

Detección, Interrupción e Investigación de la Explotación Sexual Infantil en Línea

USO DE INTELIGENCIA FINANCIERA PARA PROTEGER A LOS NIÑOS DEL DAÑO

© 2025 GAFI/OCDE. Todos los derechos reservados. Publicado por el Grupo de Acción Financiera Internacional (GAFI). www.fatf-gafi.org

Acrónimos

CSAM	Material de Abuso Sexual Infantil
EUR	Euro
GAFI	Grupo de Acción Financiera Internacional
ESIF	Extorsión Sexual e Infantil con Fines Financieros
ASVD	Abuso Sexual de Niños por Videotransmisión en Directo
LA	Lavado de Activos
STMV	Servicios de Transferencia de Moneda o Valor
ESIN	Explotación Sexual Infantil en Línea
P2P	Entre Pares (Peer-to-Peer)
PSAV	Proveedor de Servicios de Activos Virtuales
VPN	Red Privada Virtual

Definiciones

Abusador	Individuo distinto del facilitador que comete el abuso sexual de niños por videotransmisión en directo.
Ciberengaño (Catfishing)	Proceso de atraer a alguien a una relación mediante una persona ficticia en línea. En el contexto de la extorsión sexual, se usa para atraer a víctimas potenciales hacia relaciones en línea con un propósito específico.
Captura (Capping)	Grabación del material de abuso sexual infantil transmitido en directo, incluyendo material generado con fines económicos o material generado por los propios niños bajo coacción, que luego se difunde en línea.
Niño/a	Persona menor de 18 años.
Consumidor	Individuo que realiza un pago a un facilitador para ver el abuso sexual de niños en directo, a veces dirigiendo la naturaleza del abuso. Generalmente ubicado en un lugar diferente al lugar donde ocurre el abuso.
País de Destino	País donde se reciben en última instancia las transacciones financieras relacionadas con la ESIN, realizadas por un consumidor o por una víctima de extorsión sexual.
Facilitador	Individuo que organiza el abuso sexual de niños por videotransmisión en directo. En algunos casos, también actúa como abusador.
Perpetrador	El individuo, o grupos de individuos, que llevan a cabo la extorsión sexual e infantil con fines financieros.
Rescate	Monto exigido para que un perpetrador de extorsión sexual deje de publicar, o deje de amenazar con publicar, el material sexualmente explícito de una víctima.
País de Origen	País desde donde se origina una transacción financiera relacionada con la ESIN.
Adolescente	Persona de entre 13 y 17 años, inclusive.

Víctima

El niño o niña sometido/a a la explotación sexual en línea.

Tabla de Contenidos

Acrónimos	2
Definiciones	2
Resumen Ejecutivo	4
Introducción	6
Alcance	7
Metodología	8
Sección 1: Escala, Demografía e Ingresos de la Explotación Sexual Infantil en Línea	9
Contexto Global	10
Abuso Sexual de Niños por Videotransmisión en Directo	11
Extorsión Sexual e Infantil con Fines Financieros	13
Sección 2: Detección de la Explotación Sexual Infantil en Línea	17
Identificación de Transacciones Financieras Vinculadas al ASVD	18
Identificación de la ESIF a través de Transacciones Financieras	20
Sección 3: Investigación de la Explotación Sexual Infantil en Línea	22
Detección e Identificación del ASVD y la ESIF	23
Buenas Prácticas en la Investigación y Disrupción del ASVD y la ESIF	28
Sección 4: Recuperación de Activos Vinculados a la ESIN	35
Recuperación de Activos Vinculados a la ESIN	36
Sección 5: Desafíos, Recomendaciones, Oportunidades y Conclusión	38
Desafíos	39
Recomendaciones	40
Oportunidades	42
Conclusión	43
Anexo A: Identificación de Transacciones Financieras Vinculadas a la ESIN	44

Resumen Ejecutivo

A nivel mundial, investigadores estiman que 300 millones de niños en todo el mundo, es decir, 1 de cada 8 niños, son víctimas de abuso y explotación sexual en línea anualmente.

La explotación sexual infantil en línea, o el uso de internet para cometer o facilitar la explotación sexual de un niño/a, se está convirtiendo rápidamente en una tendencia delictiva dominante, compleja y habilitada por medios cibernéticos, centrada en víctimas. Estos delitos tienen consecuencias devastadoras, graves y duraderas sobre las víctimas y sus familias. Este informe examina dos tipos diferenciados de explotación sexual infantil en línea:

RECUADRO 1 – Tipos de Explotación Sexual Infantil en Línea

Abuso Sexual de Niños por Videotransmisión en Directo (ASVD) – La transmisión del abuso sexual de niños/as con fines lucrativos. Específicamente, la transmisión o difusión en tiempo real de cualquier material que muestre a un niño/a en actividad sexual, solo o con otras personas, que los consumidores pagan para ver de forma remota.

Extorsión Sexual e Infantil con Fines Financieros (ESIF) – La amenaza de exponer imágenes o videos sexualmente explícitos de un niño/a a menos que satisfaga demandas económicas.

La escala, el alcance y la trayectoria de estos delitos son alarmantes. A nivel global, investigadores de la Universidad de Edimburgo estiman que 300 millones de niños en el mundo, es decir, 1 de cada 8, son afectados por el abuso y la explotación sexual en línea anualmente. El Informe Resumen de Tendencias del Crimen Global de INTERPOL de 2022 encontró que la explotación y el abuso sexual infantil en línea se ubicaron entre las diez principales tendencias delictivas percibidas como una amenaza "alta" o "muy alta" por los países miembros. No solo representa una amenaza significativa para los niños hoy en día, sino que la trayectoria de los casos aumenta de forma alarmante. Ese mismo informe de INTERPOL encontró que el 62% de los países miembros esperaba con firmeza que estos delitos "aumenten" o "aumenten significativamente" en el futuro. En 2024, estos delitos permanecieron en la categoría de amenaza alta para los países miembros, agravados en particular, desde el último período, por el mayor uso y proliferación de tecnologías de comunicación cifrada.

Este informe tiene como objetivo proporcionar una comprensión actualizada y más precisa de los flujos financieros relacionados con la explotación sexual infantil en línea, explorando el abuso sexual de niños por videotransmisión en directo y la extorsión sexual e infantil con fines financieros. Esta comprensión mejorada ofrecerá oportunidades para vincular transacciones financieras con delincuentes, y detectar e intervenir de manera más temprana en situaciones de explotación sexual infantil en línea.

Este informe proporciona buenas prácticas para detectar y desarticular la explotación sexual infantil en línea. Dado el alto nivel de daño presente, es fundamental que las técnicas investigativas utilizadas atiendan las necesidades de los niños en riesgo y que se desarrollen y apliquen estrategias de

investigación centradas en la víctima. Se alienta a los países a desarrollar estrategias investigativas que reduzcan la dependencia del testimonio de la víctima para asegurar resultados operativos. Al poner a la víctima en el centro de la estrategia investigativa, las autoridades pueden minimizar el daño, que es el objetivo último de la prevención del delito.

El abuso sexual de niños por videotransmisión en directo y la extorsión sexual e infantil con fines financieros se encuentran en un período de escalada alarmante. Este informe concluye identificando los desafíos en la detección, interrupción e investigación de la explotación sexual infantil en línea, y proporciona recomendaciones a las partes interesadas, incluidos los miembros de la Red Global del GAFI, sobre cómo pueden mejorar su comprensión y capacidad para combatir estos delitos en el futuro.

Introducción

Alcance

Este informe tiene como objetivo proporcionar una comprensión actualizada y más precisa de los flujos financieros relacionados con la explotación sexual infantil en línea, explorando el abuso sexual de niños por videotransmisión en directo y la extorsión sexual e infantil con fines financieros. Este informe brinda información sobre la detección, interrupción e investigación de la explotación sexual infantil en línea.

Este informe utiliza los siguientes términos clave para referirse a esta actividad:

RECUADRO 2 – Definiciones de Términos Clave

Explotación Sexual Infantil en Línea (ESIN) – Los múltiples usos de las tecnologías de la información y la comunicación ('internet') para cometer o facilitar la explotación sexual de un niño/a.

Abuso Sexual de Niños por Videotransmisión en Directo (ASVD) – La transmisión del abuso sexual de niños/as con fines lucrativos. Específicamente, la transmisión o difusión en tiempo real de cualquier material que muestre a un niño/a en actividad sexual, que los consumidores pagan para ver de forma remota.

