PREVENCIÓN DE LOS CIBERCRIMENES EN LA NIÑEZ

* Fernando García Gerónimo
** Lenin Méndez Paz

* Egresado de la Licenciatura en Derecho de la Universidad Juárez Autónoma de Tabasco.
fernandogarciaa220@gmail.com

** Profesor investigador de la universidad Juárez Autónoma de Tabasco de la División Académica de Ciencias Sociales y Humanidades.
menpazl@gmail.com
ORCID: https://orcid.org/0000-0002-4539-3536

Artículo Recibido: 03 de abril 2023. Aceptado: 02 de mayo 2023.

RESUMEN. En el presente artículo se explora cómo la niñez se relaciona con las nuevas tecnologías, como son vulnerables a distintos crímenes perpetrados haciendo uso de las tecnologías de información y comunicación y cuáles son las acciones necesarias para establecer una adecuada cultura de ciberseguridad con el fin de prevenir que esta sea víctima de los cibercrimenes.

Palabras Clave: cibercrimen; niñez; tecnologías; internet; ciberseguridad.

ABSTRACT. This article explores how children relate to new technologies, how they are vulnerable to different crimes perpetrated using information and communication technologies and what actions are necessary to establish an adequate cybersecurity culture in order to prevent them from becoming victims of cybercrimes.

Palabras Clave: cybercrime; childhood; technologies; internet; cybersecurity; cybersecurity.

INTRODUCCIÓN.

Los avances en las tecnologías de la información y comunicación han revolucionado nuestra forma de vivir, comunicarnos y trabajar, sin embargo, también ha transformado el panorama delictivo, proporcionando nuevas oportunidades para las actividades ilegales, creando nuevas formas de delincuencia y cambiando la dinámica de los delitos tradicionales. Una de los grupos vulnerables es el de la niñez, quienes en nuestra actualidad tienen acceso al espacio digital a temprana edad y a menudo no son

totalmente conscientes de los riesgos y consecuencias relacionadas con la actividad digital.

DESARROLLO.

La aparición de Internet, las plataformas de medios sociales y los dispositivos móviles han creado nuevas oportunidades para que los delincuentes lleven a cabo sus actividades delictivas. La ciberdelincuencia se ha convertido en una amenaza importante en los últimos años, en los que los delincuentes utilizan técnicas sofisticadas para piratear sistemas informáticos, robar datos y cometer fraudes financieros. El anonimato de Internet y la facilidad de acceso a información sensible han hecho de la ciberdelincuencia un negocio lucrativo para los delincuentes. La red ha facilitado a los delincuentes el blanqueo de dinero, la evasión de la detección y la realización de actividades ilegales de forma anónima.

NIÑEZ.

Debemos en primer lugar definir que es lo que entendemos por niñez. Consideramos crucial que la definición de niñez sea clara y coherente para garantizar la protección adecuada de sus derechos. En el caso de México contamos con diversos códigos y leyes que nos hablan sobre la niñez.

La Ley general de los derechos de niñas, niños y adolescentes establece en su artículo 5 que se trata de niñas y niños los menores de doce años, y de adolescentes las personas de entre doce años cumplidos y menos de dieciocho años de edad. (Ley General de los Derechos de Niñas Niños y Adolescentes, 2014.)

Por otro lado la ley nacional del sistema integral de justicia penal para adolescentes nos señala de igual forma que se considera como adolescente a toda persona cuya edad está entre los doce años y menos de dieciocho cumplidos (Ley Nacional del Sistema Integral de Justicia Penal para Adolescentes, 2016).

Por su parte la organización de las naciones unidas [ONU] menciona en la Convención Sobre los Derechos Del Niño que se clasifica como tal a todo ser humano menor de dieciocho años de edad salvo que en la ley aplicable alcance antes la mayoría de edad. (ONU, 1989)

Tenemos con esto varias fuentes que nos permiten establecer una acepción clara sobre aquello a lo que nos referimos como niñez; lo cual es todo ser humano menor de 18 años

CIBERCRIMEN.

El Cibercrimen se define como un acto que infringe la ley y que se perpetra utilizando las tecnologías de la información y la comunicación (TIC) para atacar redes, sistemas, datos, sitios web o tecnología, o para facilitar la comisión de un delito. (United Nations Office on Drugs and Crime [UNODC], 2020)

Internet también ha dado lugar a nuevas formas de delincuencia, como el ciberacoso, el grooming y el robo de identidad. El anonimato de Internet ha envalentonado a los individuos a incurrir en tales comportamientos, con consecuencias devastadoras para las víctimas. Las plataformas de medios sociales también se han convertido en un caldo de cultivo para el acoso, las noticias falsas y la propaganda, que pueden incitar a la violencia y crear malestar social.

