International Centre™
FOR MISSING & EXPLOITED CHILDREN

CIBERDELINCUENCIA
DELITOS SEXUALES EN LÍNEA
CONSIDERACIONES BÁSICAS SOBRE SEGURIDAD EN INTERNET
LA HUELLA DIGITAL

28 de marzo de 2023

Contenido

¿Qué son las Tecnologías de la Información y la Comunicación (TIC)?

- El Programa de las Naciones Unidas para el Desarrollo concibe las TIC como “el universo de dos conjuntos, representados por las tradicionales Tecnologías de la Comunicación (TC) –constituidas principalmente por la radio, la televisión y la telefonía convencional– y por las Tecnologías de la Información (TI) caracterizadas por la digitalización de las tecnologías de registros de contenidos (informática, de las comunicaciones, telemática y de las interfaces)” (PNUD, 2002).

- La Sociedad de la Información de Telefónica de España indica que las TIC “son las tecnologías que se necesitan para la gestión y transformación de la información, y muy en particular el uso de ordenadores y programas que permiten crear, modificar, almacenar, proteger y recuperar esa información”.

CONTEXTO GLOBAL

Informe sobre medición de la sociedad de la información (ITU, 2018)

- Más de la mitad de la población mundial está ya en línea. A finales de 2018, el 51,2% de las personas, es decir, 3 900 millones, utilizaban Internet.
- El acceso a Internet en el hogar está ganando terreno. En 2018 casi el 60% de los hogares contaban con acceso a Internet, mientras que en 2005 este porcentaje era inferior al 20%.
- El número de jóvenes en línea tiende a superar al de personas de edad más avanzada. Se calcula que el porcentaje de jóvenes de entre 15 y 24 años que goza de acceso a Internet supera el 70% en todo el mundo, en comparación con solo el 48% de la población en general (2017).
- La Internet de las cosas ampliará en gran medida la huella digital. Dicha tecnología conectará no solo a personas, organizaciones y recursos de información, sino también a objetos dotados de capacidades de detección, procesamiento y comunicación de información digital (2017).

El Estado Mundial de la Infancia: Niños en un mundo digital (UNICEF, 2017)

- Los niños y adolescentes menores de 18 años representan aproximadamente **uno de cada tres** usuarios de internet en todo el mundo.
- Las tecnologías digitales brindan oportunidades de aprendizaje y educación para NNA, también les permite acceder a información sobre asuntos que afectan a sus comunidades y encontrar soluciones.
- Los teléfonos inteligentes están alimentando una “cultura del dormitorio”, y para muchos niños el acceso en línea es cada vez más personal, tiene un carácter más privado y está menos supervisado.
- Las TIC están intensificando los riesgos tradicionales de la niñez, como la intimidación, y fomentando nuevas formas de abuso y explotación sexual en línea, así como el acceso a contenidos inapropiados y a la transmisión en vivo de actos de abuso sexual infantil.

BENEFICIOS

- Las TIC proporcionan beneficios relacionados con el acceso inmediato a la información y a la comunicación. Su accesibilidad ha generado una nueva forma de establecer relaciones entre las personas, algo que incide de manera directa en el desarrollo de NNA que crecen y se socializan en un contexto tecnológico.

- Internet es un canal fundamental para la participación, la educación, el acceso a la información, la creatividad, el ocio y el juego, la comunicación y la libre expresión.

- Las TIC ofrecen muchas oportunidades de comunicación y aprendizaje para NNA.

RIESGOS

- Con el rápido desarrollo de las Tecnologías de la Información y la Comunicación (TIC), el AESNNA se ha extendido a un nuevo contexto y ha adquirido una nueva dimensión: la digital.

- Desafortunadamente, los NNA pueden estar expuestos a contenidos inapropiados para su edad y a MASI en Internet, sin advertencia ni consentimiento.

- La tecnología ha hecho que las formas tradicionales de delincuencia también evolucionen y cada vez hay más organizaciones delictivas que utilizan la red para lograr sus objetivos de forma rápida y lucrativa.