Extorsión Sexual e Infantil con Fines Financieros (ESIF) – La amenaza de exponer imágenes o videos sexualmente explícitos de un niño/a a menos que satisfaga demandas económicas.

Los delitos de ESIN forman parte de la definición del Glosario del GAFI de 'categorías designadas de delitos', ya que incluyen la explotación sexual de niños y pueden también involucrar, en algunos casos, participación en un grupo delictivo organizado, fraude, trata de personas y extorsión. La inclusión bajo esta definición significa que la consideración de tales delitos está dentro del ámbito del GAFI, y la respuesta de una jurisdicción a los flujos financieros y los beneficios asociados a la ESIN podría ser considerada en el Informe de Evaluación Mutua de esa jurisdicción.

Este informe deliberadamente no cubre delitos similares que no tienen motivación financiera.

Metodología

Este proyecto del GAFI fue co-liderado por delegaciones de Australia y el Reino Unido. El equipo del proyecto estuvo integrado por delegaciones de Brasil, Canadá, Côte d'Ivoire, la Comisión Europea, India, Indonesia, Irlanda, Luxemburgo, México, los Países Bajos, Singapur y España. El equipo del proyecto también contó con miembros del Grupo Asia-Pacífico sobre Lavado de Dinero (APG), el Grupo Egmont e INTERPOL.

La metodología consistió en una revisión y refinamiento del material existente disponible sobre ESIN, que incluyó:

- Una revisión bibliográfica para identificar tendencias recientes en la naturaleza y el alcance de la ESIN, con enfoque en el ASVD y la ESIF, y los flujos financieros asociados.
- Dos solicitudes a los miembros de la Red Global del GAFI para proporcionar material relevante al equipo del proyecto, incluyendo productos de inteligencia estratégica, informes y/o estudios de caso que brindaran información sobre las características, métodos, tendencias e indicadores del ASVD y la ESIF, así como ejemplos de mejores prácticas actuales e innovaciones para detectar, desarticular e investigar la ESIN.

No existe una cifra confiable que estime los ingresos generados por el abuso sexual de niños por videotransmisión en directo a nivel global; sin embargo, hay evidencia clara de que este tipo delictivo es de gran escala y se vuelve cada vez más prevalente.

Sección 1:

Escala, Demografía e Ingresos de la Explotación Sexual Infantil en Línea

1: ESCALA, DEMOGRAFÍA E INGRESOS

Contexto Global

La ESIN es un delito atroz que se aprovecha de las personas más vulnerables de la sociedad: los niños. El surgimiento de esta tendencia ha sido impulsado por desarrollos sociales: el acceso de los niños a internet, las redes sociales y las plataformas de juegos, y la movilidad que la tecnología moderna permite para acceder a contenido prácticamente ilimitado. Estos desarrollos han llevado a los niños de hoy a enfrentarse a riesgos diferentes a los de cualquier otra época de la historia. La ESIN es uno de esos riesgos, y uno que se ha vuelto dramáticamente más pronunciado en los últimos años.

Aunque este tipo delictivo habilitado cibernéticamente y centrado en víctimas continúa evolucionando y existe cierto cuerpo de trabajo que lo describe, su prevalencia e impacto, aún no existe una definición codificada a nivel mundial para este tipo de delito. En consecuencia, diversos actores de gobiernos nacionales, organizaciones internacionales, el mundo académico y la sociedad civil han realizado estimaciones de la prevalencia de esta actividad utilizando definiciones y alcances ligeramente diferentes.

Escala – A nivel global, investigadores de la Universidad de Edimburgo estiman que 300 millones de niños en todo el mundo, es decir, 1 de cada 8, son afectados por el abuso y la explotación sexual en línea anualmente. El Informe Resumen de Tendencias del Crimen Global de INTERPOL de 2022 encontró que la explotación y el abuso sexual infantil en línea se ubicaron entre las diez principales tendencias delictivas percibidas como amenaza "alta" o "muy alta" por los países miembros. Los hallazgos estratégicos de INTERPOL de 2024 muestran que estos delitos permanecieron en la categoría de amenaza "alta" para los países miembros, agravados en particular desde 2022 por el mayor uso y proliferación de tecnologías de comunicación cifrada.

Trayectoria – El Informe Resumen de Tendencias del Crimen Global de INTERPOL de 2022 encontró que el 62% de los países miembros esperaba con firmeza que estos delitos "aumenten" o "aumenten significativamente" en el futuro. Las fuerzas del orden globales perciben que la evolución del *modus operandi* criminal para desarrollar materiales de abuso infantil, captar audiencias y ganancias, distribuir contenido a escala y evadir la detección se ha intensificado. Además, los hallazgos estratégicos de INTERPOL de 2024 han subrayado el creciente número de casos de extorsión sexual de niños, que involucran tanto la coerción de contenido sexual como el beneficio económico.

Estos hallazgos sobre la escala y trayectoria global son alarmantes en sí mismos. Sin embargo, se vuelven mucho más preocupantes al considerar este tipo delictivo. La ESIN tiene consecuencias devastadoras sobre las víctimas y sus familias, que las impactan a lo largo de toda su vida, son a menudo graves y duraderas, y en algunos casos han llevado a niños a quitarse la vida. Un solo niño que enfrente tales consecuencias ya es demasiado, y todas las partes interesadas deben poner todos los medios disponibles a disposición para mitigar este riesgo para los niños.

Fuentes: <https://www.ed.ac.uk/news/2024/scale-of-online-harm-to-children-revealed-in-globa> | Informe Resumen de Tendencias del Crimen Global de INTERPOL 2022 | Informe Resumen de Tendencias del Crimen Global de INTERPOL 2024

Abuso Sexual de Niños por Videotransmisión en Directo

Metodologías del Abuso Sexual de Niños por Videotransmisión en Directo

El ASVD es un delito habilitado cibernéticamente que abarca una variedad de infracciones, incluyendo la explotación sexual y la trata de personas, ambas consideradas categorías designadas de delitos en el Glosario del GAFI. El delito involucra a individuos que desempeñan los siguientes roles para organizar el abuso sexual de la víctima menor, incluyendo forzarla a realizar actividad sexual frente a una cámara web u otro dispositivo:

- **Abusador** – Individuo distinto del facilitador que comete el abuso sexual de niños por videotransmisión en directo.
- **Consumidor** – Individuo que realiza un pago a un facilitador para ver el abuso sexual de niños en directo, a veces dirigiendo la naturaleza del abuso. Generalmente ubicado en un lugar distinto al lugar donde ocurre el abuso.
- **Facilitador** – Individuo que organiza el abuso sexual de niños por videotransmisión en directo. En algunos casos, también actúa como abusador.

Este abuso se transmite en directo a un consumidor remoto que paga para verlo y potencialmente dirigirlo. El consumidor que paga para ver el abuso accede a través de las personas que organizan el abuso y puede también ser un abusador en sí mismo. La evidencia sugiere que existen diferentes clases de consumidores: algunos son consumidores habituales, mientras que otros pueden ser consumidores circunstanciales, es decir, que originalmente no buscaban ver material de abuso infantil.

Los consumidores y facilitadores se comunican a través de aplicaciones de mensajería, incluyendo aplicaciones ampliamente conocidas como Skype, WhatsApp, Facebook y Telegram, para acordar una fecha y hora con anticipación y negociar el precio. Cuando se produce el abuso, el abusador somete a la víctima a actos sexuales y/o la fuerza a realizarlos y/o la incentiva a participar en dichos actos, a veces dirigidos por el consumidor con anterioridad al abuso y/o durante la transmisión en directo. En algunos casos, el abuso transmitido en directo es grabado y difundido en línea a una audiencia más amplia. Esta práctica se denomina coloquialmente "captura" (capping). Esto puede responder a diversos motivos, entre ellos que el material de abuso sexual infantil nuevo o inédito es una moneda de cambio valiosa dentro de la comunidad de infractores, o para generar mayores ganancias subiendo el material a la dark web o a sitios de cyberlocker donde el contenido puede descargarse por una tarifa. Esta captura representa una mayor criminalidad y una re-explotación y abuso de la víctima.

La detección del ASVD es difícil ya que la mayoría de las plataformas de interacción social tienen capacidades de transmisión en directo, y los moderadores de contenido tienen capacidades limitadas para revisar volúmenes masivos de interacciones y chats en tiempo real que son temporales dentro de un volumen de millones o cientos de millones de instancias.