Los cibercrimenes también parecen ir en aumento, según el Informe sobre Delitos en Internet 2020 del Federal Bureau of Investigation (por su siglas en inglés: FBI), el IC3 (Internet Crime Complaint Center) recibió 791.790 denuncias de presuntos delitos en Internet en 2020, lo que supone un aumento del 69% con respecto al año anterior. Este aumento de los delitos denunciados puede atribuirse a varios factores, entre ellos el mayor uso de los servicios en línea durante la pandemia del COVID-19, así como la creciente sofisticación de los ciberdelincuentes (FBI, 2021)

Por su parte, el Instituto Nacional de Estadística y Geografía identificó 28 199 incidentes de seguridad informáticos durante el 2022. Del total de incidentes, 51.8 % afectó al sector privado y 48.2 %, al sector público (INEGI, 2022, p 19.) Por desgracia, el aumento de la ciberdelincuencia ha afectado también a la niñez.

CIBERCRIMENES Y LA NIÑEZ.

El auge de Internet y las redes sociales ha creado nuevas oportunidades para que los delincuentes ataquen a la niñez. Algunos de estos crímenes incluyen el grooming, el ciberacoso y el robo de identidad.

En palabras de Garcés (2021):

> El grooming es una conducta realizada por un adulto a través de un dispositivo digital (tableta, teléfono inteligente, computadora) o de cualquier otra tecnología de la información y la comunicación, haciendo uso del engaño o de propuestas falsas para contactar o enganchar a un menor con la intención de cometer un delito que lesione su normal desarrollo físico y emocional" (p, 43)

Según el informe de 2021 del NCMEC [National Center for Missing and Exploited Children], en 2021 recibieron la cifra récord de 29.3 millones de denuncias de material sospechoso de abuso sexual infantil. Esto representa un aumento del 35% con respecto a 2020. (NCMEC, 2021)

Una definición correspondiente de ciberacoso es un acto agresivo e intencionado llevado a cabo por un grupo o individuo, utilizando formas electrónicas de contacto repetidamente y a lo largo del tiempo contra una víctima que no puede defenderse fácilmente". (Smith et al., 2008, p. 376).

Por otro lado podemos definir el robo de identidad como la recogida no autorizada, posesión, transferencia, reproducción u otra manipulación de la información personal de otra persona con el fin de cometer fraude u otros delitos que impliquen el uso de una identidad falsa. (Sproule y Archer., 2007, p. 8)

Es importante tener esto en cuenta, ya que acuerdo a una encuesta realizada por Montessori Canela; 36% de la niñez empiezan a usar dispositivos con acceso a internet a la edad de 3 años o menos. A los 6 años, un 62,3% ya se ha iniciado en su uso y antes de los 10 años esta cifra llega a un 85,1% de la niñez que ya está utilizando dispositivos con internet. (Montessori Canela, 2022)

La Asociación de Internet MX (AIMX) en el estudio sobre ciberseguridad en empresas, usuarios de Internet y padres de familia en México 2021 indica que más del 50% de la niñez tiene un dispositivo propio, ya sea un teléfono inteligente o una tableta; y que en

más del 50% de los casos cuentan con más de 2 dispositivos (AIMX, 2021)

Un estudio realizado por NortonLifeLock reveló que el 61% de los padres en México confían en que sus hijos acceden al internet responsablemente sin supervisión de las actividades en línea de sus hijos (NortonLifeLock, 2022).

Otro estudio realizado por el Pew Research Center descubrió que solo el 39 % de los padres que tienen hijos de entre 13 y 17 años han establecido controles parentales en los dispositivos de sus hijos (Pew Research Center, 2016). Estas estadísticas demuestran que muchos padres no adoptan un papel activo en la supervisión de las actividades en línea de sus hijos, dejándolos vulnerables a la ciberdelincuencia.

La falta de supervisión parental puede tener graves consecuencias para la niñez. Por ejemplo, pueden verse expuestos al ciberacoso, a la captación de menores en línea o a la descarga involuntaria de programas maliciosos o virus. Sin la orientación y la supervisión adecuadas, la niñez también puede ser más propensa a participar en comportamientos de riesgo, como compartir información personal en línea o relacionarse con extraños.

Además, la niñez puede no comprender del todo los peligros potenciales de Internet y ser más propensos a adoptar comportamientos de riesgo. Esto es especialmente cierto en el caso de la niñez, que puede carecer de la madurez o la experiencia necesarias para comprender las implicaciones de sus actividades en línea. Por ello, los padres deben vigilar las actividades de sus hijos en la red para asegurarse de que no se exponen al peligro.

IMPACTO DEL CIBERCRIMEN EN LA SOCIEDAD.

El cibercrimen tiene importantes efectos en la sociedad, que van desde las pérdidas económicas y la violación de la intimidad personal hasta las amenazas contra la seguridad nacional. Antes de hablar de los impactos que tiene de manera especifica en la niñez, es importante antes analizar cómo en general puede afectar a la sociedad de manera general.