- Además, el aumento de las conexiones a internet en todo el mundo y la multiplicidad de dispositivos conectados hace que **los ciberdelitos no encuentren fronteras, ni virtuales ni físicas**, situación que pone en riesgo a toda la población.

¿Qué es la Ciberdelincuencia?

- La **ciberdelincuencia** consiste en la comisión de actividades delictivas que se llevan a cabo a través de las Tecnologías de la Información y la Comunicación (TIC).
- La ciberdelincuencia es un delito trasnacional. Los investigadores a menudo requieren el acceso a los datos y el intercambio de datos a través de las fronteras. Esto se puede lograr si los proveedores de servicios retienen los datos que se buscan y si existen medidas que permitan que las fuerzas del orden tengan acceso a estos datos.
- Entre los principales desafíos legales se tiene:
  - Variaciones en la legislación nacional sobre la ciberdelincuencia;
  - Diferencias en las reglas sobre las pruebas y el procedimiento penal; y
  - Variaciones en el alcance y la aplicabilidad geográfica de los tratados regionales y multilaterales sobre la ciberdelincuencia.
- Identificar y detener a un ciberdelincuente es una tarea que **demanda de profesionales formados en nuevas tecnologías.**

El AESNNA es una problemática global

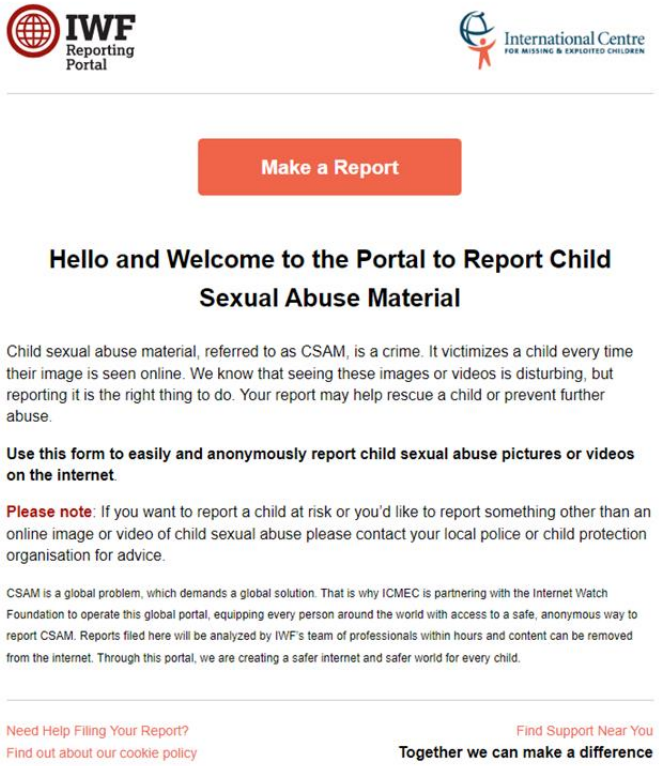
En 2021, se realizaron 29.3 millones de reportes por Material de Abuso Sexual Infantil a través de la CyberTipline de NCMEC. Un aumento del 35% comparado a 2020.