El ASVD está motivado principalmente por el beneficio económico. Si bien las sumas involucradas tienden a parecer pequeñas, el vendedor puede someter al niño a abusos sexuales en línea repetidos, lo que puede generar beneficios sustanciales con el tiempo.

Perfil de Víctimas, Consumidores, Abusadores y Facilitadores del Abuso Sexual de Niños por Videotransmisión en Directo

Víctimas

Las víctimas del ASVD generalmente no están involucradas en las transacciones financieras que permiten su abuso. Son personas vulnerables sujetas a violencia que probablemente tendrá un impacto a largo plazo en sus vidas. Las víctimas no han sido perfiladas con mayor detalle, ya que no es necesario a los efectos de este informe para apoyar a las partes interesadas en el uso de sus herramientas para apuntar a los consumidores, facilitadores y abusadores.

Consumidores

Se cree que los consumidores que pagan por el ASVD son típicamente hombres y, si bien varían en edad, los consumidores típicos tienden a ser hombres mayores. Sin embargo, esto puede no representar con precisión la demografía de los consumidores, ya que los consumidores más jóvenes pueden ser más hábiles para ocultar su actividad o pagos en línea.

Los consumidores detectados que pagan por el ASVD son predominantemente de Australia, Europa y América del Norte. Estos infractores buscan el abuso transmitido en directo apuntando a regiones del mundo con medidas nacionales de protección infantil limitadas y fácil acceso a los niños. A diferencia de los abusadores y facilitadores del ASVD, los consumidores están motivados sexualmente, no económicamente.

Abusadores y Facilitadores

Tanto hombres como mujeres son abusadores y facilitadores del ASVD. Estos roles se superponen en algunos casos y, por lo tanto, pueden compartir algunas características comunes. En los casos en que el/los abusador/es y facilitador/es son conocidos de la víctima (p. ej., padre/madre o familiar), es más probable que sean mujeres jóvenes (alrededor de los 20 años). En muchos casos en que se trata de una mujer, tiene hijos menores propios, así como otros niños a los que puede tener acceso. Cuando hay más de un individuo involucrado en el abuso, los infractores pueden tener diferentes roles en el delito: (1) comunicarse con el consumidor, (2) llevar a cabo el abuso y (3) cobrar los pagos.

Los abusadores y facilitadores del abuso sexual transmitido en directo generalmente se encuentran en el mismo lugar que la víctima menor, debido a la proximidad necesaria para cometer el delito. Según investigaciones concluidas, una gran proporción de abusadores y facilitadores se encuentran en el Sudeste Asiático. Mientras que una gran cantidad de víctimas, abusadores y facilitadores se concentran en el Sudeste Asiático, existen casos en los que el facilitador, el abusador y su/s víctima/s se encuentran en otras regiones, como América del Norte, Europa y la región de Oriente Medio y Norte de África.

Ingresos obtenidos y lavados a través del Abuso Sexual de Niños por Videotransmisión en Directo

No existe una cifra confiable que estime los ingresos generados por el ASVD a nivel global; sin embargo, existe evidencia clara de que este tipo delictivo es de gran escala y se vuelve cada vez más prevalente. Los casos concluidos y los reportes de víctimas brindan una idea de los ingresos generados a través del ASVD y cómo se lavan.

Las transacciones relacionadas con instancias de este delito se caracterizan típicamente por montos pequeños que se pagan por consumidores principalmente en Australia, Europa y América del Norte a jurisdicciones de alto riesgo para la explotación sexual infantil. Los montos de las transacciones individuales pueden considerarse bajos para el consumidor (normalmente entre 10 y 200 EUR por instancia), pero los montos pueden ser sustanciales para el abusador y el facilitador, que a menudo se

encuentran en un país en desarrollo. El facilitador también puede maximizar los ingresos generados por este delito desarrollando una relación con el consumidor, asegurándose de que se convierta en un consumidor recurrente. En algunos casos, el facilitador puede lograr persuadir al consumidor para que envíe dinero para otros gastos, como facturas médicas.

Los pagos por estos servicios se realizan típicamente a los facilitadores a través de Servicios de Transferencia de Moneda o Valor (STMV) populares, predominantemente sistemas de pago en línea entre pares (P2P) como PayPal, o a veces a través de transferencias bancarias directas o transferencias de activos virtuales (AV) a través de proveedores de servicios de activos virtuales (PSAV). Estos últimos pueden proporcionar un mayor anonimato percibido para el consumidor.

Si bien los grupos del crimen organizado no suelen estar involucrados en estos delitos debido a la falta de grandes ganancias, existe cierta evidencia de estructuras comerciales criminales en países en desarrollo que explotan las oportunidades comerciales que presenta el ASVD remunerado.

Los facilitadores y abusadores generalmente utilizan mecanismos de lavado poco sofisticados debido a la falta de grandes ganancias y al flujo lento de pagos en denominaciones pequeñas. Estos incluyen la simple conversión de transacciones internacionales en efectivo o depósitos bancarios para el gasto diario. Los facilitadores y abusadores más significativos han sido observados comprando bienes de consumo con sus ganancias ilícitas, incluyendo propiedades, electrónica y automóviles.

Si bien el componente financiero puede ser pequeño en comparación con otros tipos de delitos importantes, descubrir y entender el componente financiero de este delito puede ayudar a las autoridades operativas a identificar y proteger a las víctimas, así como a identificar, desarticular y perseguir judicialmente a los infractores.

Extorsión Sexual e Infantil con Fines Financieros

Metodologías de la Extorsión Sexual e Infantil con Fines Financieros

La ESIF es un delito habilitado cibernéticamente y centrado en la víctima que combina fraude, extorsión y explotación sexual. Los niños/as no son necesariamente objetivos intencionales, sino que son atrapados por perpetradores que buscan cualquier víctima posible. El delito generalmente implica que una víctima sea contactada inicialmente por un perpetrador desconocido a través de las redes sociales. Los testimonios de víctimas indican que el primer contacto ocurre principalmente a través de Snapchat, Instagram y Facebook, aunque otras plataformas pueden ser más prominentes en determinadas regiones del mundo.

Este perpetrador desconocido generalmente engaña a la víctima adoptando una identidad falsa, normalmente la de un/a adolescente o una persona de alrededor de 20 años (también conocido como ciberengaño o catfishing). Los perpetradores pueden crear sus propios perfiles falsos o utilizar perfiles existentes hackeados o comprados. Al crear nuevos perfiles, pueden usar bots y scripts, o interactuar con otras cuentas hackeadas para fabricar evidencia de uso y participación en la cuenta, llevando a las víctimas a creer que el perpetrador es un usuario auténtico.

El perpetrador se comunica con la víctima utilizando diversas técnicas para despertar su interés en la identidad falsa adoptada. Las técnicas para manipular a la víctima se despliegan generalmente muy rápido, en minutos o pocas horas, en lugar de técnicas de grooming a largo plazo observadas en otros tipos de abuso sexual infantil. Una vez que el interés de la víctima ha alcanzado un nivel apropiado, a menudo estimulado por recibir contenido sexualmente explícito de la identidad falsa del perpetrador, se le invita a intercambiar fotografías o videos sexualmente explícitos, o a unirse a una videollamada sexualmente explícita que es grabada o capturada en pantalla. Los perpetradores intentan llevar a la

víctima de la plataforma original a plataformas cifradas de extremo a extremo.

Una vez que el perpetrador tiene el material sexualmente explícito de la víctima, usa ese material para amenazarla o coaccionarla para que envíe dinero (un rescate). Teniendo acceso a su presencia en redes sociales, puede chantajearla con amenazas de enviar el material explícito a sus pares, familiares u otros miembros de la comunidad en línea. Estas amenazas son generalmente agresivas y pueden involucrar múltiples cuentas de redes sociales bombardeando a la víctima al mismo tiempo. Esta presión rápida a través de técnicas de ingeniería social está diseñada para aprovechar la vulnerabilidad de la víctima y convencerla rápidamente de pagar un rescate por las imágenes.

Este {i('modus operandi')} ha resultado atractivo para los perpetradores por varias razones: puede cometerse desde cualquier lugar del mundo, generalmente requiere una inversión mínima de tiempo por víctima potencial, la percepción de anonimato permite distanciarse del delito, y el número casi ilimitado de víctimas potenciales hace que siempre haya nuevas oportunidades de ganancias ilícitas.