Los efectos del cibercrimen contra de los individuos esto se puede ver claramente en

actividades como el fraude cibernético y el acoso cibernético

Hablar de fraude cibernético significa hablar de cualquier fraude cometido a través o con la ayuda de programación informática o comunicaciones relacionadas con Internet, como sitios web, correo electrónico y salas de chat. (Rusch, 1999)

El Instituto de Hacienda y Crédito Público por medio de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros [CONDUSEF] señaló en un reporte que los fraudes cibernéticos en México cada vez crecen en proporción pasando del 32% en 2016 al 69% en 2020. (CONDUSEF, 2020)

Estos fraudes tienen como fin engañar a la gente para que facilite información confidencial, como datos de tarjetas de crédito o contraseñas de acceso y con esta información, pueden llevar a cabo transacciones no autorizadas, realizar compras o acceder a cuentas financieras, lo que se traduce en pérdidas económicas directas para particulares o empresas.

Otra de las maneras en las que los individuos se pueden ver afectados por la ciberdelincuencia es por medio del ransomware, el ransomware es una categoría de software malicioso que, cuando se ejecuta, inhabilita la funcionalidad de un ordenador de algún modo. El programa ransomware muestra un mensaje que exige un pago para restaurar la funcionalidad, el programa, en efecto, pide un rescate por el ordenador. (O'Gorman y McDonald, 2012).
Hablar de ciberdelincuencia no únicamente significa hablar de acciones que afectan a individuos en particular o empresas, sino también de acciones que pueden afectar a naciones enteras, como lo puede ser en el caso de ataques a la infraestructura critica.

La infraestructura crítica hace referencia a sistemas, digitales o físicos, que brindan servicios esenciales para la sociedad y que en caso de ser afectados podrían tener un impacto grave que afecte la seguridad de todo un país (González, 2022)

Un ejemplo de esta clase de ataques es el perpetrado por un virus denominado TRITON en junio y agosto de 2017. Este virus fue utilizado contra los controladores de seguridad de una instalación petroquímica

de Medio Oriente, el virus otorgaba a los atacantes un control remoto completo, proporcionándoles la capacidad de causar daños físicos y pérdida de vidas si la planta entraba en entrara en un estado inseguro. (FBI, 2022)

EFECTOS DEL CIBERCRIMEN EN LA NIÑEZ.

El cibercrimen afecta a la niñez de diversas de formas, ya sea de manera directa o indirecta, ya que la niñez es un periodo de crecimiento, y debido al rápido desarrollo del internet y la tecnología, esta puede tener un impacto significativo en sus vidas.

En el caso de víctimas de acoso en línea, estas a menudo experimentan angustia emocional, la exposición constante a mensajes negativos e hirientes puede provocar un deterioro del bienestar mental y la autoestima. El acoso y la intimidación en línea persistentes pueden tener efectos psicológicos a largo plazo en las personas. tal como lo demuestra un estudio, Las víctimas de ciberacoso corren más riesgo que las no víctimas de autolesionarse y de tener conductas suicidas. (John et al., 2018) de la misma manera, las víctimas de ciberacoso declaran experimentar más soledad junto con mayores sentimientos de aislamiento e impotencia. (Nixon, 2014)

Otra de las conductas que ponen en riesgo a la niñez es el grooming, ya presentamos una definición de grooming, pero no hemos profundizado en sus efectos, El grooming puede causar graves traumas emocionales y psicológicos en la niñez. Whittle et al., (2013) señalan los efectos que puede tener el grooming en la niñez, los seductores suelen emplear tácticas manipuladoras para ganarse la confianza y la lealtad de la niñez, pueden utilizar halagos, regalos, atención y manipulación emocional para crear una sensación de dependencia y control. Esta manipulación puede confundir y abrumarlos, haciéndolo más susceptible a las intenciones del abusador.

Debido a este vinculo, El grooming suele implicar una traición a la confianza, ya que el abusador suele presentarse como una figura digna de confianza en la vida de la víctima. Cuando la víctima se da cuenta de las verdaderas intenciones del abusador, puede sufrir una profunda pérdida de confianza, que afecta a su capacidad para establecer relaciones sanas y repercute en sus futuras interacciones con los demás.

Aunado a esto, el grooming puede causar graves traumas emocionales y psicológicos en la niñez. Pueden experimentar sentimientos de confusión, culpa, vergüenza y miedo. Los abusadores pueden explotar la vulnerabilidad de la víctima, haciéndole creer que el abuso es culpa suya o que debe mantenerlo en secreto, lo que aumenta aún más su angustia emocional. Y la faceta más grave de estas interacciones es la explotación y abuso sexuales: El grooming conduce a menudo a la explotación y el abuso sexual de la víctima.

El abusador puede intensificar la relación, introduciendo contenidos explícitos o inapropiados, participando en actividades sexuales o coaccionando a la víctima para que realice actos sexuales. Esto puede causar daños físicos y emocionales significativos, provocando traumas duraderos e impactando potencialmente en el desarrollo sexual y la autoestima de la víctima. (Whittle et al. 2013)

La exposición a contenido inapropiado de igual forma puede ocasionar un impacto negativo en la niñez. Hablar de contenido inapropiado significa hablar de información o imágenes que molesten a la niñez material dirigido a adultos, información inexacta o información que pueda inducir o tentar a la niñez a comportamientos ilícitos o peligrosos. (Internet Matters, 2021).