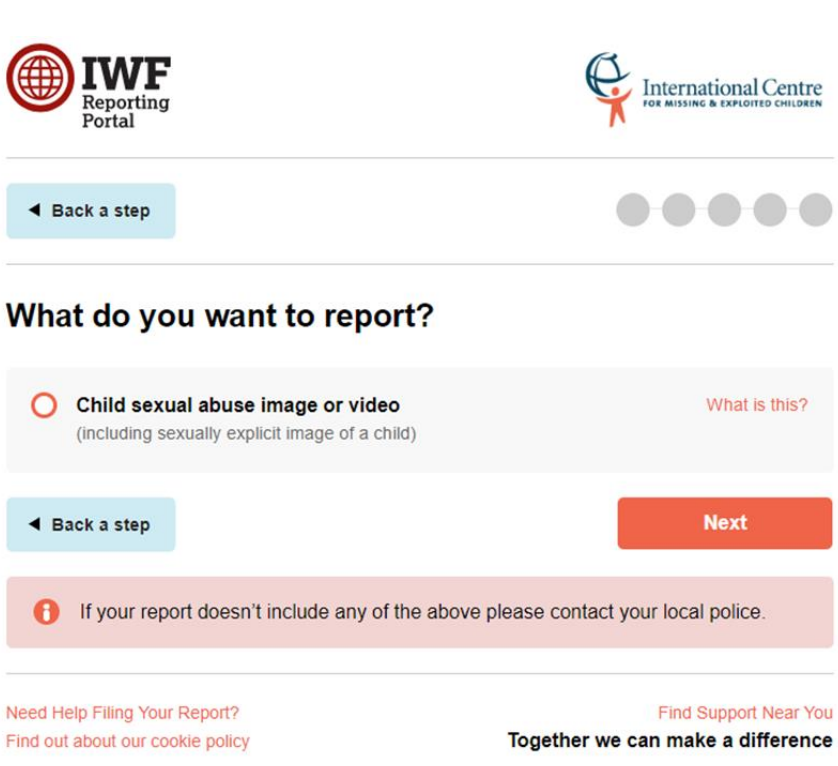
De acuerdo a los reportes de la Internet Watch Foundation (IWF) recibidos en el año 2021 se encontró que las víctimas, son en su mayoría niñas entre 7 y 13 años.

Según el último informe de Evaluación de la Amenaza Global de WeProtect, la Autoproducción de Material de Abuso Sexual de NNA aumentó 77% entre 2019 y 2020.

