ANÁLISIS SOBRE LA CIBERDELINCUENCIA

BOLETÍN

EN ESTA EDICIÓN

PREVENCIÓN EN ENTORNOS DIGITALES: JUEGOS, MANIPULACIÓN, FRAUDES, CONTENIDO INAPROPIADO, RECLUTAMIENTO EN LÍNEA

DIRECCIÓN DE CIBERDELITOS
MINISTERIO DEL INTERIOR

Prevención en entornos digitales: juegos, manipulación, fraudes, contenido inapropiado, reclutamiento en línea

Ministerio del Interior
Subsecretaría de Combate al Delito
Dirección de Ciberdelitos

Responsables y Colaboradores
Redacción técnica del documento:
INGENIERO DIEGO TEJADA CAMPOS, Analista de Ciberdelitos
MAGISTER GABRIEL REINOSO MARTÍNEZ, Analista de Ciberdelitos
MAGISTER CARLOS SIMBAÑA COBA, Analista de Ciberdelitos
INGENIERO CÉSAR TRELLES SEGOVIA, Analista de Ciberdelitos

Revisión técnica del documento:
MAGISTER JORGE NÉJER GUERRERO, Especialista de Ciberdelitos
INGENIERO FREDDY GALLARDO SOSA, Especialista de Ciberdelitos

Redacción y compilación:
MAGISTER DUVAL MONTATIXE CAIZALUISA, Analista de Ciberdelitos

2025

Contenido

PRESENTACIÓN

El presente boletín surge como una iniciativa institucional orientada a comprender, visibilizar y prevenir las principales formas de ciberdelincuencia que se desarrollan en los entornos digitales actuales, con una atención prioritaria en la protección de niñas, niños y adolescentes. en una sociedad cada vez más conectada, donde las tecnologías de la información y la comunicación forman parte de la vida cotidiana, el ciberespacio se ha convertido en un entorno clave para la interacción social, educativa y económica, pero también en un espacio donde se manifiestan riesgos que pueden afectar gravemente la seguridad y los derechos fundamentales de las personas.

Desde la Dirección de Ciberdelitos del Ministerio del Interior, se ha considerado indispensable abordar de manera integral fenómenos como la manipulación digital, fraudes en línea, la exposición a contenidos inapropiados y las estrategias de captación y reclutamiento utilizadas por actores delictivos, tanto individuales como vinculados, estructuras de delincuencia organizada. Estas conductas trascienden el ámbito estrictamente tecnológico y se relacionan con realidades sociales, económicas y culturales que incrementan la vulnerabilidad de determinados grupos, en especial de la población más joven.

Este boletín se enmarca en el compromiso permanente del Ministerio del Interior con la seguridad integral y la protección de la ciudadanía, reafirmando la necesidad de una cooperación interinstitucional sostenida, la corresponsabilidad social y el uso responsable de las tecnologías como pilares fundamentales para enfrentar de manera efectiva la ciberdelincuencia en el Ecuador.

Jorge Fernando Illescas Peña
Director de Ciberdelitos del Ministerio del Interior

INTRODUCCIÓN

El objetivo del presente boletín es fortalecer la prevención y protección de la ciudadanía, especialmente de niños, niñas y adolescentes, frente a los riesgos y peligros presentes en los entornos digitales. El acelerado crecimiento del uso de internet, plataformas de juegos en línea y redes sociales ha generado nuevas formas de interacción que, aunque ofrecen oportunidades de educación, entretenimiento y comunicación, también exponen a los usuarios a amenazas que pueden vulnerar su seguridad e integridad.

Este boletín se enfoca en identificar y visibilizar los principales peligros digitales asociados a la manipulación emocional, fraudes en línea, acceso a contenido inapropiado y estrategias de reclutamiento utilizadas por actores delictivos. Asimismo, busca promover prácticas seguras, fomentar el acompañamiento familiar y brindar herramientas que permitan reconocer señales de riesgo y actuar oportunamente.

Conceptos y características fundamentales

Glosario de términos relevantes

Catsishing: se refiere a la fabricación de una identidad falsa online por parte de un ciberdelincuente con fines de engaño, fraude o explotación, se utiliza más comúnmente para estafas “románticas” en aplicaciones de citas, sitios web y plataformas de medios sociales (Proofpoitn, 2024).

El término catfishing se popularizó tras el documental de 2010 Catfish, donde Nev Schulman relata su experiencia al iniciar una relación en línea con una joven llamada “Megan”, que más tarde descubre ser una mujer mayor con una identidad completamente falsa (INCIBE, 2025).

Fake news: Se refieren a cualquier tipo de información imprecisa, descontextualizada o directamente falsa, que alguien difunde de manera intencionada para manipular la opinión o simplemente para obtener algún tipo de beneficio (INCIBE, 2025).

Sexting: Consiste en él envió voluntario de contenido intimo a través de fotos y/o videos mediante medios tecnológicos (Guardia Nacional CERT-MX, 2024).

Grooming: Práctica en la cual un adulto establece una relación de confianza con un niño, niña o adolescente con el propósito final de abusar sexualmente de ellos. Este proceso puede ocurrir tanto en persona como a través de Internet y redes sociales (Unicef, s.f.).

Sextorsión: Forma de explotación sexual infantil en la que una persona amenaza o chantajea a un menor, la mayoría de las veces con la posibilidad de que la persona demandante haga públicas las imágenes sexuales o de desnudos del menor, si no obtiene contenido sexual adicional, dinero, o participación del menor en actos sexuales (Missing & Explointed, 2025).

