

# CONSEJOS PARA PROTEGERSE CONTRA LA IA Y LOS ULTRA FALSOS (DEEPAKES)

## CONOZCA LAS AMENAZAS

La tecnología de inteligencia artificial (IA) evoluciona rápidamente, y con ella, surgen nuevas amenazas para la seguridad en línea. Por ejemplo, los depredadores en línea utilizan IA generativa (IAG) para crear material de abuso sexual infantil (MASI) modificado o falso y, en ocasiones, participan en sobornos dirigidos a menores. Esta tecnología también está siendo utilizada por niños y adolescentes para atacar a sus compañeros.

## LAS IMÁGENES MASI CON IAG SIGUEN SIENDO MASI

Seamos claros: **las imágenes de abuso sexual infantil de IAG siguen siendo material de abuso sexual infantil (MASI)**. Son ilegales, emocional y psicológicamente dañinas y profundamente traumáticas. Comprender esta amenaza en constante evolución es el primer paso para proteger a niños, niñas y adolescentes.

*Crear un deepfake solía requerir experiencia técnica y herramientas dedicadas; hoy, cualquier persona con una conexión a Internet puede usar IA para convertir una foto normal en una imagen de desnudo<sup>1</sup>.*



## NUEVAS TECNOLOGÍAS IAG Y RIESGOS ASOCIADOS

Entender las últimas tecnologías y sus riesgos asociados es crucial para prevenir, proteger y empoderar a las víctimas y sobrevivientes.

**La tecnología de IA** permite a un usuario crear nuevas imágenes, videos, audio y texto según solicitudes o indicaciones del usuario<sup>2</sup>. Esto podría incluir cualquier representación visual, como imágenes generadas por computadora, que parezcan mostrar a un menor participando en una conducta sexualmente explícita.

**La tecnología de ultra falsos (deepfakes)** utiliza IA para crear imágenes o videos realistas de personas haciendo o diciendo cosas que nunca hicieron. El término deepfake combina “aprendizaje profundo” (un tipo de IA utilizado para generar el contenido) y “falsificación”.

**Los servicios de desnudez simulada** permiten que una persona suba al internet una imagen inocente de una persona vestida para crear una representación virtual de esa persona desnuda.

Los informes muestran que estos servicios se promocionan como herramientas en sitios web y foros de desnudez, a veces incluso disfrazados de “guías para pedófilos”, que enseñan a los depredadores cómo explotar a menores mediante IA. Los depredadores en línea utilizan servicios de desnudez para subir una imagen completamente vestida de un niño o adolescente y, mediante IA, generar una versión falsa y sexualizada de dicha imagen. Estas imágenes falsas se utilizan posteriormente para soborno u otras formas de explotación.

<sup>1</sup> [commonsensemedia.org/kids-action/articles/deepfakes-can-be-a-crime-teaching-ai-literacy-can-prevent-it](https://commonsensemedia.org/kids-action/articles/deepfakes-can-be-a-crime-teaching-ai-literacy-can-prevent-it)

<sup>2</sup> [missingkids.org/theissues/generative-ai](https://missingkids.org/theissues/generative-ai)

## CONSEJOS PARA PROTEGERSE CONTRA LA IA Y LOS ULTRA FALSOS (DEEPFAKES)

### EL AUMENTO ES ALARMANTE:

En 2024, el Centro Nacional para Niños Desaparecidos y Explotados (NCMEC por sus siglas en inglés) recibió **67,000 informes que involucraban IAG**, un aumento del 1.325% en comparación con solo 4,700 en 2023. Los depredadores usan IAG para crear MASI falso pero realista y obligar a los niños a obedecer o a una mayor explotación<sup>3</sup>.

Según THORN, **1 de cada 10 menores afirma conocer casos en los que sus amigos y compañeros de clase han creado desnudos ultra falsos** de otros niños utilizando herramientas de inteligencia artificial generativa<sup>4</sup>.