En un estudio publicado por Livingstone et al. (2014) relata las experiencias de 25,000 niños, niñas y adolescentes europeos usando el internet, explora las vivencias y preocupaciones de la niñez en relación con los riesgos en línea y las experiencias negativas, el estudio investiga diversos riesgos en línea, como el ciberacoso, los contenidos sexuales en línea, los problemas de privacidad, los contenidos nocivos generados por los usuarios y los contactos no deseados.

Una de las principales preocupaciones expresadas por la niñez fue por los contenidos inapropiados en línea, como la violencia, la pornografía o las imágenes gráficas. Afirmaron que las sensaciones que tales contenidos provocan en ellos son asco y miedo. (Livingstone et al., 2014) Estos ejemplos ilustran algunos de los peligros a los que está expuesta la niñez, pero no pretenden demeritar la importancia que tiene el internet para esta.

La importancia del internet para la niñez

El internet desempeña un papel importante en la vida de la niñez y ofrece diversas ventajas y oportunidades. les proporciona acceso a una gran cantidad de información y recursos de aprendizaje, permitiéndoles ampliar sus conocimientos y explorar sus intereses. El Internet aumenta las oportunidades de socialización de los jóvenes a través de plataformas de aprendizaje, redes sociales, aplicaciones, juegos o herramientas de comunicación como la mensajería instantánea (Daoud, 2020), fomenta la colaboración y el intercambio cultural. Fomenta la expresión creativa y la creación de contenidos, permitiendo a la niñez mostrar su talento, además, Internet expone a la niñez a diversas culturas y perspectivas, fomentando la empatía, la tolerancia y la conciencia global. Ofrece contenidos de entretenimiento y recreativos, y proporciona un valioso apoyo y recursos a la niñez que posee necesidades especiales.

Durante la pandemia de covid el internet tuvo un rol esencial en la vida de la niñez, Con el cambio que tuvieron las escuelas a la enseñanza a distancia, Internet se hizo esencial para que la niñez continuara su educación. Un informe de la Organización para la Cooperación y el Desarrollo Económicos (OECD) señala que la niñez utiliza Internet para jugar, chatear y establecer conexiones sociales. (OECD. 2019).

Las redes sociales plataformas en línea, las herramientas de videoconferencia y los recursos educativos permitieron a la niñez acceder a aulas virtuales, participar en clases interactivas, entregar trabajos y comunicarse con profesores y compañeros. Pero la educación no es el único factor importante, ya que con un acceso limitado a actividades y lugares al aire libre, Internet ofrecía una amplia gama de opciones de entretenimiento para la niñez. Podían ver películas, programas de televisión y vídeos educativos, escuchar música, jugar en línea y participar en experiencias virtuales, lo que les ayudaba a mitigar el aburrimiento y les proporcionaba salidas recreativas.

Las medidas de distanciamiento social y los encierros limitaron las interacciones en persona, pero Internet permitió a la niñez mantenerse en contacto con sus amigos y familiares. Las plataformas de redes

sociales, las videollamadas y las aplicaciones de mensajería permitieron reuniones virtuales, manteniendo las conexiones sociales y reduciendo la sensación de aislamiento.

Debido a la importancia que ha cobrado internet en los últimos años es necesario establecer una serie de recomendaciones para evitar que la niñez sean victimas de ciberdelitos.

AUTONOMÍA PROGRESIVA DE LA NIÑEZ.

La Suprema Corte de Justicia de la Nación define a la autonomía progresiva de la niñez como el desarrollo gradual y empoderamiento de la independencia y la capacidad de tomar decisiones de estos a medida que crecen y maduran. Consiste en darles niveles crecientes de responsabilidad, libertad y control sobre sus propias vidas de una manera comprensiva y adecuada a su edad. (Martinez et al., 2022).

Debido a que la autonomía progresiva reconoce que la autonomía de la niñez debe apoyarse dentro de un marco que promueva su seguridad, bienestar y desarrollo, una serie de recomendaciones para prevenir los cibercrimenes debe tomar en cuenta este principio. Implica ofrecer oportunidades adecuadas a su edad para aprender de sus experiencias, tomar decisiones y responsabilizarse de las consecuencias de esas decisiones. Respetar la autonomía progresiva implica capacitar a la niñez para que asuman un papel activo en su propia seguridad en línea. En lugar de imponer normas estrictas sin explicaciones, las recomendaciones deben centrarse en educar e informar sobre los riesgos potenciales, fomentar la capacidad de pensamiento crítico y enseñarles a tomar decisiones con conocimiento de causa. Este enfoque es para promover un desarrollo del sentido de propiedad y responsabilidad sobre sus comportamientos en línea.