Cyberbullying: Es el acoso o intimidación realizado entre usuarios de una edad similar y contexto social equivalente, mediante el aprovechamiento de medios digitales, desde un teléfono móvil hasta Internet o a través de videojuegos online, entre otros (Ayuda en acción, 2025).

El acoso escolar también es conocido como bullying, palabra derivada del verbo inglés to bully (intimidar) (UNICEF, 2023).

Gaslighting: Es un patrón de abuso emocional en la que la víctima es manipulada para que llegue a dudar de su propia percepción, juicio o memoria. Esto hace que la persona se sienta ansiosa, confundida o incluso depresiva (Gurdian, 2017).

El Gaslighting se configura como un tipo de abuso psicológico el cual ha llamado la atención en los últimos años debido a su complejidad y efectos devastadores sobre la salud mental de quienes lo sufren.(INFOBAE, 2025)

Egosurfing: Consiste en utilizar las redes sociales y los buscadores de Internet, como Google, utilizando términos de búsqueda relativos a nosotros, como nuestro nombre, apellidos, DNI, etc., para localizar información sobre nosotros en páginas webs y otras plataformas (INCIBE, 2021).

PELIGROS EN LOS ENTORNOS DIGITALES

El uso masivo de las tecnologías de la información se incrementó de manera exponencial en la pandemia y aceleró la transformación digital a nivel global hablar de trabajo e línea, video

conferencias, comercio en línea entre otros es tan común hoy en día, antes de la pandemia parecían tan distantes, esta masificación ha generado nuevos escenarios de riesgo que también son aprovechados por grupos criminales para realizar actividades ilícitas.

Riesgos

El entorno digital ha generado nuevas formas de vulnerabilidad y la exposición a riesgos, los principales riesgos presentes en los entornos digitales incluyen:

- **Riesgos de privacidad y manejo de la información confidencial**: tienen que ver con la preservación de los datos personales del usuario, como números de tarjeta de crédito o contraseñas.
- **Riesgos propios de la interacción con terceros:** tienen que ver con la manipulación sexual, el ciberacoso y otras actividades sociales peligrosas realizadas en línea.
- **Riesgos de acceso a información falsa o sensible:** tienen que ver con el acceso a la pornografía, el material cruento y mórbido, o también la información falsa (fake news).
- **Riesgos derivados del mal uso de internet:** Son todos aquellos otros riesgos derivados del mal uso de internet, como pueden ser la adicción psicológica, el aislamiento social, entre otros (Editorial Etecé, 2025).

Escenarios

Influenciados por la narcocultura (practicas, valores, creencias, actitudes y símbolos asociados a narcotraficantes), el uso masivo del internet exaltando a delincuentes, narcotraficantes y grupos delincuenciales legitimando o normalizando sus acciones, esto vinculado a la pobreza, la falta a de acceso a servicios básicos, la violencia doméstica, problemas de adicciones, falta de oportunidades económicas, discriminación social, necesidad de pertenencia forman un escenario favorable para el sexting, ciberacoso, fraude en línea, reclutamiento, estafas entre otros.

La privacidad en las comunicaciones, los juegos en línea, las apuestas deportivas digitales, las aplicaciones de mensajería instantánea, las redes sociales, las plataformas de citas son espacios propicios para el accionar anonimizado de delincuentes y grupos delictivos organizados.

En este sentido podemos identificar diferentes escenarios:

- **Juegos en línea:** Delincuentes identifican y seleccionan a víctimas generando confianza de los menores obsequiando dinero, recompensas (cajas de botín, vidas adicionales, armas, entre otras) pueden ser víctimas de sexting, pornografía incluso ser coaccionados para cometimiento de delitos; plataformas como Roblox, Fortnite, Free Fire están en la mira.
- **Apuestas deportivas digitales:** La proliferación de sitios de apuestas en línea concibe un nuevo problema para las niñas, niños y adolescentes (NNA), generando el riesgo como el desarrollo de problemas de adicción y ludopatía, implicando problemas como

endeudamiento con amigos, robos con el fin de obtener dinero para para apuestas, creando un comportamiento criminal que puede ser usado por organizaciones criminales para sus fines delincuenciales.

- **Redes sociales:** delincuentes gracias a la facilidad de crear un perfil falso y obtener muchos amigos sin necesidad de conocerlos establecen contacto con NNA a través de foros públicos y servicios de mensajería directa, esta exposición puede llevar a casos de ciberacoso, pornografía, extorsión, incluso reclutamiento resaltando los beneficios de unirse al grupo (dinero, status, entre otras), redes sociales como Twitch, Discord, Facebook, Instagram y TikTok son las más usadas para este fin.
- **Plataformas de citas:** adolescentes pueden establecer fácilmente conexiones emocionales fuertes con el fin de engancharlas, manipularlas, coaccionarlas o inducirlas para realizar cosas inapropiadas llegando al ámbito de cometer delitos, los delincuentes utilizan técnicas como el catfishing.

CASOS REALES DE PELIGROS DIGITALES

Sexting y temas relacionados

El sexting se define como el envío, recepción o reenvío voluntario de mensajes, fotografías o vídeos con contenido sexual explícito o sugestivo mediante el uso de dispositivos digitales y redes sociales. Aunque a menudo se presenta como una expresión de libertad sexual o una manifestación afectiva entre pares, esta práctica encierra un riesgo considerable cuando se realiza sin conciencia sobre los límites de privacidad y las consecuencias de su difusión. En un entorno caracterizado por la inmediatez y la viralidad, una sola imagen puede propagarse ilimitadamente, provocando graves daños psicológicos, sociales y jurídicos.

Ayúdanos a localizar más víctimas de un depredador en línea

¿Qué ocurrió?

