET SEGURA FOR KIDS, Sexting. [en línea]. 2020. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.is4k.es/necesitas-saber/sexting>

IONET, Soporte TI Vs TIC ¿Cuál es la Diferencia?. [en línea]. 2020. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.ionet.cl/post/soporte-ti-vs-tic-cual-es-la-diferencia>

JIMÉNEZ, Javier. ¿Expones Demasiados Datos En Redes Sociales? . [en línea]. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.redeszone.net/noticias/seguridad/datos-expuestos-usuarios-redes-sociales/>

KASPERSKY, ¿Qué es la Ciberseguridad?. [en línea]. 2020. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>

KASPERSKY, ¿Qué es la Deep Web y la Dark Web?. [en línea]. 2020. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.kaspersky.es/resource-center/threats/deep-web>

KASPERSKY, ¿Qué es un Troyano y Qué Daño Puede Causar?. [en línea]. 2022. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://latam.kaspersky.com/resource-center/threats/trojans>

KASPERSKY. Hackers de Sombrero Negro, Blanco y Gris: Definición y Explicación. [en línea]. 2022. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://latam.kaspersky.com/resource-center/definitions/hacker-hat-types>

KASPERSKY, Ingeniería Social: Definición. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering>

KASPERSKY DAILY, El Telégrafo, El Abuelo De Internet: El Principio De La Era De La Información. [en línea]. Cifrado. 2015. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.kaspersky.es/blog/telegraph-grandpa-of-internet/6273/>

LONGSTREET, Phil. GONZÁLEZ, Esther. y BROOKS, Stoney. Internet Addiction: When The Positive Emotions Are Not So Positive. [en línea]. 2019. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.sciencedirect.com/science/article/abs/pii/S0160791X18300290>

LÓPEZ, José María. Deep Web: Qué Es y Cómo Entrar en el Lado Más Oculto de Internet. [en línea]. 2017. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://hipertextual.com/2021/04/deep-web-como-entrar-que-es>

LUENGO, Manuel. Te Contamos Qué es un Hacker y Cuántos Tipos Hay. [en línea]. 2021. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.adslzone.net/reportajes/seguridad/hacker-tipos/>

MALWAREBYTES, Adware. [en línea]. 2022. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://es.malwarebytes.com/adware/>

MÁRQUEZ RIVERA, Jesús Manuel . El Gusano De Morris. [en línea]. 2011. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://blog.utp.edu.co/alejandropinto/files/2011/04/El-Gusano-de-Morris-El-D%c3%ada-Que-Internet-Se-Detuvo.pdf>

MCAFEE, ¿Qué es la Identidad Digital y Todo lo que Puedes Hacer para Protegerla?. [en línea]. 2021. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.mcafee.com/blogs/languages/espanol/que-es-la-identidad-digital-y-todo-lo-que-puedes-hacer-para-protegerla/>

MICROSOFT, ¿Cómo Proteger a Tus Niños y Adolescentes de los Riesgos en Línea?. [en línea]. 2022. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://news.microsoft.com/wp-content/uploads/prod/sites/41/2022/02/eBook-GuiaCiberseguridad-para-padres-de-familia-VF.pdf>

MICROSOFT, Protéjase Del Phishing. [en línea]. 2022. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44#:~:text=El%20phishing%20es%20un%20ataque,que%20fingen%20ser%20sitios%20leg%C3%ADtimos.>

NIC, ¿Qué Es Internet?. [en línea]. 2018. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://nic.ar/es/enterate/novedades/que-es-internet>

OBSERVATORIO GUATEMALTECO DE DELITOS INFORMÁTICOS, Historia Del Cibercrimen. [en línea]. 2017. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://ogdi.org/historia-del-cibercrimen>

OFICINA DE SEGURIDAD DEL INTERNAUTA, ¿Qué es el Vishing?. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-vishing#:~:text=Es%20un%20tipo%20de%20fraude,informaci%C3%B3n%20personal%20de%20sus%20v%C3%ADctimas.>

OZANUS, P. Scott. La Primera Infancia Como Base de la Fuerza Laboral del Futuro. [en línea]. 2017. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://blogs.worldbank.org/es/voices/la-primera-infancia-como-base-de-la-fuerza-laboral-del-futuro>

PANDA SECURITY, ¿Qué Es Un Macro Virus Y Cómo Funciona?. [en línea]. 2017. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.pandasecurity.com/es/mediacenter/malware/virus-melissa/>

PANDA SECURITY, Scam. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.pandasecurity.com/es/security-info/scam/>

PANDA SECURITY, Spyware. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://www.pandasecurity.com/es/security-info/spyware/>

PNUD, Cómo La Covid-19 Ha Acelerado La Transformación Digital. [en línea]. Blog. 2020. [Citado en 10 de Marzo de 2021]. Disponible en internet: <https://www.undp.org/content/undp/es/home/blog/2020/how-covid-19-has-sped-up-digital-transformation.html>

POLICÍA NACIONAL DE COLOMBIA, Carta Nigeriana Herencia. [en línea]. 2021. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://caivirtual.policia.gov.co/contenido/carta-nigeriana-herencia>