El respeto de la autonomía progresiva fomenta así mismo la comunicación abierta entre la niñez y sus cuidadores. Las recomendaciones deben promover un entorno en el que estas sientan comodidad hablando de sus experiencias en línea, buscando orientación cuando la necesiten y denunciando cualquier incidente preocupante. Esto ayuda a generar confianza y garantiza que la niñez pueda buscar apoyo cuando se enfrentan a riesgos de ciberdelincuencia.

PREVENCIÓN DE CIBERCRIMENES.

La ciberseguridad es un elemento necesario en nuestro presente, entendemos ciberseguridad el conjunto de acciones dirigidas a proteger los equipos informáticos de uso común, servidores, sistemas electrónicos y redes de posibles ataques maliciosos e intentos de robo de información o control del dispositivo (Universidad Europea, 2022.) Como la tecnología sigue evolucionando a un ritmo sin precedentes, la niñez está cada vez más expuesta a peligros en línea, la supervisión por parte de los adultos no es la adecuada y no existe una cultura de ciberseguridad establecida, es difícil mantener un cuidado adecuado de los menores, por eso analizaremos diversas medidas que pueden adoptarse para evitar que la niñez sea víctimas de la ciberdelincuencia.

1. Educación

La educación es un aspecto crucial de la prevención de la ciberdelincuencia. Hay que enseñar a la niñez a mantenerse seguros en línea, a reconocer y evitar posibles peligros y a responder adecuadamente al ciberacoso y a otras formas de acoso en línea. Los padres, profesores y otros cuidadores también deben ser educados sobre cómo reconocer y abordar los riesgos en línea para la niñez. Un estudio conducido en estudiantes de preparatoria en Nigeria donde se realizaron una serie de actividades para concientizar sobre los crímenes demostró que la educación es efectiva para incrementar la prevención de cibercrimenes (Amosun e Ige, 2013)

Hay diversos pasos que proponemos para lograr esto:

a. Se debe mantener una conversación abierta con la niñez sobre la seguridad en Internet. Los padres deben explicar que Internet puede ser una herramienta divertida y útil, pero también peligrosa si no tienen cuidado.
b. Enseñar a la niñez a no compartir nunca información personal en Internet, como su nombre completo, dirección, número de teléfono o cualquier otro dato identificativo.
c. Animar a la niñez a utilizar contraseñas seguras y explíqueles la importancia de no compartirlas con nadie.
d. Enseñar a la niñez a reconocer las amenazas de robo de identidad en línea. Así como explicarles que nunca

deben hacer clic en enlaces ni descargar archivos adjuntos de fuentes desconocidas.

e. Enseñar a la niñez la importancia de la configuración de la privacidad y cómo controlar quién puede ver sus perfiles y publicaciones en las redes sociales.
f. Hablar sobre el ciberacoso y otras formas de acoso en línea y animarlos a denunciar si ven que alguien está siendo acosado o intimidado en Internet.
g. En el caso de los padres establecer normas y directrices para las actividades de sus hijos en Internet, incluido el tiempo que pueden pasar conectados y los sitios web y aplicaciones que pueden utilizar. Así como supervisar las actividades en línea de sus hijos y esté al tanto de con quién hablan y qué hacen en Internet.
h. Mantenerse informado sobre las últimas tendencias y amenazas para la seguridad en Internet, y comparta esta información con la niñez, niñas y adolescentes.
i. Por último, animar a la niñez a hablar con un adulto de confianza si se sienten incómodos o amenazados en Internet.

2. Controles Parentales

En palabas de Sammons y Cross (2017):

> Los controles parentales son funciones o programas que permiten supervisar y restringir lo que una persona hace en Internet. Hay una gran variedad de programas que bloquean y filtran sitios web y contenidos, registran sus actividades, limitan su tiempo en línea y ven su historial de navegación y sus comunicaciones. Aunque las funciones de los programas de control parental varían, algunos registran las pulsaciones del teclado, hacen capturas de pantalla de lo que hacen, registran los chats en varios sitios o aplicaciones y registran dónde están mediante informes sobre la ubicación de un portátil, tableta, teléfono u otro dispositivo. (p, 204)

Según Kaspersky (S.f.). estas son algunas de las funciones más comunes del software de control parental:

a. Filtros de contenido: Estas herramientas bloquean el acceso a

sitios web y aplicaciones que se consideran inapropiados para la niñez en función de clasificaciones de edad o categorías específicas.

b. Límites de tiempo: Estas funciones permiten a los padres establecer límites sobre la cantidad de tiempo que sus hijos pueden pasar en línea o utilizando ciertas aplicaciones.
c. Control de actividad: esto permite a los padres supervisar la actividad en línea de sus hijos, incluido el historial de navegación web, la actividad en redes sociales y la mensajería.
d. Gestión de aplicaciones: son opciones que permiten a los padres controlar a qué aplicaciones puede acceder o descargar su hijo.
e. Seguimiento de la ubicación: Algunas herramientas de control parental permiten a los padres seguir la ubicación de sus hijos mediante GPS, lo que puede ser útil para garantizar su seguridad y bienestar. (Kaspersky, s.f.)