Perfil de Víctimas y Perpetradores de la Extorsión Sexual e Infantil con Fines Financieros

Víctimas

Las víctimas de la ESIF son en su mayoría adolescentes varones, aunque hay un número creciente de mujeres y niñas objetivo. Los perpetradores pueden apuntar a cualquier víctima, pero tienen más éxito con víctimas con conexiones significativas en redes sociales, como las que están conectadas a equipos deportivos, clubes u otros grupos sociales, de modo que puedan identificar amigos o contactos a quienes amenazar con enviar las imágenes.

Las víctimas son de todo el mundo. Hasta la fecha, en el contexto internacional, la mayoría de los perpetradores han apuntado principalmente a hablantes nativos de inglés, ya que los perpetradores que llevan a cabo esta actividad aún no han alcanzado la sofisticación necesaria para operar en muchos idiomas. Esta sofisticación puede desarrollarse con el tiempo con el uso de tecnologías emergentes.

Perpetradores

El perfil de los perpetradores de la ESIF varía considerablemente del de la extorsión sexual con motivación sexual. Los perpetradores de la ESIF generalmente trabajan solos, aunque se han observado grupos o equipos que utilizan metodologías comunes. Estos grupos o equipos generalmente involucran tanto a hombres como a mujeres, aunque con una proporción muy significativa de miembros masculinos. Estas organizaciones actúan tanto doméstica como internacionalmente.

Las ubicaciones geográficas de los perpetradores han variado con el tiempo con la emergencia de este tipo delictivo. Algunos de los países más afectados por estos perpetradores, como Estados Unidos, Canadá y Australia, han realizado análisis de denuncias de víctimas. Estas denuncias muestran generalmente que Nigeria, Filipinas y Côte d'Ivoire son las ubicaciones más comunes de los perpetradores identificados.

RECUADRO 3 – Metodología de la ESIF en los Países Bajos

Dos niños (B.T. y S.Q.) recibieron un mensaje de WhatsApp de alguien desconocido con diferentes números. B.T. recibió directamente un mensaje con una foto de una mujer en ropa interior. Después de enviar una foto semidesnuda propia, recibió un Tikkie de €15, que pagó. Inmediatamente recibió un mensaje que dejaba claro que la persona del otro número había descubierto quién era (su nombre y fotos de su página de Facebook), basándose en el nombre asociado a la cuenta bancaria con la que pagó el Tikkie. Siguió un Tikkie de €150, con la amenaza de que su foto sería enviada a sus amigos y familiares si no pagaba. B.T. pagó también este Tikkie. Rápidamente recibiría más Tikkies de diferentes números de teléfono. Los montos oscilaban entre €20 y cientos de euros. En total, B.T. pagó €3.500 en Tikkies. B.T. envió entonces un mensaje diciendo que se le estaba agotando el dinero, tras lo cual se le pidió que enviara una captura de pantalla del resumen de su cuenta bancaria como prueba. Esto mostraba que le quedaban €300. Se le pidió que comprara tarjetas de regalo con el dinero restante y que enviara los códigos correspondientes por WhatsApp.

La niña (S.Q.) recibió una foto de un hombre desnudo después de chatear con la persona durante un tiempo. S.Q. envió fotos desnudas de sí misma, tras lo cual recibió inmediatamente un mensaje con una captura de pantalla de sus fotos, pidiéndole que pagara dinero. Si no pagaba, las fotos serían enviadas a sus amigos y familiares. Recibió un Tikkie de €50, que pagó de inmediato. La persona que enviaba los Tikkies descubrió su nombre a partir del nombre asociado a la cuenta bancaria vinculada a los pagos. Siguió más Tikkies, que S.Q. también pagó. Tras un tiempo, se le agotó el dinero, lo que tuvo que demostrar con capturas de pantalla de su historial de transacciones. Estas mostraron que estaba mintiendo, por lo que siguieron más Tikkies. En total, pagó €470 a tres cuentas bancarias diferentes en un plazo de 71 minutos.

Fuente: Países Bajos

Ingresos obtenidos y lavados a través de la Extorsión Sexual e Infantil con Fines Financieros

Los rescates individuales de las víctimas a los perpetradores se perciben como de valor relativamente bajo (50-1.500 EUR), con rescates iniciales generalmente inferiores a 250 EUR. Esto puede deberse a que las víctimas objetivo son generalmente adolescentes que no tienen medios financieros significativos. Los perpetradores a veces buscan pagos de rescate adicionales de las víctimas después del pago inicial. Sin embargo, tales acuerdos son generalmente de corta duración ya que el efectivo disponible se agota rápidamente, aunque es común que las víctimas sean luego forzadas a convertirse en mulas de dinero para los perpetradores.

Los medios para enviar los pagos de rescate son generalmente directos pero poco sofisticados. Al igual que con el ASVD, los rescates también se pagan utilizando STMV, predominantemente sistemas de pago P2P en línea como PayPal, o a veces a través de transferencias bancarias directas o transferencias de activos virtuales a través de PSAV. Para la ESIF, hay una proporción mucho mayor de fondos pagados a los perpetradores en tarjetas prepagadas, créditos a plataformas de juegos y tarjetas de regalo.

Las transacciones de rescate pueden ser muy difíciles de detectar porque los montos y detalles de las transacciones son generalmente poco llamativos. En adición a los pagos realizados directamente de las víctimas a los perpetradores, también hay evidencia del uso de personas intermediarias o mulas que reciben el pago en su nombre.

Si bien los pagos individuales de rescate pueden percibirse como pequeños, los ingresos totales para los perpetradores pueden ser significativos dado el tiempo mínimo de inversión que se realiza en cada víctima potencial. Los ingresos totales para los perpetradores se lavan generalmente a través de mecanismos simples, como la conversión del rescate en gastos cotidianos. Los patrones de transacciones de los perpetradores muestran que estos gastan un porcentaje mayor de fondos en línea

que la población general, incluyendo compras generales en línea, compras de aplicaciones, juegos y apuestas en línea.

Sección 2:

Detección de la Explotación Sexual Infantil en Línea

2: DETECCIÓN DE LA EXPLOTACIÓN SEXUAL INFANTIL EN LÍNEA

Esta lista de indicadores también está disponible en el Anexo A para facilitar su uso. Debe tenerse en cuenta que los indicadores vinculados a la detección de la ESIN están en constante evolución, y las jurisdicciones deben continuar informando y fortaleciendo estos indicadores a través de la colaboración continua entre sus UIF, entidades obligadas, fuerzas del orden y otras partes interesadas.

Identificación de Transacciones Financieras Vinculadas al Abuso Sexual de Niños por Videotransmisión en Directo

Como se indicó anteriormente, los consumidores que pagan por ver el ASVD utilizan típicamente STMV populares, predominantemente sistemas de pago en línea P2P como PayPal. Si bien menos común, algunos consumidores realizan depósitos bancarios directos o transfieren activos virtuales a través de PSAV. Las entidades obligadas que brindan o facilitan estos servicios financieros pueden detectar transacciones que puedan estar vinculadas a casos de ASVD utilizando una combinación de los indicadores que se detallan a continuación:

Indicadores Generales de Transacciones Relacionadas con el Abuso Sexual de Niños por Videotransmisión en Directo

- Transacciones desde países desarrollados hacia jurisdicciones de alto riesgo para la explotación sexual infantil.
- Diferencias de edad significativas entre remitentes y receptores.
- Transacciones de montos bajos (entre 10 y 200 EUR por instancia), en denominaciones exactas en moneda del país de origen o destino.
- Pagos realizados a receptores en otra jurisdicción con quienes el remitente no tiene una conexión legítima aparente.
- Transacciones realizadas a intervalos irregulares pero de forma repetida a cuentas el mismo día o en días sucesivos.
- Transacciones realizadas tarde en la noche o muy temprano en la mañana (señalando que el consumidor puede encontrarse en un huso horario diferente).
- El propósito de la transacción hace referencia a redes sociales, nombres de usuario, términos sexuales o pornográficos, o la fecha/hora en que se recibió el material.
- Historial financiero extendido caracterizado por pagos durante un período prolongado, señalando que se ha formado una relación a largo plazo entre el consumidor y el facilitador.
- La transacción puede describirse como destinada a gastos médicos o de subsistencia o referirse a relaciones entre el remitente y el receptor. Por ejemplo, descriptores como "apoyo familiar", "cuotas

escolares", "asistencia", "apoyo", "facturas médicas", "alojamiento", "educación", "asistencia financiera", "regalo", "compra de ropa", "compra de juguetes", "uniforme", "amigo", "novio", "novia" o "patrocinador".