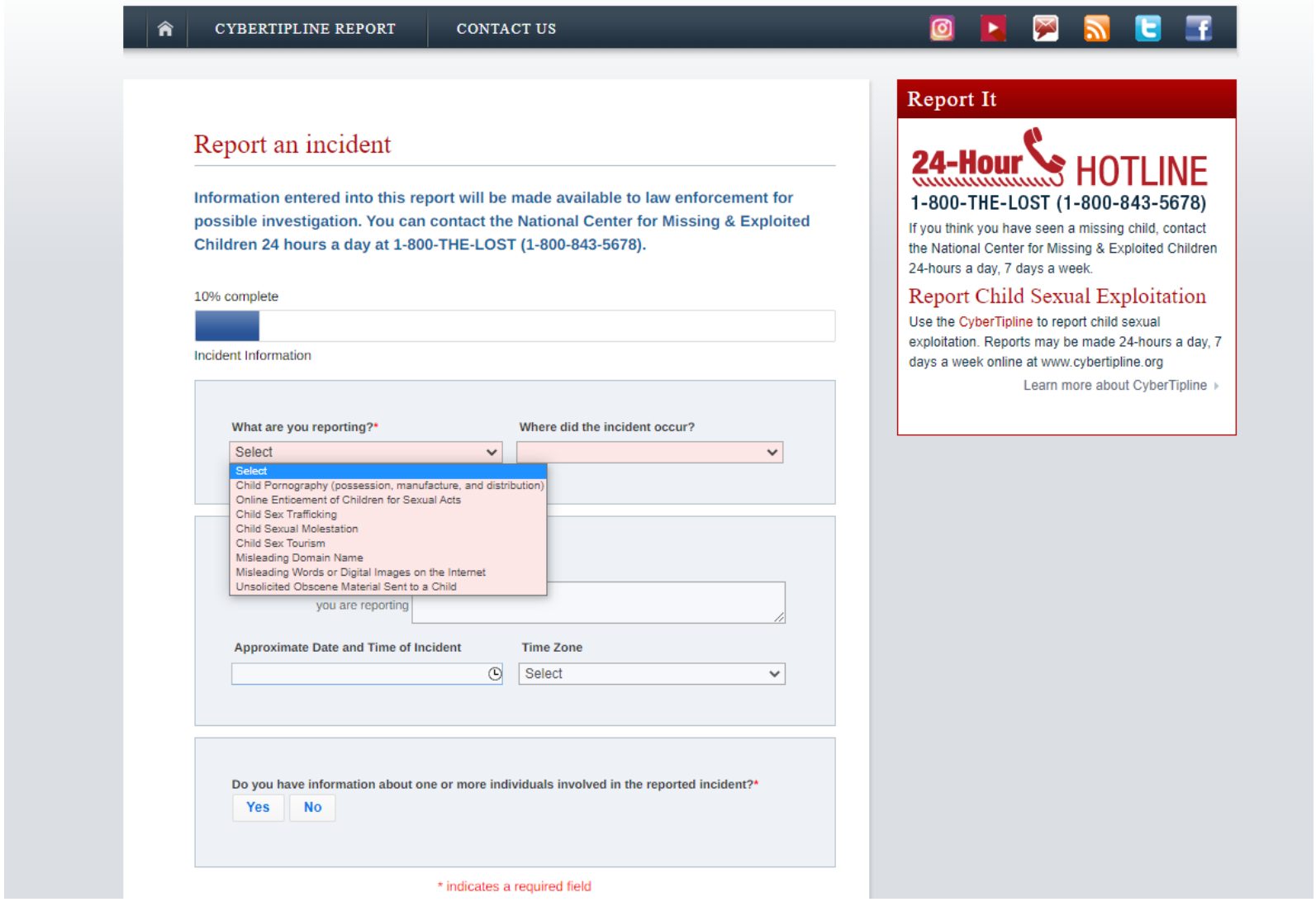
Mecanismos de denuncia

- ¡Haz tu reporte! https://report.iwf.org.uk/org/



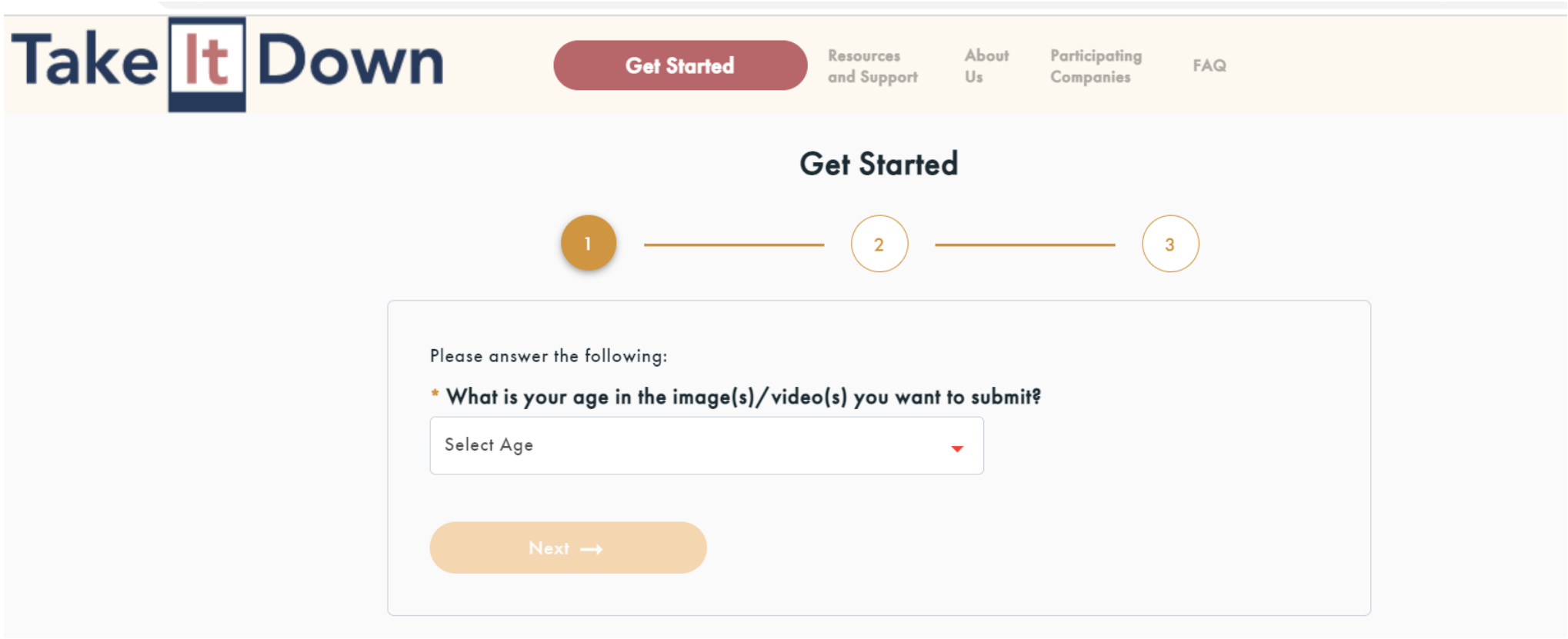


CyberTipline Report de NCMEC: https://report.cybertip.org/



Take it down-NCMEC

- Disponible en: https://takeitdown.ncmec.org/



RIESGOS EN LÍNEA Y FUERA DE LÍNEA

- **CYBERBULLYNG:** engloba el uso de las TIC para causar daño de manera repetida, deliberada y hostil. Esto puede incluir, pero no limitarse, al uso del Internet, teléfonos celulares u otros dispositivos electrónicos para difundir o enviar textos o imágenes que dañan o avergüenzan a una persona.

TIPS PARA NNA:

- La mayoría de las redes sociales tienen mecanismos de seguridad, denuncia y bloqueo. Actívalas si alguien te ofende, acosa o amenaza.
- Evita contestar a las provocaciones o insultos.
- Si te acosan, pide ayuda inmediatamente a un adulto de confianza.
- Compórtate con respeto hacia los demás en Internet.

❖ **GROOMING:** es el proceso mediante el cual un adulto busca establecer o construir una relación con un niño, niña o adolescente, ya sea en persona o mediante el uso de Internet u otras tecnologías digitales para facilitar el contacto sexual en línea o fuera de línea.

Etapas del Grooming:

1. Identifica a la niña, niño o adolescente víctima, a través de redes sociales o chats.
2. Ganar la confianza de la NNA.
3. Seducir a la potencial víctima a través de conversaciones.