Aunque los controles parentales pueden ser útiles para mantener a la niñez seguros en Internet, es importante recordar que no son infalibles. La niñez puede encontrar formas de acceder a contenidos inapropiados o adoptar conductas de riesgo en Internet.

3. Redes y dispositivos seguros

Para prevenir la ciberdelincuencia, es importante garantizar la seguridad de los dispositivos y las redes. Esto puede conseguirse utilizando contraseñas seguras, activando la autenticación de dos factores e instalando antivirus y cortafuegos. Los padres también deben asegurarse de que su red Wi-Fi doméstica sea segura y de que la niñez no utilice redes Wi-Fi públicas sin supervisión. Nosotros consideramos los siguientes puntos

a. Contraseñas seguras: Una contraseña segura es aquella que un hacker no puede adivinar o descifrar fácilmente con herramientas informáticas y que es única y compleja. (Norton, enero 18 del 2018). Las contraseñas también deben ser únicas, es decir, no deben utilizarse para varias cuentas. Utilizar un gestor de contraseñas puede ayudarle a generar y recordar contraseñas seguras.
b. Autenticación de dos factores: La autenticación de dos factores (2FA) es un sistema de autenticación que

añade una capa adicional de seguridad a tus cuentas al añadir dos (o a veces más) niveles de inicio de sesión a tus cuentas. (Stouffer, 2022) Proporciona una capa adicional de seguridad más allá de una simple contraseña. Requiere que los usuarios proporcionen una segunda forma de identificación, como un código enviado a su teléfono antes de acceder a sus cuentas. 2FA puede ayudar a evitar el acceso no autorizado a las cuentas, incluso si la contraseña se ve comprometida.

c. Configuración de antivirus y firewall: El software antivirus está diseñado para detectar y eliminar software malicioso, como virus, gusanos y troyanos, de su ordenador o dispositivo. Un firewall es un sistema de seguridad de redes informáticas que restringe el tráfico de Internet hacia, desde o dentro de una red privada. (Kaspersky, 2022)
d. Supervisión del uso del Wi-Fi por la niñez: La niñez debe ser supervisada cuando utilicen redes Wi-Fi públicas para evitar que accedan a contenidos inapropiados o compartan información sensible con extraños. Los padres también deben considerar el uso de programas de control parental para supervisar las actividades en línea de sus hijos y limitar su acceso a determinados sitios web y aplicaciones.

4. FOMENTO DE HÁBITOS SALUDABLES EN EL HOGAR.

Fomentar hábitos saludables como limitar el tiempo frente a la pantalla, participar en actividades físicas y realizar actividades sociales fuera de línea puede ayudar a reducir la exposición de la niñez a los riesgos en línea. Es importante encontrar un equilibrio entre las actividades en línea y fuera de línea y animar a la niñez a pasar tiempo al aire libre y a participar en interacciones cara a cara. Hay distintas maneras de lograr esto con la ayuda de los padres; algunas recomendaciones propias son:

a. Dar ejemplo: La niñez suele aprender de sus padres, así que es esencial predicar con el ejemplo. Los padres deben asegurarse de que practicar hábitos saludables, como limitar el tiempo frente a la pantalla, hacer ejercicio con regularidad y

participar en actividades sociales fuera de línea.

b. Actividades familiares: los padres deben animar a sus hijos a realizar actividades físicas convirtiéndolas en una actividad familiar. realizando actividades al aire libre como excursiones o deportes.
c. Limitar el tiempo frente a la pantalla: los padres deben ser claros al tiempo que su hijo puede pasar cada día frente a los dispositivos electrónicos..
d. Fomento de aficiones e intereses: los padres pueden animar a sus hijos a dedicarse a aficiones e intereses ajenos a la tecnología. Puede tratarse de tocar un instrumento musical, pintar o hacer deporte. Fomentar estos intereses les ayudará a reforzar su autoestima, desarrollar nuevas habilidades e intereses y reducir su dependencia de la tecnología.
e. Fomento de la interacción social cara a cara: los padres pueden animar a los más pequeños a relacionarse cara a cara organizando citas para jugar, asistiendo a actos sociales o participando en actividades de grupo, como equipos o clubes deportivos. Esto les ayudará a desarrollar habilidades sociales, entablar relaciones y reducir su dependencia de las interacciones sociales en línea.

En general, dando ejemplo, fomentando aficiones e intereses saludables, limitando el tiempo frente a la pantalla, promoviendo la interacción social cara a cara y utilizando el refuerzo positivo, los padres pueden ayudar a sus hijos a desarrollar hábitos saludables y reducir su exposición a los riesgos en línea.