En un estudio reciente, THORN encuestó a 1,200 jóvenes de entre 13 y 20 años sobre su conocimiento de los desnudos ultra falsos, sus experiencias vividas y su participación en la creación de dicho contenido. El estudio reveló que **1 de cada 6 encuestados indicó conocer personalmente** a alguien que había vivido al menos una de las siguientes experiencias:

- ❗ Descubrieron que un desnudo ultra falso de ellos estaba siendo (re)compartido
- ❗ Crearon un desnudo ultra falso de ellos mismos
- ❗ Alguien más les hizo un desnudo ultra falso
- ❗ Creó un desnudo ultra falso de un menor
- ❗ Compartió nuevamente un desnudo ultra falso de un menor<sup>5</sup>

### SEGÚN EL NCMEC, ESTAS SON LAS FORMAS EN QUE SE UTILIZA IAG PARA EXPLOTAR A NIÑOS Y ADOLESCENTES:

**Texto para chatear:** Ingresar texto para que un modelo de chat finja ser un niño y participe en un chat sexualmente explícito.

**Texto a texto:** Ingresar texto para generar guías, tutoriales o sugerencias sobre cómo manipular y dañar a niños y adolescentes tanto en línea como fuera de línea.

**Texto a imagen:** Ingresar indicaciones de texto para generar imágenes MASI o alterar archivos previamente cargados para hacerlos sexualmente explícitos.

#### Imagen a imagen:

- Subir imágenes de MASI conocidas e intentar generar MASI completamente nuevo en base a estas imágenes conocidas.
- Subir contenido de MASI conocido y alterar o agregar nuevos elementos abusivos a imágenes existentes.
- Subir imágenes inocentes de un niño y generar imágenes sexualmente explícitas o explotadoras del niño para gratificación personal o para compartirlas y utilizarlas para perpetrar sextorsión financiera contra un niño<sup>6</sup>.

**Cuadro de aviso: Consejo para proteger:** Exhorte a los niños y adolescentes a pensar de manera crítica sobre el contenido que encuentran en línea y enséñeles a cuestionar la autenticidad de las imágenes y los videos, entendiendo que la IA puede fabricar contenido de apariencia realista, pero falso.

<sup>3</sup> [missingkids.org/gethelpnow/cybertipline/cybertiplinedata](https://missingkids.org/gethelpnow/cybertipline/cybertiplinedata)

<sup>4</sup> [thorn.org/press-releases/report-1-in-10-minors-say-peers-have-used-ai-to-generate-nudes-of-other-kids](https://thorn.org/press-releases/report-1-in-10-minors-say-peers-have-used-ai-to-generate-nudes-of-other-kids)

<sup>5</sup> [thorn.org/blog/deepfake-nudes-are-a-harmful-reality-for-youth-new-research-from-thorn](https://thorn.org/blog/deepfake-nudes-are-a-harmful-reality-for-youth-new-research-from-thorn)

<sup>6</sup> [missingkids.org/content/dam/missingkids/pdfs/final-written-testimony-john-shehan-house-oversight-subcommittee-hearing.pdf](https://missingkids.org/content/dam/missingkids/pdfs/final-written-testimony-john-shehan-house-oversight-subcommittee-hearing.pdf)

## CONSEJOS PARA PROTEGERSE CONTRA LA IA Y LOS ULTRA FALSOS (DEEPFAKES)

### IMPLICACIONES LEGALES Y ÉTICAS DEL ABUSO SEXUAL INFANTIL EN LA COMUNIDAD IAG

Cualquier contenido sexualmente explícito de un menor se considera ilegal. Crear, compartir o incluso poseer este tipo de contenido en un dispositivo es ilegal y puede tener consecuencias de por vida. Tanto adultos como menores pueden ser considerados responsables al cometer delitos en línea. Además de las posibles infracciones penales federales, muchos estados tienen estatutos penales específicos sobre la sextorsión y el acoso en línea de menores, que pueden tener diversas consecuencias legales, como una advertencia verbal de un juez de menores o de familia, servicio comunitario o terapia por orden judicial, o incluso consecuencias más graves, como el encarcelamiento. Para más información, consulte los recursos del gobierno estatal y local de su zona.