Ashley cayó en la trampa de Chansler a finales de 2008, cuando tenía 14 años. Alguien que decía ser un adolescente la contactó en línea con fotos sexuales vergonzosas de ella. Su nombre de usuario era CaptainObvious, y la amenazó con enviar las fotos de Ashley a todos sus amigos de Myspace si no le enviaba una foto suya en topless. Sin pensar en las consecuencias, la envió. No creía que el chico supiera quién era ni nada sobre ella. No pasó nada más hasta el verano de 2009, cuando el personaje de Chansler volvió a enviarle un mensaje, amenazando con publicar su foto en topless en internet si no le enviaba imágenes más explícitas.

Al principio lo ignoró, pero luego él le envió un mensaje a su celular. Sabía su número y presumiblemente dónde vivía. De alguna manera, debió haber hackeado información de sus redes sociales. Chansler era implacable. La acosaba para que le diera fotos y seguía amenazándola. La idea de arruinar su reputación y decepcionar a sus padres hizo que Ashley finalmente cediera ante su acosador.

Los siguientes meses fueron una pesadilla mientras Ashley cumplía con las exigencias de Chansler. Estaba atrapada y sentía que no podía hablar con nadie. No dejaba de pensar que, si enviaba más fotos, el monstruo al otro lado de la computadora finalmente la dejaría en paz. Pero la cosa solo empeoró, hasta el día en que su madre descubrió las imágenes en su computadora (FBI, 2015).

Chansler, quien estudiaba farmacia, usó múltiples identidades y docenas de nombres de usuario falsos, como "HOLA" y "chicoguapo313", para engañar a chicas de 26 estados de EE. UU., Canadá y el Reino Unido.

Una menor realiza sexting y es suplantada para vender su contenido sexual.

Los adolescentes deben ser conscientes de que las prácticas de sexting tienen ciertos riesgos asociados. En este caso real una menor comparte unas fotos íntimas de forma voluntaria y acaba siendo suplantada en una red social para vender su propio contenido sexual.

¿Qué ocurrió?

En España, una orientadora educativa bastante preocupada porque tenía constancia de que a una menor de edad le habían suplantado la identidad, contó que la menor había tenido contacto a través de redes sociales con una persona desconocida con la que había compartido fotos y vídeos de carácter íntimo y sexual.

Posteriormente, esta persona abrió una cuenta en una red social con el nombre de la menor y vendía las fotografías y vídeos que ésta le había enviado, además de proporcionar otros datos privados y su cuenta de Instagram.

La menor había sido consciente de los hechos tras avisarle un compañero de clase.

La orientadora también explicó que había más menores del centro de educación que habían sufrido este tipo de situaciones y que sospechaba que era la misma persona que estaba

extorsionando a las pequeñas, aunque dudaban de que pudiera ser alguien del propio centro escolar.

Modus operandi del ciberdelincuente

Los ciberdelincuentes que practican sextorsión o grooming siguen patrones conductuales repetitivos:

- **Captación:** buscan víctimas en redes sociales, chats o videojuegos en línea, presentándose con identidades atractivas o afines a la edad del menor.
- **Vinculación emocional:** entablan conversaciones frecuentes para generar confianza y dependencia afectiva.
- **Obtención del material íntimo:** solicitan o inducen el envío de imágenes comprometedoras, alegando afecto o confianza mutua.
- **Chantaje o coerción:** amenazan con divulgar el material si la víctima no accede a sus exigencias (nuevas fotos, dinero o actos sexuales).
- **Difusión o explotación:** en los casos más graves, comercializan o distribuyen el contenido en redes clandestinas o plataformas de pornografía infantil.

El *modus operandi* descrito por Ferrazuola (2019) y Peris y Maganto (2018) muestra que la lógica del ciberdelincuente se basa en el engaño y la manipulación emocional, no en la fuerza física (Ferrazzuolo, 2019) (Peris & Maganto, 2018).

Además, la Dirección de Ciberdelitos ha desarrollado dos boletines de análisis sobre la Ciberdelincuencia relacionados a esta problemática denominados *"**Pederastia en el Entorno Digital o Grooming"*** y ***"Pornografía infantil y de adolescentes en el entorno digital"***, en el que se analizan escenarios y formas de captación, los entornos digitales más utilizados por los agresores, los factores que favorecen la victimización de NNA, y como proteger a los niños, niñas y adolescentes en el entorno digital; estos boletines son de acceso público se los puede en el canal oficial del ministerio del interior de la sección biblioteca/Dirección de Ciberdelitos/Análisis de la Ciberdelincuencia https://www.ministeriodelinterior.gob.ec/biblioteca/ .

Tipología del sexting

La literatura científica distingue varias modalidades según la naturaleza del contenido y el papel del participante:

- **Soft sexting:** intercambio de mensajes o imágenes de carácter sexual sugestivo.
- **Hard sexting:** envío o recepción de material con desnudos o actos sexuales explícitos.
- **Sexting activo:** cuando el sujeto produce y remite el contenido.
- **Sexting pasivo:** cuando el individuo recibe o almacena dicho contenido.

Estas categorías son relevantes porque muestran la amplitud del fenómeno, que puede comenzar con gestos aparentemente inofensivos y evolucionar hacia situaciones de coacción, humillación o explotación sexual cuando el material es redistribuido sin consentimiento.