5. ENSEÑARLE SOBRE PRIVACIDAD A LA NIÑEZ.

Hay que enseñar a la niñez la importancia de la privacidad y los riesgos que conlleva compartir información personal en Internet. Los padres deben animar a sus hijos a ser cautelosos a la hora de compartir información personal, como su nombre, edad y ubicación, y a evitar compartir información sensible, como contraseñas o información financiera. Algunas otras recomendaciones propias son:

a. Empezar a temprana edad: se debe mostrar a la niñez lo antes posible sobre la privacidad en Internet y los riesgos asociados a compartir información personal. Esto les ayudará a comprender la importancia de proteger su información personal desde una edad temprana.
b. Utilizar ejemplos de la vida real: Utilizar ejemplos de la vida real puede ayudar a la niñez a comprender los riesgos asociados a compartir información personal en línea. Por ejemplo, puede hablarles de las consecuencias de compartir información personal con extraños, como el robo de identidad o el ciberacoso.
c. Hablar de las posibles consecuencias: Hable de las posibles consecuencias de compartir información personal en Internet, como la vergüenza, el acoso o incluso el peligro físico. Esto ayudará a la niñez a comprender la gravedad del asunto y les animará a ser más precavidos con lo que comparten en Internet.
d. Establecer parámetros de privacidad: es fundamental ayudar a la niñez a establecer la configuración de privacidad en sus cuentas de redes sociales y explíqueles cómo funcionan, así como animarles a compartir información personal sólo con personas que conozcan y en las que confíen.
e. Disponibilidad para hablar: Los padres deben hacer saber a los hijos que pueden acudir a ellos si alguna vez se sienten incómodos o preocupados por algo que ven en Internet.

CONCLUSIONES.

El crecimiento de las tecnologías de la información y la comunicación ha sido enorme en los últimos años, las TICs forman parte de nuestra vida diaria, y estas tecnologías tienen impacto en la vida de la niñez, ya que es usada por esta en diversas áreas (comunicación, educación, actividades recreativas). la prevención de los cibercrimenes en la niñez es un tema que debe ser abordado de manera prioritaria por lo cual es menester tomar los pasos adecuados para inculcar cuidados en esta, ya que esta es particularmente vulnerables a los cibercrimenes, en especial cuando no existen las precauciones necesarias ni el cuidado adecuado por parte de los padres. Diversas estadísticas muestran no

únicamente que los cibercrimenes son una amenaza creciente, sino que también existen deficiencias en el cuidado que las personas toman con respecto a su actividad en la red
Es necesario establecer lo que se llama una cultura de ciberseguridad en la niñez esto implica educarles sobre los peligros en línea y enseñarles a usar la tecnología de manera segura y responsable.

Implementar esta cultura presenta una serie de retos particulares, pero se puede empezar desde el hogar con cosas como implementar diversas actividades y cuidado en casa, tales como el fomento de hábitos saludables, un correcto dialogo ante la niñez y adolescentes, hasta la implementación del software para monitoreo y cuidado de las redes.

Los elementos más importantes que hemos identificado para establecer un cuidado optimo son:

1. La educación: La cual debe ser prioritaria tanto en casa como en las instituciones educativas
2. Los controles parentales: Estos son las herramientas y software necesarios para establecer un monitoreo adecuado
3. El cuidado de redes y dispositivos: Lo cual se logra estando al día en las ultimas actualizaciones de seguridad y el uso de antivirus
4. El fomento de hábitos saludables en el hogar: los cuales están a cargo de los padres y deben de ser practicados en el hogar

Enseñarle sobre privacidad a la niñez: la cual implica usar ejemplos reales sobre las amenazas y consecuencias de compartir información personal en las redes.

LITERATURA CITADA

Amosun, P. A., & Ige, O. A. (2013). Impact of an Action Cyber Crime Prevention Programme on In-School Aged Children's Attitude to Crime Prevention Concepts in Civic Education and Social Studies. European Scientific Journal, 9(21).

Anderson, M. Parents, (7 de enero del 2016). Teens and Digital Monitoring. Pew Research Center: Internet, Science & Tech. Recuperado de https://www.pewresearch.org/internet/2016/01/07/parents-teens-and-digital-monitoring/

Asociación de Internet Mx. (2021) Ciberseguridad en Empresas, Usuarios de Internet y Padres de Familia en México 2021. https://irp.cdn-website.com/81280eda/files/uploaded/Estudio%20de%20Ciberseguridad%20AIMX%202021%20%28Pu%CC%81blica%29%2020210614.pdf

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (2020), Fraudes cibernéticos y tradicionales. https://www.condusef.gob.mx/documentos/comercio/FraudesCiber-3erTrim2020.pdf

Daoud, R., Starkey, L., Eppel, E., Vo, T. D., & Sylvester, A. (2020). The educational value of internet use in the home for school children: A systematic review of literature. Journal of Research on Technology in Education, 53(4), 353-374.