- Compras en proveedores que ofrecen herramientas de cifrado en línea, servicios de VPN, software para borrar rastros en línea, u otras herramientas o servicios de privacidad y anonimato en línea.
- Cuentas o clientes con un alto volumen de transacciones hacia Facebook, Microsoft, Google Play, OnlyFans, TikTok, Instagram u otros sitios de redes sociales.
- Transacción vinculada a una persona incluida en un registro público de delincuentes sexuales.

Transacciones Realizadas por Consumidores

- Transacciones realizadas a cuentas ubicadas o accedidas en jurisdicciones de alto riesgo para el ASVD.
- Compras en plataformas de citas o plataformas que ofrecen contenido de entretenimiento para adultos.
- Compras en plataformas de webcam/videotransmisión, incluidas las que ofrecen entretenimiento para adultos.
- Compras en plataformas de juegos en línea o tiendas de videojuegos.
- Compras de software de captura de video.
- Fondos enviados o recibidos de una persona imputada por delitos relacionados con la explotación sexual infantil.
- Transacciones vinculadas a una persona que es objeto de medios negativos relacionados con delitos de explotación sexual infantil.

Transacciones Realizadas por Facilitadores/Abusadores

- Las remesas de dinero generalmente se retiran de inmediato.
- Los receptores están bajo investigación policial por sospecha de ser parte de la facilitación de la explotación sexual infantil en línea.
- Pagos por funciones o servicios premium en plataformas de redes sociales.
- Compras de software de captura de video para uso en sitios web o redes sociales.
- Transacciones en plataformas de juegos en línea o tiendas de videojuegos.
- Adquisición de spyware o aplicaciones de vigilancia.
- Múltiples depósitos de montos similares rastreados a fuentes extranjeras, particularmente de países consumidores de alto riesgo de ASVD.
- Pagos a proveedores/plataformas de alojamiento de archivos en línea.
- Compras en sitios web de transmisión de contenido creativo (p. ej., membresías o suscripciones a estos sitios).

Identificación de la Extorsión Sexual e Infantil con Fines Financieros a través de Transacciones Financieras

Como se detalla anteriormente, la mayoría de las víctimas reportan haber pagado rescates a facilitadores a través de STMV, transferencias bancarias, activos virtuales a través de PSAV o tarjetas de regalo. Las entidades obligadas que brindan estos servicios tienen la capacidad de detectar

transacciones que puedan ser indicativas de ESIF utilizando una combinación de los indicadores que se enumeran a continuación:

Indicadores Generales de Transacciones Relacionadas con la Extorsión Sexual e Infantil con Fines Financieros

- Transacciones realizadas entre dos personas sin relación aparente.
- Transacciones generalmente inferiores a 500 EUR, pero a veces de hasta 1.500 EUR, en denominaciones exactas.
- La transacción inicial entre remitente (víctima) y receptor (perpetrador) generalmente inferior a 250 EUR.
- Múltiples transacciones de un remitente a un receptor en un corto período de tiempo que luego cesan completamente.
- Transacciones realizadas a un país de operación común de perpetradores de ESIF (p. ej., Côte d'Ivoire, Nigeria, Filipinas). Las entidades obligadas deben tener en cuenta la tendencia cambiante de los países donde predominantemente ocurre esto con el tiempo.
- El propósito de la transacción hace referencia a redes sociales, nombres de usuario, términos sexuales o pornográficos, lenguaje amenazante/suplicante o la fecha/hora en que se recibió el material.
- El receptor de la transacción no es local al remitente.
- Los detalles del pago parecen una donación benéfica.
- Transacción vinculada a una persona incluida en un registro público de delincuentes sexuales.

Transacciones Realizadas por Víctimas

- Transacciones realizadas por un adolescente o joven adulto varón y, en menor medida, adolescente o joven adulta mujer.
- Transacciones originadas en países predominantemente de habla inglesa, si son internacionales.
- Recepción de denuncias de personas sobre vínculos de transacciones con extorsión sexual.
- Pagos que ocurren típicamente entre las 19 hs. y las 7 hs. (generalmente mientras la extorsión sexual está ocurriendo en tiempo real).
- El remitente (víctima) no ingresa el nombre del beneficiario o ingresa un nombre que no coincide con el titular real de la cuenta.
- Reducción de fondos en las cuentas del remitente en pocas horas (generalmente menos de 24 horas).
- Compra no característica de tarjetas de regalo digitales o créditos de juegos.
- Usos no característicos de cuentas de plataformas P2P del individuo.
- Compra no característica de activos virtuales.
- Cuando el personal bancario le hace preguntas, el remitente es evasivo u ofrece una explicación implausible de la actividad.
- Cliente comprando múltiples tarjetas de regalo (p. ej., Amazon, PlayStation u otros proveedores de juegos).

Transacciones Realizadas por Perpetradores

- Una cuenta que recibe múltiples transacciones aparentemente no vinculadas entre sí.

- La cuenta receptora tiene múltiples motivos no relacionados identificados para las transacciones recibidas.
- Los montos recibidos son retirados rápidamente de la cuenta.
- Pagos a servicios en línea que ofrecen privacidad y/o anonimato (p. ej., cifrado, VPN, números de teléfono virtuales).
- Pagos asociados a múltiples tarjetas de crédito prepagadas o tarjetas de regalo.
- Recepción de fondos de múltiples servicios de comercialización de alojamiento de archivos en línea en diferentes jurisdicciones.
- Compra de bienes (vehículos, bienes raíces, electrodomésticos) en un corto período de tiempo, sin justificación para los medios utilizados.
- Personas con un estilo de vida y consumo inconsistente con los ingresos de su actividad laboral.

Sección 3:

Investigación de la Explotación Sexual Infantil en Línea

3: INVESTIGACIÓN DE LA EXPLOTACIÓN SEXUAL INFANTIL EN LÍNEA

Detección e Identificación del Abuso Sexual de Niños por Videotransmisión en Directo y la Extorsión Sexual e Infantil con Fines Financieros

La denuncia por parte de las víctimas es una vía clave de detección de muchos delitos, pero no es así en el caso de la ESIN. En el caso de la ESIF, si bien la denuncia por parte de las víctimas puede ser un medio de detección, las víctimas a menudo se sienten avergonzadas y son vulnerables a la extorsión porque quieren evitar que otros sepan que han compartido imágenes explícitas. Esto puede llevarlas a no querer denunciar la extorsión, y la inteligencia ha demostrado que la ESIF es un delito vastamente subdenunciado.

La denuncia de víctimas es un medio de detección aún menos común para el ASVD. Esto se debe a barreras relacionadas con el perfil de las víctimas, por ejemplo su edad, vulnerabilidad, acceso a medios de denuncia, pero también a factores como la coacción o la presencia de relaciones familiares en el entorno del abuso. En el caso del ASVD, el método de detección predominante, ya sea de la actividad del consumidor o del facilitador, es la recepción de inteligencia de otros países.

Uso de Información Financiera

La Sección 2 establece los indicadores que pueden utilizarse para identificar transacciones relacionadas con el ASVD o la ESIF. Reportar estas transacciones identificadas a las Unidades de Inteligencia Financiera (UIF) y a las fuerzas del orden es un medio fundamental de detección de la ESIN.

La inteligencia financiera obtenida durante las investigaciones o a través de las UIF también juega un papel clave en la detección y desarticulación de infractores que viajan internacionalmente para cometer delitos sexuales en el exterior. La experiencia de la Policía Federal Australiana muestra que una gran proporción de consumidores de ASVD procederán a cometer delitos de contacto en el exterior. Cuando se superpone con otras fuentes de datos, como los informes de CyberTipline del Centro Nacional para Niños Desaparecidos y Explotados (NCMEC) de los Estados Unidos, la inteligencia financiera puede ayudar a construir perfiles más precisos de posibles infractores, que luego pueden compartirse con las agencias nacionales de seguridad fronteriza o con los socios internacionales de aplicación de la ley.