Estrategias de prevención

a. Ámbito familiar y educativo

La educación sexual y digital temprana es fundamental. Padres y docentes deben abordar el sexting sin estigmatizarlo, promoviendo el diálogo sobre consentimiento, respeto y privacidad. El acompañamiento activo, no el control represivo, es clave para generar confianza y prevenir el silencio.

b. Ámbito institucional y jurídico

Las instituciones deben garantizar canales eficaces de denuncia y medidas rápidas para eliminar contenido íntimo difundido sin autorización. La legislación penal debe aplicarse con rigor, especialmente cuando se trata de material que involucra a menores, pues su difusión puede constituir delito de pornografía infantil.

c. Ámbito tecnológico

Las plataformas digitales deben implementar sistemas de verificación de edad, algoritmos de detección automática de material sexual no consentido y procedimientos ágiles para la retirada de contenido. Asimismo, deben promover la alfabetización digital, empoderando a los usuarios para gestionar su privacidad.

Prevención – Recomendaciones.

- **No ceder a ningún tipo de chantaje** en caso de que se produzca.
- **Cortar cualquier tipo de comunicación** con la persona a la que le envió las fotos, **reportándola y bloqueándola** en todas las plataformas desde las que se hubiese contactado (Instagram, correo electrónico, TikTok, etc.).
- **Contactarse con la plataforma (redes sociales, correo electrónico, etc.) en la que se encontraba el perfil falso** para informarles tanto de la suplantación de identidad como del contenido de abuso sexual infantil que se estuviere difundiendo en ella.
- **Guardar evidencias de lo ocurrido**, ya que constituye un delito muy grave por ser menor de edad y se podría considerar contenido de abuso sexual infantil.
- **Efectuar la denuncia** de forma presencial ante la autoridad competente.
- **Practicar egosurfing (navegar por Internet buscando información sobre uno mismo)**. En el caso de detectar alguna publicación indeseada, reportar a los proveedores de servicios implicados (sitios web, redes sociales, etc.) para solicitar la eliminación de contenidos.
- En caso de **detectar resultados indeseados en algún buscador, denunciar a la autoridad competente**.
- **Contactar con las familias** de todo(a)s lo(a)s menores afectado(a)s, para que fuesen conocedores de la situación.
- **Apoyar al o la menor** en esos momentos, haciéndole saber que no es culpable de lo sucedido y que tiene gente que le apoyaba

Manipulación digital

De acuerdo con la definición de la Real Academia Española, manipular es "*Intervenir con medios hábiles y, a veces, arteros, en la política, en el mercado, en la información, etc., con distorsión de la verdad o la justicia, y al servicio de intereses particulares.*"

En este sentido, la manipulación en entornos digitales se fundamenta en el control emocional de las personas mediante engaños que apelan a la confianza, el miedo o el afecto. Estas acciones suelen ser planificadas para influir en las emociones, decisiones o comportamientos de la víctima. En la mayoría de los casos, la manipulación es el punto de partida de fraudes financieros, extorsiones, abusos sexuales o procesos de captación ideológica.

Contacto engañoso por WhatsApp

¿Qué ocurrió?

Esta modalidad se caracteriza cuándo personas reciben mensajes por WhatsApp de un número desconocido que inicia la conversación apelando a la cercanía o mostrando un interés respetuoso. Desde el primer contacto, el tono amable y aparentemente empático despierta curiosidad y apertura, lo que lleva a mantener la conversación por cortesía, afinidad o interés sentimental.

La comunicación se vuelve más frecuente y personal, mientras el interlocutor observa las respuestas y los límites de la víctima. De esta manera, se establece un vínculo emocional que puede ser utilizado para obtener información e inducir acciones comprometedoras, donde pequeñas concesiones como compartir información o mantener el diálogo, se transforman en puntos de vulnerabilidad propicios para fraudes o chantajes.

Esta práctica corresponde a una forma de ingeniería social que se apoya en la manipulación emocional y el escalamiento de confianza, aprovechando la disposición natural de las personas a interactuar de forma amable y recíproca con personas de confianza.

Prevención - Recomendaciones:

- Conversar con los menores en casa sobre la naturaleza de los vínculos en línea: alertar ante personas que "te ofrecen entrar en un grupo exclusivo", "ganar dinero fácil" o "ser parte de algo grande" y lo más importante, ganarse la confianza de los menores o adolescentes para que puedan alertarnos a tiempo.
- Supervisar cuándo y dónde los menores usan chats, videojuegos o redes sociales. Dentro de lo posible evitar conocer personas por internet.
- Usar controles parentales, establecer límites de tiempo en línea, y revisar contactos.
- Contactar a autoridades locales si se solicita al menor participar, guardar capturas de pantalla o si le solicitan trasladarse a algún lugar sin consulta de los padres o tutores. (Europol, 2025)

- Evitar responder mensajes de números desconocidos que apelan a la cercanía o confianza. Este tipo de contacto puede activar un proceso de manipulación sin que la persona lo perciba.
- Si por alguna razón excepcional necesita responder, se debe previamente verificar la identidad del remitente por otro canal antes de continuar.
- Abstenerse de compartir fotos, ubicación, información familiar o detalles personales, aunque la conversación parezca genuina e inocente. Los delincuentes construyen la manipulación en base a la confianza.
- Ante insistencias, cambios en el tono o solicitudes de confidencialidad, bloquear y reportar el número en la aplicación. Estas señales indican un intento de control o influencia emocional.
- Denunciar ante las autoridades competentes o en canales oficiales.

(De Gree, 2025) (Santos , 2025)

Reclutamiento digital

Los entornos digitales son aprovechados por redes delictivas para captar y manipular a personas especialmente a niñas, niños y adolescentes, estos aprovechan la anonimidad, la facilidad de comunicación y el acceso masivo a la información personal, grupos delictivos organizados buscan reclutar principalmente a niñas, niños y adolescentes vulnerables mediante promesas de riqueza, aventura o simplemente generar sentimientos de pertenencia.