*Muchos jóvenes pueden no darse cuenta de que “simplemente jugar” con herramientas de IA para generar desnudos falsos de compañeros de clase u otras personas puede cruzar los límites legales, con consecuencias que alteran la vida<sup>7</sup>.*



### CÓMO EVITAR EL ABUSO SEXUAL INFANTIL DE IAG

- Asegúrese de que su perfil y el de su hijo estén configurados como privados y que todas las imágenes sean solo para amigos y no sean de acceso público.
- Utilice la configuración de control parental. Consulte **Connect2Protect: Control parental** para obtener más información.
- Mantenga abiertas líneas de comunicación con los niños sobre sus actividades en línea.
- Exhórtelos a que acudan a usted con cualquier inquietud o pregunta que puedan tener sobre inteligencia artificial, desnudos ultra falsos y seguridad en línea.

### CÓMO RESPONDER

Tome medidas inmediatas si sabe o sospecha que un niño bajo su cuidado es víctima de abuso sexual infantil en línea.

- Mantenga la calma.
- Considere poner el equipo en modo avión y asegúrese de que el Bluetooth y el Wi-Fi estén apagados para que el delincuente no pueda borrar, eliminar o alterar la evidencia de forma remota.
- Guarde todas las comunicaciones, no las elimine.
- Comuníquese con las autoridades y asegúrese de que puedan acceder al dispositivo.
- No envíe imágenes desde el dispositivo de su hijo a ningún otro dispositivo. Es ilegal difundir material de abuso sexual infantil.
- Informe el incidente a la policía.

<sup>7</sup> [commonsensemedia.org/kids-action/articles/deepfakes-can-be-a-crime-teaching-ai-literacy-can-prevent-it](https://commonsensemedia.org/kids-action/articles/deepfakes-can-be-a-crime-teaching-ai-literacy-can-prevent-it)



## CONSEJOS PARA PROTEGERSE CONTRA LA IA Y LOS ULTRA FALSOS (DEEPFAKES)

### CÓMO INFORMAR

Puede enviar un informe de una de las siguientes maneras:

- Llame a la línea de denuncia Know2Protect al **833-591-KNOW (5669)**. Toda la información recibida a través de la línea de denuncia será revisada por el personal correspondiente y remitida a las oficinas locales de la Oficina de Investigaciones de Seguridad Nacional para su posible investigación.
- Comuníquese directamente con las autoridades policiales locales, estatales o tribales. En caso de emergencia, llame **al 911**.
- Envíe un informe al **CyberTipline** del Centro Nacional para Niños Desaparecidos y Explotados [report.cybertip.org](https://report.cybertip.org).

Visite [dhs.gov/know2protect/how-to-report](https://dhs.gov/know2protect/how-to-report) para obtener más información.

### Recursos

- **Página de apoyo para sobrevivientes:** Know2Protect comparte recursos y consejos para ayudar a las víctimas de abuso sexual infantil en línea. Visite [dhs.gov/know2protect/survivor-support](https://dhs.gov/know2protect/survivor-support) para obtener más información.
- **Bájalo (Take it down):** El Centro Nacional para Niños Desaparecidos y Explotados ofrece un servicio gratuito para ayudar a eliminar fotos y videos de desnudos, parcialmente desnudos o sexualmente explícitos tomados antes de los 18 años. Visita [takeitdown.ncmec.org](https://takeitdown.ncmec.org) para obtener más información.
- **Boletín informativo sobre IA generativa:** La IA permite producir un número exponencial de imágenes y vídeos que muestran abuso sexual infantil. Más información en [dhs.gov/know2protect/publication/generative-ai-csea](https://dhs.gov/know2protect/publication/generative-ai-csea).
- **THORN:** Consulta “Navegando por desnudos ultra falsos: una guía para hablar con tu hijo sobre seguridad digital” en [info.thorn.org/navigating-deepfake-nudes#get-the-guide](https://info.thorn.org/navigating-deepfake-nudes#get-the-guide) y “Desnudos ultra falsos y jóvenes” en [thorn.org/research/library/deepfake-nudes-and-young-people](https://thorn.org/research/library/deepfake-nudes-and-young-people).