Europol. (2021). Europol's 2020 internet organized crime threat assessment. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

FBI. (2021). IC3 2020 Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

FBI. (2022). TRITON Malware Remains Threat to Global Critical Infrastructure Industrial Control Systems (ICS). https://docs.house.gov/meetings/JU/JU00/20220329/114533/HHRG-117-JU00-20220329-SD009.pdf

Garcés Nava A. E. (2021). La parte especial del código penal nacional. El impacto de las nuevas tecnologías para la creación de nuevos tipos penales. INACIPE

González, S. (10 de Marzo de 2022). Ciberataques a la infraestructura crítica de un país y sus consecuencias, Welivesecurity, https://www.welivesecurity.com/la-es/2022/03/10/ciberataques-infraestructura-critica-pais-consecuencias/

Instituto Nacional de Estadística y Geografía. (2022). Censo nacional de seguridad pública federal 2022-1. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/CNSPF/CNSPF-2022.pdf

Internet Matters. (2021, October 27). What parents need to know about inappropriate content. https://www.internetmatters.org/issues/inappropriate-content/learn-about it/#:~:text=Inappropriate%20content%20includes%20information%20or,Content%20containing%20swearing

John, A., Glendenning, A. C., Marchant, A., Montgomery, P., Stewart, A., Wood, S., & Hawton, K. (2018). Self-harm, suicidal behaviours, and cyberbullying in children and young people: Systematic review. Journal of medical internet research, 20(4), e9044.

Kaspersky. (21 de Octubre del 2022) What is a firewall? Definition and explanation. https://www.kaspersky.com/resource-center/definitions/firewall

Kaspersky. (s.f.). Internet Safety for Children: Tips to Keep Kids Safe Online. https://www.kaspersky.com/resource-center/preemptive-safety/kids-online-safety

Ley General de los Derechos de Niñas Niños y Adolescentes [LGDNNA]. Artículo 5, 4 de diciembre de 2014 (México)

Ley Nacional del Sistema Integral de Justicia Penal para Adolescentes. [LNSIJPA], Artículo 3, 16 de junio de 2016 (México)

Martínez Verastegui , A., Andrés Hernández, P., Hernández Reyes, G. Y. (2022). Derechos de niñas, niños y adolescentes. Centro de Estudios Constitucionales SCJN

Montessori Canela Internacional (2022, October 7). Observatorio sobre el uso de internet en menores de edad. https://www.montessoricanela.com/observatorio-sobre-el-uso-de-internet-en-menores-de-edad-riesgos-beneficios-y-limites/

National Center for Missing & Exploited Children. (2022) CyberTipline Statistics. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata#files

Nixon, C. L. (2014). Current perspectives: the impact of cyberbullying on adolescent health. Adolescent health, medicine and therapeutics, 143-158.

Norton, (18 de enero del 2018). How to choose a secure password. https://us.norton.com/blog/how-to/how-to-choose-a-secure-password

NortonLifeLock. (2020) 2020 Norton Cyber Safety Insights Report: Special Release – Home & Family. Recuperado de https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/infographics/2022_NLCSIR_HomeFamily_Report_FINAL.pdf

Organization for Economic Cooperation and Development. (2019). What do we know about children and technology? https://www.oecd.org/education/ceri/Booklet-21st-century-children.pdf

O'Gorman, G., & McDonald, G. (2012). Ransomware: A growing menace. Arizona, AZ, USA: Symantec Corporation.

ONU: Asamblea General, Convención sobre los Derechos del Niño, 20 Noviembre 1989, United Nations, Treaty Series, vol. 1577, p. 3, https://www.refworld.org.es/docid/50ac92492.html

Rusch, J. J. (1999, June). The "social engineering" of internet fraud. In Internet Society Annual Conference. http://taupe.free.fr/book/psycho/social%20engineering/TheSocial%20Engineering%20of%20Internet%20Fraud.pdf

Sammons, J., & Cross, M. (2016). The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy. Syngress.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, 49(4), 376-385. doi: 10.1111/j.1469-7610.2007.01846.x

Sproule, S., & Archer, N. (2007, July). Defining identity theft. In Eighth World Congress on the Management of eBusiness (pp. 20-20). IEEE.

Stouffer, C. (16 de Junio de 2022), What is 2FA? A simplified guide to two-factor authentication. NortonLifeLock. Recuperado de https://us.norton.com/blog/privacy/what-is-2fa#

United Nations Office on Drugs and Crime. (Febrero del 2020). E4J, University Module Series, Cybercrime. Recuperado el 29 de Marzo del 2023 de https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html

Universidad Europea, (19 de Abril del 2022), ¿Qué es la ciberseguridad?. https://universidadeuropea.com/blog/que-es-ciberseguridad/

Whittle, H. C., Hamilton-Giachritsis, C., & Beech, A. R. (2013). Victims' voices: The impact of online grooming and sexual abuse. Universal Journal of Psychology, 1(2), 59-71. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=174428aa5fe3e452a55a14fc2c7512e8735c07fe