"El reclutamiento, uso y utilización de niñas y niños por parte de bandas de delincuencia organizada NUNCA es voluntario, y siempre es forzado". (Unicef, 2025)

Grupos irregulares usaron WhatsApp para reclutar a jóvenes

¿Qué ocurrió?

En Colombia, durante los confinamientos, los grupos armados usaron WhatsApp para invitar a jóvenes a fiestas clandestinas, que funcionaban como puerta de entrada a estructuras criminales. Los menores eran atraídos mediante pequeños créditos o, en ocasiones, por medio de secuestros. Esta tendencia continuó tras la pandemia: entre 2022 y 2024, las redes sociales como TikTok y Facebook se convirtieron en espacios claves para la captación de menores, de acuerdo con la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos en Colombia. (Sanjurjo, 2025)

Redes delincuenciales reclutan menores vía plataformas en línea

¿Qué ocurrió?

La Europol alertó que redes delictivas europeas están utilizando plataformas digitales para reclutar menores, ofreciéndoles inicialmente incentivos como amistad, "trabajo fácil", o reconocimiento; y luego solicitando su participación en actividades delictivas, por ejemplo,

transportar droga, cometer robos, distribuir propaganda. Los menores, manipulados emocionalmente y aislados, pasan de ser víctimas a cómplices.

Como actúan los reclutadores

Los reclutadores manipulan y explotan a los Niños, Niñas y Adolescentes mediante coerción psicológica y manipulación de algunos métodos como:

1. El método del "amante": los reclutadores pueden atraer a víctimas menores de edad colmándolas de elogios, atención y afecto excesivos para crear una falsa sensación de intimidad y conexión, y una sensación de apego y dependencia hacia el traficante.
2. Mentir y tergiversar los hechos o gaslighting: Esta técnica de control implica manipular la percepción que el niño tiene de la realidad, haciéndole dudar de sus propias experiencias o sentimientos.
3. Ofertas de trabajo o empleos falsos: Los reclutadores crean anuncios de trabajo engañosos en plataformas en línea o portales de empleo. Estas publicaciones pueden prometer puestos bien pagados o fáciles de obtener para atraer a posibles víctimas (Uitts, 2023).

Tabla 1: Principales estrategias de reclutamiento utilizadas

Estrategias de caza	Estrategias de pesca
Búsqueda proactiva de víctimas específicas (en redes sociales, salas de chat en línea o aplicaciones de citas) y compradores potenciales en línea.	Búsqueda pasiva de víctimas: publicación de anuncios en línea disponibles para todos (por ejemplo, anuncios de trabajo falsos o agencias de empleo falsas)
El traficante inicia el contacto basándose en información o características como vulnerabilidades económicas, emocionales u otras, lo que los hace susceptibles a la explotación.	Las víctimas inician el contacto respondiendo a anuncios en línea que prometen altos salarios u otros beneficios (por ejemplo, viajes) con poca información laboral.
Al principio amistoso, luego más agresivo a medida que se desarrolla la relación.	Publicitan ofertas de trabajo para atraer cualquier número de víctimas: anuncios clasificados en línea, plataformas de redes sociales, bolsas de trabajo y sitios web especializados en servicios sexuales.

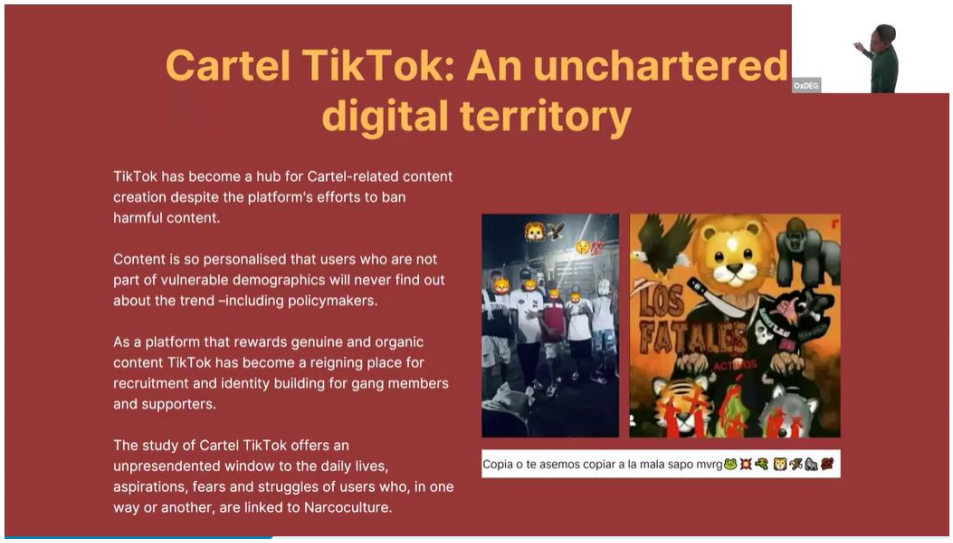
Fuente: Human Trafficking Front. https://humantraffickingfront.org/the-use-of-the-internet-to-recruit-children-by-traffickers/

Glocks, emojis de animales y 'Rulay': cómo bandas relacionadas con cárteles reclutan a jóvenes ecuatorianos a través de contenido viral en TikTok

Según un estudio publicado por Oxford Internet Institute, en el marco de la serie de seminarios del Grupo de Etnografía Digital de Oxford, se evidencia que grupos de delincuencia organizada están utilizando TikTok y otras redes sociales para captar a jóvenes ecuatorianos mediante la difusión de contenido que glorifica la violencia, el uso de armas y el dinero fácil (Brito , 2025). Para este fin, utilizan música, emojis, tendencias virales y otros códigos propios de la cultura juvenil, lo que les permite influir en adolescentes de manera indirecta, sin necesidad de contacto directo. Los investigadores desde el enfoque antropológico han desarrollado una metodología hibrida que combina la profunda investigación etnográfica (produciendo descripciones detalladas de las expresiones culturales de la cultura de las bandas digitales) con el entrenamiento y el despliegue de modelos de lenguaje a gran escala (LLMs). Este enfoque combinado permite una comprensión más matizada del fenómeno y, al mismo tiempo, posibilita escalar el análisis hacia grandes conjuntos de datos, revelando patrones de comportamiento más amplios dentro de los entornos digitales.