4. Obtener información y/o contenido íntimo de NNA, que le permite ejercer presión posteriormente.
5. Acosar, chantajear, amenazar y manipular para lograr sus objetivos: La recepción de más fotografías o videos con contenido sexual o incluso, encuentros físicos con fines sexuales.

❖ **SEXTING:** es la autoproducción, intercambio y transmisión de mensajes, imágenes o videos de desnudos o casi desnudos, sexualmente sugerentes, a través de teléfonos celulares u otros dispositivos tecnológicos.

Una vez que se envía una imagen, video o mensaje, incluso a través de una cámara web, pierdes el control sobre ese contenido. Otra persona puede capturar y/o grabar este contenido y publicarlo en Internet.

El sexting es una práctica de riesgo que puede producir un daño irreparable a la privacidad e intimidad de la persona que comparte sus propias imágenes.

- **SEXTORSIÓN:** cuando una persona chantajea a otra, amenazándola con compartir imágenes o videos íntimos, con el fin de obtener favores sexuales, dinero, más contenido u otros beneficios.

- La víctima es coaccionada a ejecutar acciones de tipo sexual o pago de una cantidad de dinero, con la amenaza de que estas imágenes serán divulgadas si no lo hace.

¿Qué es la huella digital?

La huella digital es el rastro de datos que una persona deja cuando usa Internet (incluye sitios web, correos electrónicos y la información que envías en línea). La huella digital se crea de forma activa o pasiva.