RECUADRO 4 – Uso de Información Financiera para Investigar la ESIN

UIF de Indonesia (PPATK) aprovechando información financiera: Con base en información recibida por la PPATK, se demostró que un ciudadano neozelandés, el Sr. X, había enviado fondos a Filipinas, Vietnam, los Emiratos Árabes Unidos e Indonesia desde 2021. Las transacciones son sospechosas de ser para el pago de imágenes relacionadas con la explotación sexual infantil. Las descripciones de las transacciones incluyen "regalo", "fotos y diversión" y "transferencia de prueba". La base de datos de la PPATK encontró que el Sr. X realizaba activamente transacciones a mujeres en Indonesia con pequeños montos de frecuencia recurrente. La Sra. A, una de las destinatarias de fondos, a menudo usaba descripciones de transacciones sospechosas y realizaba transacciones con personas con perfiles de propietarios y empleados en los sectores hotelero, de karaoke y de entretenimiento. La Sra. A también reside en una zona turística, Bali, propensa a casos de ESIN. La Sra. A recibió fondos de hombres en varios países a través de remesas de dinero por un total de IDR 173 millones (aproximadamente €10.000). **Fuente: Indonesia**

Proyecto Sombra de Canadá (Project SHADOW): Es una asociación público-privada canadiense co-liderada por Scotiabank y el Centro Canadiense para la Protección de la Infancia, con el apoyo de organismos policiales canadienses y FINTRAC, la UIF de Canadá, para combatir la explotación sexual infantil en línea. A través de esta asociación, FINTRAC pudo identificar y compartir indicadores financieros para apoyar a las entidades obligadas en el reconocimiento de transacciones financieras sospechosas de estar relacionadas con el lavado de fondos vinculados a la ESIN. Los indicadores financieros de FINTRAC se utilizaron en un caso de ESIF, donde una víctima envió un video sexualmente explícito de sí misma a un individuo que conoció en línea. El individuo (perpetrador) amenazó con difundir el video si no enviaba CAD \$400. La víctima envió el dinero, y el incidente también fue denunciado a las fuerzas del orden, que luego enviaron información sobre el delito a FINTRAC. **Fuente: Canadá**

Derivaciones del Sector Privado

Tanto el ASVD como la ESIF dependen fundamentalmente de la infraestructura en línea para facilitar los delitos. La infraestructura relevante para la ESIN incluye plataformas de redes sociales, proveedores de servicios de internet, operadores de redes móviles, aplicaciones de mensajería, servicios en la nube, redes de distribución de contenidos, navegadores y tiendas de aplicaciones, entre otros. Este sector privado está en una posición particular para detectar la ESIN directamente y, en algunos casos, en tiempo real.

El CyberTipline del NCMEC es una organización sin fines de lucro con sede en EE. UU. que puede actuar como canal para que los proveedores de servicios electrónicos presenten informes de sospechas de ESIN en los Estados Unidos y otras jurisdicciones, los cuales luego se ponen a disposición de las fuerzas del orden de todo el mundo. Aunque casi 36 millones de informes del CyberTipline de sospecha de explotación sexual en línea de menores fueron realizados al NCMEC en 2023, estos provenían de solo 245 empresas, con 5 de estas empresas representando más del 91% de los informes.

RECUADRO 5 – Detección e Investigación mediante Informes del CyberTipline

CyberTipline del NCMEC: Es un sistema de reporte centralizado para informar sobre la sospecha de explotación sexual en línea de menores. El público y los proveedores de servicios electrónicos pueden realizar informes sobre sospecha de atracción en línea de menores con fines sexuales, abuso sexual infantil, material de abuso sexual infantil, turismo sexual infantil, trata sexual infantil, materiales obscenos no solicitados enviados a un menor, nombres de dominio engañosos e imágenes o palabras digitales engañosas en internet.

Uso de los Informes del CyberTipline por parte de Noruega: El NCMEC denunció a la Persona A ante el distrito policial de Øst y el Servicio Nacional de Investigación Criminal de Noruega, bajo sospecha de pago por el abuso sexual de niños menores de 14 años transmitido en directo desde Filipinas. En los dispositivos electrónicos del sospechoso se encontraron varios chats que demostraban que efectivamente pagaba para ver el abuso sexual de niños menores de 14 años transmitido en directo desde Filipinas. Como resultado de esta investigación, Noruega compartió información con las autoridades filipinas sobre los facilitadores. Como resultado, la Policía Nacional de Filipinas arrestó al menos a cinco facilitadores y protegió a varios niños de nuevos abusos sexuales. La Persona A fue condenada a 14 años de prisión y debió pagar una indemnización por daños a dos de las víctimas, por un total de NOK 500.000 (aprox. 42.000 EUR). **Fuente: Noruega**

RECUADRO 6 – Sistema de Eliminación 1930 de India

El "Sistema de Eliminación 1930" de India es un marco y plataforma estructurados para abordar diversos delitos habilitados cibernéticamente, incluyendo la ESIN. Las víctimas pueden denunciar estos delitos a través del portal de cibercriminalidad (www.cybercrime.gov.in) o la línea de ayuda dedicada 1930. Todos los informes se envían a cyberpolice.nic.in, que se conecta al panel de control de los organismos policiales para su investigación y acción. Los organismos policiales de India, utilizando este panel de control, coordinan solicitudes de eliminación de contenido dañino, reportado por bots especializados en redes sociales y otras plataformas en línea. Los consejos de otras fuentes, como el NCMEC, se agregan y analizan a través de herramientas de filtrado basadas en IA. Estos casos se almacenan en la Base de Datos de Delincuentes Cibersexuales, lo que ayuda a rastrear a los infractores conocidos y prevenir reincidencias. Estos datos también se integran en un panel de control más amplio para el monitoreo, mapeo y gestión de casos en tiempo real en todas las regiones.

Fuente: India

Trabajo Encubierto en Línea

El alto nivel de daño presente en muchos casos de ESIN y la naturaleza de estos delitos significa que, en ciertos casos, puede ser proporcionado y apropiado utilizar medios encubiertos para detectar e identificar la comisión de delitos de ESIN. En algunos casos, las fuerzas del orden pueden hacerse pasar por niños o como posibles consumidores para construir relaciones con facilitadores, abusadores, consumidores y perpetradores, a fin de recopilar información, evidencia e identificar víctimas. Las acciones realizadas por las fuerzas del orden durante las operaciones encubiertas en línea deben estar de acuerdo con los principios básicos de las leyes, políticas y procedimientos vigentes.

Buenas Prácticas en la Investigación y Disrupción del Abuso Sexual de Niños por Videotransmisión en Directo y la Extorsión Sexual e Infantil con Fines Financieros

Investigación

Estrategia de investigación centrada en la víctima

Dado el alto nivel de daño presente, es fundamental que las técnicas investigativas utilizadas atiendan las necesidades de las víctimas a través de una respuesta informada sobre el trauma y se aplique una estrategia de investigación centrada en la víctima. La prioridad en las investigaciones siempre debe ser la protección de los niños. Se alienta a los países a desarrollar estrategias investigativas que reduzcan la dependencia del testimonio de la víctima para asegurar resultados operativos. Los enfoques basados en

la inteligencia financiera y la interceptación de pagos pueden ofrecer vías de investigación menos angustiantes y reducir la dependencia del testimonio de la víctima, que a menudo resulta re-traumatizante.

Uso de fuentes de información y evidencia únicas para este tipo delictivo

El uso estándar de información y fuentes de evidencia se aplica a la investigación de estos delitos; por ejemplo, una amplia gama de datos nacionales puede utilizarse en la identificación de víctimas e infractores, como datos de inmigración e impuestos, información sobre sistemas nacionales de bienestar social, datos de crimen e inteligencia, datos de salud y atención social, y registros penales.

Sin embargo, existe especificidades en la evidencia y la información relevante para investigar el ASVD y la ESIF. Por ejemplo, la naturaleza generalmente internacional de estos delitos significa que la información a menudo necesita desplegarse a través de fronteras y la evidencia es a menudo inherentemente transfronteriza. Otro aspecto específico es el papel fundamental de los datos de comunicaciones, tanto en el ASVD como en la ESIF. Los informes de las agencias de aplicación de la ley indicaron que las derivaciones iniciales a menudo solo identificaban nombres de usuario, direcciones IP y direcciones de correo electrónico. Por lo tanto, para traducir estas derivaciones en identificación de víctimas e infractores, es imperativo que los organismos policiales se relacionen con las autoridades responsables del acceso a los datos de comunicaciones.