El seminario del antropólogo digital Gabriel Brito investigador visitante en Oxford Internet Institute aborda este fenómeno aún poco investigado relacionado al reclutamiento de bandas vinculadas con GDOs a través de las redes sociales, el seminario se encuentra disponible en el siguiente enlace: https://www.youtube.com/watch?v=cgatO9CvWgI o en la página del instituto https://www.oii.ox.ac.uk.

Figura 1: Estrategias principales de reclutamiento utilizadas por los traficantes



Fuente: Oxford Internet Institute https://www.oii.ox.ac.uk/news-events/videos/glocks-animal-emoji-and-rulay-how-cartel-related-gangs-recruit-young-ecuadorians-through-viral-content-on-tiktok/

Frente a esta problemática, resulta imprescindible fortalecer las capacidades estatales de monitoreo digital, análisis de contenidos y ciberinteligencia, además de promover la cooperación

con plataformas digitales, actualizar la normativa, desarrollar acciones de alfabetización digital y contra-narrativa que reduzcan el impacto de estos mensajes.

Para atender este fenómeno, la Subsecretaría de Combate al Delito, a través de la Dirección de Ciberdelitos del Ministerio del Interior, cuenta con tres herramientas técnicas "la Guía de Reporte de Contenido Inapropiado, la Guía Metodológica de Cibermonitoreo y el Manual de Actuación para el Tratamiento de Contenido Digital". Estos instrumentos establecen procedimientos para la identificación y gestión de contenido inapropiado, ilegal o dañino, apoyando el trabajo de inteligencia, preventivo e investigativo de la Policía Nacional que puedan derivar a procesos con la Fiscalía General del Estado.

Su aplicación permite mejorar la calidad de las investigaciones y articular la información obtenida en línea con las operaciones realizadas en territorio.

En conjunto, estas herramientas fortalecen la capacidad del Estado para detectar y desarticular redes delictivas que operan en el ciberespacio, protegiendo especialmente a niñas, niños, adolescentes y comunidades vulnerables ante estas formas de captación digital.

Prevención - Recomendaciones.

Para padres, cuidadores y comunidad educativa

- Supervisar y acompañar el uso de internet
- Establecer reglas claras:
  - ✓ No compartir datos personales
  - ✓ No enviar fotos o videos íntimos
  - ✓ No reunirse en persona con contactos en línea sin autorización
- Revisar privacidad en aplicaciones:
  - ✓ Perfil privado
  - ✓ Desactivar ubicación
  - ✓ Bloqueo de desconocidos
  - ✓ Promover comunicación abierta: Que los menores puedan pedir ayuda sin miedo
- Atender señales de alerta
  - ✓ Cambios de conducta y aislamiento
  - ✓ Secretismo con el celular
  - ✓ Nuevos "amigos" adultos o perfiles sin verificación
  - ✓ Presencia de regalos, dinero o viajes inexplicables

Para adolescentes y jóvenes

- Protege tu privacidad: todo lo que compartes puede ser guardado y usado contra ti

- No creas en promesas fáciles: Trabajo fácil, fama, regalos implica riesgos
- Confía en tu instinto: Si algo te incomoda, bloquea y reporta
- Si vas a ver a alguien:
  - ✓ En lugar público
  - ✓ Avisar a alguien de confianza
  - ✓ No aceptar transporte del contacto

Para instituciones y plataformas

- Mejorar detección de perfiles falsos y contenido de riesgo
- Implementar controles parentales y moderación
- Colaborar con entidades de protección y policía
- Campañas educativas y de denuncia

Otros casos relacionados al fenómeno

Venta fraudulenta de entradas para el concierto de un conocido cantante

En este caso real un ciberdelincuente contactó con su víctima aprovechando un comentario que la usuaria publicó en la cuenta oficial de Instagram del artista, en el cual se interesaba por la compra de unas entradas para su próximo concierto, puesto que estaban agotadas.

¿Qué ocurrió?

Una joven al no encontrar entradas disponibles, decidió poner un comentario en la cuenta de Instagram del artista, por si a algún fan le sobraba alguna o le interesaba venderlas.

Pasadas unas horas, un usuario le contactó afirmando tener dos entradas disponibles, proponiéndole continuar la conversación en WhatsApp.

A continuación, el ciberdelincuente le envió una solicitud de pago a través de un medio de pago digital o una cuenta bancaria y, aunque a la usuaria le pareció correcto, él afirmaba que hubo un error en el pago y le solicitó que repitiera la operación, resultando pagar el doble del precio inicial.

Al día siguiente el desconocido volvió a ponerse en contacto, asegurando que no podía facilitarle las entradas y que le devolvería todo el dinero.

A partir de entonces, el ciberdelincuente bloqueó a la usuaria.

Prevención – Recomendaciones.