Por ejemplo, los sitios web pueden rastrear tu actividad instalando cookies en tu dispositivo, y las aplicaciones pueden recopilar tus datos sin que lo sepas.

Una huella digital puede determinar la reputación digital de una persona, la cual ahora es casi tan importante como su reputación fuera de Internet.

Consejos sobre Ciberseguridad

- Hable con su hijo sobre la seguridad en Internet y sobre qué es la huella digital.
- Antes de usar una plataforma en línea o un sitio web, familiarícese con la configuración de privacidad y seguridad y con los mecanismos de denuncia.
- Revise sus propios perfiles para saber qué información comparte con el público.
- Asegúrese de configurar la privacidad en sus redes.
- Hable con la escuela u otros grupos de la comunidad en sobre lo que están haciendo para garantizar una experiencia en línea segura. La ciberseguridad es una responsabilidad compartida.

- Mantente siempre cerca cuando las NNA utilicen Internet.
- Establece normas de uso de los dispositivos con acceso a la Red.
- Habla con tus hijos sobre los peligros de la Red, interésate por lo que hacen cuando navegan y adviérteles de que se dirijan a ti y te comenten cualquier contenido, mensaje o situación que les incomode.
- Mantén la webcam siempre desconectada.
- Instala un buen antivirus y un bloqueador publicitario en el navegador.
- Configura sistemas de control parental que eliminan automáticamente las amenazas más comunes.

RECOMENDACIONES

- Promover la alfabetización digital en adultos y las habilidades de autoprotección por parte de los NNA.

- Empoderar a las figuras protectoras y visibilizar los sistemas de control, formal e informal, para facilitar la detección, investigación y atención de los casos de AESNNA en línea y fuera de línea, creando entornos seguros de confianza que garanticen la intervención inmediata a nivel familiar, asistencial y legal.

- Colocar a la niñez en el centro de la política digital y tomar las consideraciones y acciones necesarias para garantizar su protección en el entorno virtual.

CONCLUSIONES

- Las TIC contribuyen a la emergencia de nuevos valores y costumbres provocando continuas transformaciones en nuestras estructuras sociales, culturales y económicas.
- Las TIC no son buenas ni malas, su uso es el que las convierte en una excelente oportunidad, no sólo a nivel recreativo, sino en lo educativo y cultural, sin embargo, estas pueden transformarse en una peligrosa arma que pone en riesgo la integridad de NNA.
- La rápida evolución de las TIC origina nuevas formas de explotación y abuso sexual de NNA.
- El Estado tiene la obligación de prohibir, perseguir y castigar cualquier forma de violencia contra los niños y las niñas que se cometa a través de las TIC mediante su sistema penal, tipificando y procesando estos ciberdelitos y velando porque las víctimas reciban la atención y reparaciones necesarias.

- La protección, la prevención y la atención de los niños y las niñas víctimas de violencia, desde una perspectiva de sus derechos, requiere adoptar un paradigma basado en el respeto y la promoción de su dignidad humana y su integridad física y psicológica como titulares de derechos.
- Los NNA deben ser protegidos frente a todos los riesgos y formas de exposición a la violencia. Las habilidades técnicas, personales y sociales para enfrentar los riesgos en línea y fuera de línea se adquieren y desarrollan con el paso de los años, con un proceso de aprendizaje que debe iniciarse desde la primera infancia para que ellos mismos sepan identificar los riesgos y evitarlos o pedir ayuda cuando sea necesario. La prevención y educación son fundamentales.
- La Ciberdelincuencia conlleva retos para nuestros sistemas de justicia, para superarlos es necesario reformar la legislación nacional para tipificar los delitos facilitados por las TIC; actualizar los conocimientos y capacidades de las fuerzas del orden, y fortalecer la cooperación internacional para resolver casos transfronterizos.

¡GRACIAS!

Andrea Recinos

- Gerente Nacional de Proyectos para El Salvador.
- **arecinos@icmec.org**