La Operación O de la Agencia Nacional del Crimen del Reino Unido fue desencadenada por un paquete de inteligencia que incluía no solo transacciones financieras y material de video/imágenes de abuso sexual infantil, sino también chats de Skype. En el caso de la Operación O en el Reino Unido, la colaboración estrecha e intercambio de inteligencia con las autoridades de Filipinas fue crucial para identificar a más facilitadores y víctimas.

La Unidad Nacional de Delitos Especiales de Dinamarca experimentó con el uso de tecnología de reconocimiento facial para comparar imágenes de víctimas con imágenes de una base de datos de víctimas previamente identificadas. Esta tecnología ha sido implementada como una herramienta permanente para aumentar la velocidad de identificación de víctimas en casos de abuso sexual infantil.

Inicio de grupos de trabajo multiagenciales

Cuando se realizan investigaciones grandes, y particularmente internacionales, se debe considerar el uso de grupos de trabajo multiagenciales para garantizar el manejo efectivo de la investigación. Desde 2020, el Centro Australiano para Contrarrestar la Explotación Infantil (ACCCE) ha organizado Grupos de Trabajo de Identificación de Víctimas de fuerzas del orden nacionales e internacionales para analizar material con el fin de identificar a víctimas del abuso sexual infantil. En 2022, uno de estos grupos de trabajo fue creado para apuntar a los criminales de captura más activos en foros de la dark web, con participantes de Australia, Canadá, Nueva Zelanda, Noruega, Estados Unidos, Europol e INTERPOL, entre otros. Como resultado, 77 víctimas fueron derivadas a 12 países diferentes y se derivaron 10 infractores.

RECUADRO 7 – Operación Guardián Cibernético

Entre el 26 de febrero de 2024 y el 29 de marzo de 2024, la Policía de Singapur, la Policía de Hong Kong y la Agencia Nacional de Policía de Corea iniciaron una operación conjunta internacional, la Operación Guardián Cibernético, y colectivamente arrestaron a 272 personas en 236 ubicaciones en las tres jurisdicciones por delitos relacionados con la ESIN. Durante esta operación de un mes de duración, estos socios internacionales detectaron casos de ESIN y protegieron a varios niños retenidos en cautiverio.

Fuente: Singapur, Corea y Hong Kong (China)

RECUADRO 8 – Actuando sobre la Difusión Proactiva de Inteligencia

La Policía en Jersey recibió un paquete de inteligencia de un tercer país tras la desarticulación de una red de trata infantil con base en Filipinas. La investigación identificó a un hombre de Jersey que había hecho contacto con la red y había realizado pagos por imágenes de abuso sexual infantil en línea. También se descubrió que el sospechoso había viajado a Filipinas para abusar de niños en persona. Se encontró que el software de videoconferencia Skype había sido utilizado, y los exámenes de las conversaciones de chat de Skype indicaron que el sospechoso había estado comunicándose con niñas y pagándoles para realizar espectáculos sexualmente explícitos. Los chats también mostraban que el sospechoso había realizado pagos para añadir crédito a varios números de teléfono móvil en pesos filipinos a través de PayPal. El sospechoso fue condenado posteriormente por posesión de imágenes indecentes de niños. Falleció en prisión.

Fuente: Dependencia de la Corona Británica de Jersey (Reino Unido)

Investigaciones paralelas

Este informe ha encontrado que los ingresos y flujos involucrados en el ASVD y la ESIF son a menudo modestos, particularmente en comparación con otros delitos generadores de ingresos; sin embargo, las investigaciones deben aún buscar oportunidades para investigar los delitos de lavado de activos (LA) además de centrarse en el delito primario de ESIN. Las investigaciones paralelas se centran en la investigación simultánea del delito predeterminado de ESIN y el delito de LA, lo que une la experiencia de ambos ámbitos investigativos.

Realizar una investigación financiera paralela del delito de ESIN puede permitir la identificación de los ingresos del crimen (es decir, activos criminales). Más críticamente, sin embargo, en el caso de la ESIN, la investigación financiera puede proporcionar el vínculo entre la fuente del dinero, quién lo recibe, cuándo se recibe y dónde se almacena o deposita, como prueba de actividad criminal. También puede ayudar a las autoridades competentes a descubrir e identificar a todos los participantes en una empresa criminal.

Disrupción

Tanto el alto nivel de daño generado por la ESIN como los desafíos para su detección, denuncia e investigación, hacen que exista un papel central para iniciativas sistemáticas de disrupción de la ESIN, no solo iniciativas que interrumpan casos individuales. Dos vías para la disrupción de la ESIN son la disrupción financiera y la disrupción de la infraestructura.

La **Operación Cazador (Operation Huntsman)** en Australia, liderada conjuntamente por AUSTRAC (UIF) y el ACCCE, es un ejemplo de disrupción exitosa de la infraestructura financiera que sustenta la ESIF. La operación identificó miles de "mulas bancarias" nacionales, que a menudo resultaron ser personas vulnerables y víctimas en sí mismas, en algunos casos de prolongadas estafas románticas. La mayoría de estas mulas también fueron identificadas como facilitadoras de una amplia variedad de delitos de fraude de alto valor monetario. La acción contra su participación en la ESIF comprometió su utilidad para permitir delitos de mayor valor por parte de los perpetradores, disminuyendo su red de mulas nacionales y el acceso a medios eficientes y de bajo costo para recibir fondos extorsionados o fraudulentos. Esto ha ayudado a crear un entorno en línea hostil para los perpetradores que apuntan a niños en Australia, forzándolos a depender de proveedores de "finanzas como servicio" más costosos o, más incómodamente, de tarjetas de regalo. Como resultado, el ACCCE está viendo una disminución en los informes e instancias de ESIF en Australia.

Las plataformas de redes sociales y otras formas de infraestructura en línea también son vectores primarios para el ASVD y la ESIF. Meta, por ejemplo, reportó en julio de 2024 haber eliminado alrededor de 63.000 cuentas de Instagram en Nigeria que intentaban dirigirse a individuos para la ESIF.

Sección 4:

Recuperación de Activos Vinculados a la Explotación Sexual Infantil en Línea

4: RECUPERACIÓN DE ACTIVOS VINCULADOS A LA ESIN

Recuperación de Activos Vinculados a la Explotación Sexual Infantil en Línea

Uno de los medios más efectivos para combatir el crimen con motivación financiera es ir tras los activos de quienes han cometido los delitos. Las leyes de recuperación de activos se emplean frecuentemente en casos de narcotráfico, lavado de activos, fraude y corrupción. Si bien la búsqueda de la recuperación de activos puede ser más típica en estas áreas, también se pueden considerar oportunidades para usar las leyes de recuperación de activos para apuntar a los ingresos, instrumentos y beneficios relacionados con la ESIN.

RECUADRO 9 – Persecución de Vivienda Vinculada a la Explotación Sexual Infantil en Línea

Ejemplo 1: En los últimos años, el Grupo de Trabajo de Confiscación de Activos Criminales (CACT) de la Policía Federal Australiana (AFP), trabajando junto con el ACCCE, el Equipo de Respuesta a la Explotación Sexual Infantil (CSERT) de AUSTAC y los Equipos Conjuntos contra la Explotación Infantil (JACETs), ha tomado medidas específicas para perseguir los activos de los infractores involucrados en la ESIN. Utilizando la Ley de Ingresos del Crimen del Commonwealth de Australia de 2002, el CACT ha adoptado una estrategia específica para castigar y disuadir a los infractores que crean y/o consumen material de explotación infantil, confiscando los ingresos, instrumentos y beneficios de sus delitos. Un caso complejo en 2022 resultó en que un hombre australiano fuera sentenciado a 15 años de prisión por una serie de delitos de abuso infantil, incluyendo ASVD, que resultó en la protección de 15 jóvenes víctimas en Filipinas. El hombre pagó por el abuso sexual de niños en Filipinas mientras observaba e instruía por webcam desde su casa en Australia. El CACT obtuvo órdenes de restricción sobre la vivienda del hombre a finales de 2020. Los procedimientos de recuperación de activos del CACT contra la vivienda del hombre se finalizaron en 2022, con el hombre realizando un pago financiero equivalente a la mitad del valor de la vivienda a la Cuenta de Activos Confiscados del Commonwealth. Este caso fue la primera vez que el CACT buscó confiscar la vivienda de una persona acusada de delitos sexuales contra menores.