- **Utilizar plataformas fiables y contrastadas**, que ofrezcan protección al comprador ante casos de fraude.
- **No mantener conversaciones ni hacer transacciones económicas fuera de la plataforma**.
- **Consultar las valoraciones** del vendedor y comprar a aquellos que tengan buena reputación.
- **No proporcionar información personal o bancaria**.

- **No acceder a ningún enlace ni descargar ningún fichero** que le puedan enviar.
- **No aceptar métodos de pago no seguros**.
- **Bloquear al usuario y reportarlo** en la plataforma.
- P**onerse en contacto con la entidad bancaria** para tomar las medidas de seguridad convenientes.
- **Recopilar todas las evidencias** posibles.
- **Interponer una denuncia** de forma presencial ante autoridad competente del Estado.
- **Denunciar a través de la Superintendencia de Bancos** si no se obtiene solución satisfactoria a través de la entidad bancaria.
- Con los datos que se ha facilitado podrían intentar defraudarle nuevamente.

Un menor usa la tarjeta bancaria sin permiso del titular para gastar en videojuegos.

La supervisión, contando, además, con la ayuda de herramientas de control parental, es clave a la hora de evitar situaciones como la de este caso real, en el que una madre sufrió pérdidas económicas a raíz de compras no autorizadas por parte de su hijo.

¿Qué ocurrió?

La madre de un menor preadolescente, muy preocupada porque tenía numerosos cargos en su tarjeta bancaria de cantidades de entre $30 y $50, llegando a ascender todos ellos a la cifra de $5000.

Informó que no reconocía las operaciones, pero que sospechaba que podrían haber ocurrido a raíz de tener su tarjeta vinculada a la PlayStation de su hijo, ya que los cargos aparecían como realizados desde la plataforma de PlayStation y desde Google Pay, habiendo también una suscripción a PlayStation Plus.

La madre indicó que había hablado con su hijo, pero que el menor negaba haber realizado dichas compras. Aun así, ella creía que había sido él, puesto que en ocasiones había recibido correos electrónicos que indicaban que su hijo contaba con más videojuegos y mejoras de los que ella había autorizado. Además, nos reconoció que no era la primera vez que su hijo tenía este tipo de comportamientos.

La persona explicó que anuló la tarjeta con la que se habían llevado a cargo los pagos, solicitando una nueva sin vincularla a su móvil. Sin embargo, había observado que se habían vuelto a realizar unos cargos similares a los que se realizaban en la tarjeta anulada.

Prevención - Recomendaciones.

- Intentar reclamar la devolución del pago en la plataforma web a través de la que se realizó la compra exponiendo la situación.
- Ponerse en contacto con su entidad bancaria, explicar la situación y solicitar:
    - ✓ Si es posible, la devolución del importe.

- ✓ El bloqueo de futuros cargos provenientes de las plataformas implicadas.
- ✓ En el caso de desconocer dónde está almacenada la información de la tarjeta, solicitar su cancelación.

- Valorar utilizar una tarjeta prepago, de un solo uso, o una tarjeta específica para las compras por Internet, y si es posible, activarla solo en los momentos precisos de uso.
- Contactar con Atención al Cliente de la plataforma utilizada.
- Anular la suscripción a plataforma utilizada si no se desea que el hijo siguiese contando con ella.
- Contactar con el Centro de Ayuda de Google Pay.
- Cambiar las contraseñas por otras robustas de todos los servicios (tanto del menor como de la persona adulta), por si finalmente los cargos no los estuviera realizando su hijo.
- Activar el doble factor de autenticación en todos los servicios que dispongan.
- Activar la solicitud de validación de pago en las plataformas que se lo permitan.
- Recopilar las evidencias de todo lo sucedido mediante capturas de pantalla de los correos, mensajes, facturas o justificantes de pago, etc.
- En el caso de llegar a la conclusión de que no había sido su hijo, valorar interponer una denuncia ante la autoridad pertinente.

Referente al menor:

- No culpabilizar a su hijo, dar apoyo incondicional en estos momentos.
- Mantener la calma y esperar a un momento de tranquilidad para dialogar.
- Hacer ver que no se trata de buscar culpables, sino de buscar soluciones.
- Potenciar habilidades como la tolerancia a la frustración y la asunción de responsabilidad en el menor.
- Plantearse consecuencias coherentes con el hecho.
- Instalar una herramienta de control parental en los dispositivos del menor.
- Supervisar de forma diaria su actividad para poder prevenir futuras situaciones problemáticas.
- Conocer el entorno tecnológico en el que se desenvuelve su hijo: qué videojuegos le interesan, cómo se comporta en el entorno digital, etc.
- Mantener las tarjetas, datos bancarios y contraseñas fuera del alcance del menor.
- Buscar ayuda especializada.

RECOMENDACIONES ANTE LOS PELIGROS EN ENTORNOS DIGITALES

Actúa de inmediato

- Si identificas comportamientos sospechosos, intentos de manipulación, acoso, sextorsión u otro riesgo digital, contacta de forma inmediata a las autoridades competentes.
- Recuerda que toda forma de violencia o amenaza en línea debe ser denunciada para activar mecanismos de protección.

Canales de ayuda

Fiscalía General del Estado: Para denuncias relacionadas con ciberdelitos y delitos cometidos por medio de las TIC.

ECU 911: Para reportar situaciones de emergencias relacionadass con entornos y riesgos digitales.

Policía Nacional: Aporta en la investigación de ciberdelitos y delitos cometidos por medio de las TIC, acercarse a la Unidad de Policial más cercana

1800 - Delito: Es un servicio telefónico de la Policía Nacional de Ecuador para que la ciudadanía reporte información sobre diversos delitos de forma anónima y confidencial 1800-delitos (1800-335 486).