POLICÍA NACIONAL DE COLOMBIA, Denunciar Delitos Informáticos. [en línea]. Virtual. 2021. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.policia.gov.co/denuncia-virtual/delitos-informaticos>

POWER DATA, ¿Qué Es La Transformación Digital?. [en línea]. 2019. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://www.powerdata.es/transformacion-digital>

SÁNCHEZ, Cristina. Así Fue El Primer ‘ransomware’ Del Mundo: Disquetes Con Sida Que Secuestraban Tu PC. [en línea]. 2017. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.elconfidencial.com/tecnologia/2017-05-27/primer-ransomware-diskete-panama_1389351/>

REDHAT, ¿Qué es la Gestión de Riesgos?. [en línea]. 2019. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.redhat.com/es/topics/management/what-is-risk-management>

REVISTA SEMANA, El Cibercrimen Es Un Delito Más Rentable Que El Narcotráfico . [en línea]. Cibercrimen. 2015. [Citado en 15 de Marzo de 2021]. Disponible en internet:

<https://www.semana.com/internacional/articulo/principales-cifras-del-cibercrimen-mundo-colombia/213988/>

REVISTA SEMANA, ¿Colapsará El Internet En Colombia Por La Avalancha Del Teletrabajo? . [en línea]. Tecnología. 2020. [Citado en 20 de Marzo de 2021]. Disponible en internet: <https://www.semana.com/economia/articulo/capacidad-de-conexion-a-internet-de-colombia-para-facilitar-el-teletrabajo/657315/>

RINALDI, Paola. ¿De Dónde Viene El Delito Cibernético? Origen Y Evolución Del Delito Cibernético. [en línea]. 2017. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/>

RODRÍGUEZ, Vicente. y PÉREZ, Daniel. Fraudes Financieros, Salud Y Calidad De Vida: Un Estudio Cualitativo. [en línea]. 2020. [Citado en 11 de Marzo de 2022]. Disponible en internet: <https://www.gacetasanitaria.org/es-fraudes-financieros-salud-calidad-vida-articulo-S0213911119302742>

TECH TARGET, La Gente Puede Ser El Eslabón Más Fuerte En La Ciberseguridad, Dice Ncsc. [en línea]. 2017. [Citado en 22 de Marzo de 2021]. Disponible en internet: <https://searchdatacenter.techtarget.com/es/cronica/La-gente-puede-ser-el-eslabon-mas-fuerte-en-la-ciberseguridad-dice-NCSC>

UNICEF, Ciberseguridad. [en línea]. 2020. [Citado en 15 de Marzo de 2022]. Disponible en internet: <https://www.unicef.org/mexico/ciberseguridad>

UNIVERSIDAD AUTÓNOMA DE MÉXICO, ¿qué Es Un Dispositivo Móvil?. [en línea]. 2018. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://revista.seguridad.unam.mx/numero-07/dispositivos-moviles>

UNIVERSIDAD DE PALERMO, Internet, ¿oportunidad O Amenaza Para Los Negocios?. [en línea]. Escritos En La Facultad 97. 2014. [Citado en 15 de Marzo de 2021]. Disponible en internet: <http://fido.palermo.edu/servicios_dyc/publicacionesdc/vista/detalle_articulo.php?id_libro=501&id_articulo=10417>

VANDERBURG, Eric. The Evolution Of A Cybercrime: A Timeline Of Ransomware Advances. [en línea]. 2017. [Citado en 25 de Abril de 2021]. Disponible en internet: <https://www.carbonite.com/blog/article/2017/08/the-evolution-of-a-cybercrime-a-timeline-of-ransomware-advances>

VELÁSQUEZ, Melissa. y MELO, Carolina. ¿Por Qué Son Tan Adictivas Las Redes Sociales?. [en línea]. 2021. [Citado en 14 de Marzo de 2022]. Disponible en internet: < https://cnnespanol.cnn.com/2021/10/29/redes-sociales-adictivas-facebook-instagram-twitter-orix/>

VILLALBA, Juan José. “muchas Víctimas No Hablan Por Vergüenza”: El Perturbador Caso Del Hombre Que Sedujo Y Estafó A Más De Cincuenta Mujeres. [en línea]. 2021. [Citado en 12 de Marzo de 2022]. Disponible en internet: <https://elpais.com/icon/actualidad/2021-04-22/muchas-victimas-no-hablan-por-verguenza-el-perturbador-caso-del-hombre-que-sedujo-y-estafo-a-mas-de-cincuenta-mujeres.html>

VPN OVERVIEW, Los Mejores Proveedores De VPN Del Año 2022. [en línea]. 2022. [Citado en 16 de Marzo de 2022]. Disponible en internet: <https://vpnoverview.com/es/mejores-proveedores-vpn/mejores-servicios-vpn/>

WELIVESECURITY, Cómo Configurar Tor Para Navegar en la Deep Web de Forma Segura. [en línea]. 2020. [Citado en 14 de Marzo de 2022]. Disponible en internet: <https://www.welivesecurity.com/la-es/2020/07/23/como-configurar-tor-navegar-deep-web-forma-segura/>