CONCLUSIONES

Los entornos digitales generan nuevos escenarios de riesgo para niños, niñas y adolescentes (NNA). La expansión del internet, redes sociales, videojuegos, plataformas de citas y mensajería instantánea ha incrementado la exposición a amenazas como sexting, sextorsión, grooming, manipulación emocional, fraudes, suplantaciones y reclutamiento delictivo.

Los ciberdelincuentes actúan mediante manipulación psicológica y estrategias de ingeniería social, creando vínculos afectivos, confianza o dependencia para luego ejercer coerción, extorsión o explotación. El engaño, la empatía simulada y el chantaje son patrones comunes en los casos analizados.

Los escenarios sociales vulnerables como pobreza, narcocultura, violencia doméstica y falta de oportunidades aumentan la exposición de los NNA, generando contextos favorables para que grupos delictivos legitimen su accionar y utilicen el mundo digital como vía de captación.

El sexting y la sextorsión no pueden entenderse únicamente como desviaciones de conducta juvenil, sino como manifestaciones contemporáneas de vulnerabilidad digital. Estos fenómenos reflejan la tensión entre el deseo de comunicación íntima y la falta de límites en entornos tecnológicos. Abordarlos requiere una estrategia integral basada en tres pilares: educación, acompañamiento y sanción. La construcción de una cultura digital preventiva, donde la privacidad y la dignidad sean valores inquebrantables, permitirá reducir la victimización y fortalecer la resiliencia de niñas, niños y adolescentes frente a los riesgos del ciberespacio.

Bibliografía

Ayuda en acción. (05 de 08 de 2025). *Ciberbullying: qué es y cómo prevenirlo eficazmente*. Obtenido de https://ayudaenaccion.org/blog/educacion/ciberbullying/

De Gree, A. (13 de febrero de 2025). *Cómo identificar estafas en WhatsApp*. Obtenido de https://www.avast.com/c-identify-whatsapp-scams

Editorial Etecé. (24 de abril de 2025). *Riesgos de Internet*. Obtenido de https://concepto.de/riesgos-de-internet/#riesgos-de-privacidad-y-manejo-de-la-informacion-confidencial

Europol. (13 de noviembre de 2025). *Europol alerta sobre redes de delincuencia organizada que reclutan menores para actos delictivos.* Obtenido de https://www.europol.europa.eu/media-press/newsroom/news/europol-warns-of-organised-crime-networks-recruiting-minors-for-criminal-acts

FBI. (julio de 2015). *Help Us Locate Additional Victims of an Online Predator*. Obtenido de https://www.fbi.gov/news/stories/sextortion

Ferrazzuolo, V. (2019). *Era digital: delito y prevención.* Buenos Aires: Jusbaires.

Guardia Nacional CERT-MX. (02 de 07 de 2024). *¿Sabes qué es el Sexting y cómo prevenir riesgos?* Obtenido de https://www.gob.mx/gncertmx/articulos/sabes-que-es-el-sexting-y-como-prevenir-riesgos

Gurdian, N. (24 de enero de 2017). *Gaslighting: el abuso emocional más sutil*. Obtenido de https://psicologiaymente.com/social/gaslighting

INCIBE. (21 de 04 de 2021). *Egosurfing: ¿Qué información hay sobre mí en Internet?* Obtenido de https://www.incibe.es/ciudadania/blog/egosurfing-que-informacion-hay-sobre-mi-en-internet

INCIBE. (11 de 2025). *Fake news y bulos en la Red.* Recuperado el 12 de 11 de 2025, de https://www.incibe.es/menores/tematicas/fake-news-y-bulos

Missing & Explointed. (12 de noviembre de 2025). *Sextorsión*. Obtenido de https://www.missingkids.org/es/sextorsion

Peris, M., & Maganto, C. (2018). *Peris, M., & Maganto, C. (2018). Sexting, sextorsión y grooming.* Madrid: Ediciones Pirámide.

Proofpoitn. (8 de enero de 2024). *¿Qué es el catfishing?* Obtenido de https://www.proofpoint.com/es/threat-reference/catfishing

Sanjurjo, B. (03 de septiembre de 2025). *Preocupación en la región: crece el reclutamiento de menores por grupos criminales a través de entornos digitales.* Obtenido de https://www.infobae.com/america/america-latina/2025/09/03/preocupacion-en-la-region-crece-el-reclutamiento-de-menores-por-grupos-criminales-a-traves-de-entornos-digitales/

Santos , E. (01 de septiembre de 2025). *La Guardia Civil alerta de la estafa que empieza con una videollamada y con la que te pueden robar la cuenta*. Obtenido de https://www.huffingtonpost.es/sociedad/la-guardia-civil-alerta-estafa-empieza-videollamada-te-robar-cuenta.html

Uitts, B. (26 de septiembre de 2023). *The Use of the Internet to Recruit Children by Traffickers*. Obtenido de https://humantraffickingfront.org/the-use-of-the-internet-to-recruit-children-by-traffickers/

Unicef. (Junio de 2025). *Aproximación al reclutamiento de niños, niñas y adolescentes en Ecuador.* Obtenido de Unicef.org: https://www.unicef.org/ecuador/documents/aproximaci%C3%B3n-al-reclutamiento-de-ni%C3%B1os-ni%C3%B1as-y-adolescentes-en-ecuador

Unicef. (s.f.). *Grooming: qué es y cómo podemos proteger a los niños*. Recuperado el 12 de noviembre de 2025, de https://www.unicef.es/blog/salud-mental/grooming-que-es-y-como-podemos-proteger-los-ninos