Ejemplo 2: En 2023, un hombre de 34 años fue condenado en Australia por acceder y poseer material de explotación sexual infantil y condenado a 3 años de prisión. Más de 6.000 imágenes y videos de explotación sexual infantil fueron localizados en los dispositivos electrónicos y de almacenamiento del hombre, encontrados en su hogar. El CACT obtuvo una orden de restricción sobre la vivienda en marzo de 2024, y fue exitosamente confiscada al Commonwealth en junio de 2024. La vivienda, con un valor de aproximadamente AUD \$375.000, será vendida y las ganancias netas serán destinadas a la Cuenta de Activos Confiscados del Commonwealth, que se utiliza para financiar diversas iniciativas de prevención del crimen y seguridad comunitaria, incluyendo el programa australiano de educación en seguridad infantil en línea ThinkUKnow.

Fuente: Australia

RECUADRO 10 – Ordenando la Restitución

En abril de 2024, Samuel Ogoshi y Samson Ogoshi, quienes fueron extraditados de Nigeria a los Estados Unidos en agosto de 2023, se declararon culpables de conspiración para explotar sexualmente a adolescentes varones. Los acuerdos de declaración de culpabilidad describen los roles integrados desempeñados por Samuel y Samson Ogoshi en la creación de perfiles falsos, la atracción y extorsión de víctimas. Desarrollaron un esquema fraudulento en el que pretendían ser una joven mujer en perfiles de redes sociales y alentaban a adolescentes varones y jóvenes adultos a participar en conductas sexualmente explícitas y producir imágenes de esa conducta. Una vez que las víctimas producían y enviaban esas imágenes, los Ogoshi usaban esas imágenes para chantajear a sus víctimas por dinero, amenazando con enviar las imágenes a otros, incluyendo familiares, amigos y compañeros de clase. Los Ogoshi apuntaron a más de 100 adolescentes varones y jóvenes adultos, al menos uno de los cuales se suicidó como resultado del devastador impacto que la extorsión sexual puede tener sobre las víctimas. Como parte de su acuerdo de declaración de culpabilidad, se ordenó a los Ogoshi pagar restitución a sus víctimas, incluida la familia de la víctima que se quitó la vida. En septiembre de 2024, los acusados fueron sentenciados a 210 meses de prisión seguidos de 5 años de supervisión liberada.

Fuente: Estados Unidos de América

Sección 5:

Desafíos, Recomendaciones, Oportunidades y Conclusión

5: DESAFÍOS, RECOMENDACIONES, OPORTUNIDADES Y CONCLUSIÓN

Desafíos en la Detección, Interrupción e Investigación de la Explotación Sexual Infantil en Línea

Desafíos actuales

Falta de comprensión global integral sobre el alcance y escala de la ESIN – Aún no existen definiciones claras y coherentes de los tipos de delitos que abarca la ESIN. Tampoco, por ende, estimaciones globales confiables sobre los ingresos de la ESIN, el ASVD o la ESIF. Esto puede minimizar el impacto percibido de estos delitos y la comprensión de los flujos financieros ilícitos relacionados. Las jurisdicciones no están considerando (o no están considerando suficientemente) estos tipos delictivos al identificar y evaluar sus riesgos nacionales de LA.

Tecnología – La tecnología continúa evolucionando y expandiéndose a un ritmo exponencial. La prevalencia creciente de activos virtuales, incluyendo activos virtuales con anonimato mejorado, así como el cifrado extremo a extremo creciente de las comunicaciones, está creando barreras adicionales para la detección de la ESIN.

Intercambio de información interno incompleto – Para alcanzar una comprensión sólida de estos delitos y detectarlos, investigarlos y prevenirlos con éxito, es fundamental que las autoridades competentes y el sector privado trabajen de la mano, pero también que las autoridades competentes cooperen efectivamente entre sí. El intercambio de información actualmente es incompleto y no está optimizado de manera consistente para detectar, investigar y prevenir la ESIN.

Barreras en el intercambio internacional de información – Muchas de las barreras en el intercambio interno de información se aplican igualmente a nivel internacional. La inconsistencia en los marcos legales sobre la ESIN, y la medida en que el ASVD y la ESIF están explícitamente tipificados en las jurisdicciones, puede obstaculizar la colaboración transfronteriza.

Detección multiplataforma – Se ha observado que los infractores operan sin problemas en una variedad de plataformas de redes sociales e instituciones financieras. Sin la capacidad de compartir información entre plataformas de redes sociales e instituciones financieras, es difícil obtener una visión precisa de las actividades de un facilitador individual.

Desafíos emergentes

Imágenes "desnudificadas" (Nudify-ing) – El software cada vez más sofisticado para "desnudificar" imágenes (transformar una imagen no explícita en una imagen explícita) se está volviendo libremente disponible en internet. Dicha tecnología puede generar imágenes explícitas de niños, a veces muy comprometedoras. Estas imágenes podrían usarse para extorsionar a personas vulnerables sin haberlas

engañado para que proporcionasen imágenes explícitas reales.

Inteligencia Artificial Generativa – La IA Generativa tiene el potencial de ser utilizada para automatizar la comisión de ESIF, a través de su uso para desarrollar guiones de extorsión, encontrar víctimas potenciales y mantener conversaciones iniciales con ellas, potencialmente en muchos idiomas diferentes. A finales de 2024, el NCMEC ya había recibido más de 7.000 informes de explotación infantil generada por IA generativa.

Potencial aumento de la participación de grupos del crimen organizado y la comercialización de la ESIN – Actualmente, el nivel típicamente bajo de ingresos relacionados con el ASVD y la ESIF limita la participación de grupos significativos del crimen organizado. Sin embargo, existe cierta evidencia de estructuras comerciales criminales en países en desarrollo que explotan cada vez más las oportunidades comerciales que presenta el ASVD remunerado.

Recomendaciones para que las Jurisdicciones Mejoren su Capacidad de Detectar, Interrumpir, Investigar y Perseguir Judicialmente la Explotación Sexual Infantil en Línea

● Considerar como un delito centrado en la víctima

El alto nivel de daño duradero causado a las víctimas significa que, ante todo, todas las partes interesadas deben mantener un enfoque centrado en la víctima para responder a estos delitos. Categorizar y responder a la ESIN puramente como ciberdelincuencia, en lugar de como un delito habilitado cibernéticamente centrado en la víctima, conlleva el peligro de perder de vista los delitos sexuales violentos o la devastadora explotación sexual que subyace a la actividad de ESIN.

● Adoptar y difundir Indicadores Financieros de la ESIN a las partes interesadas relevantes

Las jurisdicciones deben considerar adoptar los indicadores de transacciones financieras vinculadas al ASVD y a la ESIF proporcionados en este informe en su respuesta nacional a la ESIN. También deben difundir los indicadores actualizados a las autoridades y entidades reguladas relevantes y tomar medidas para fomentar su integración en los procesos de monitoreo de transacciones.

● Profundizar la conciencia sobre los delitos de ESIN y su investigación

Al comienzo de este proyecto, muchos participantes no estaban familiarizados con estos tipos delictivos, y esta falta de conciencia dificultó la obtención de información del GAFI y de la Red Global del GAFI. Para familiarizar a las autoridades competentes implicadas, las jurisdicciones deben considerar la sensibilización de todas las autoridades competentes y la capacitación del personal relevante sobre los indicadores financieros y la investigación de las transacciones de ESIN.

● Identificar y evaluar el riesgo de flujos financieros y LA asociados a la ESIN

Dado el menor nivel de ingresos generados por el ASVD y la ESIF en relación con otros, las jurisdicciones pueden no estar inclinadas a incluirlos en sus procesos de evaluación de riesgos. Sin embargo, el nivel de daño asociado y la motivación financiera detrás de estos delitos deben alentar a las jurisdicciones a considerarlos bajo sus evaluaciones de riesgo nacional.

● Cooperación público-privada

Según algunos de los ejemplos de vanguardia proporcionados en este informe, las jurisdicciones deben desarrollar proactivamente relaciones con el sector privado y los socios de la sociedad civil que trabajan para interrumpir estos delitos. Todas las partes interesadas deben tener una comprensión común de las amenazas que enfrenta la jurisdicción y conocer las vías más eficientes disponibles para denunciar sospechas o instancias de estas amenazas.

● Mejorar la cooperación y el intercambio de información interno

Las jurisdicciones también deben desarrollar mecanismos para facilitar la cooperación y el intercambio de información entre sus autoridades relevantes para permitir un enfoque holístico que optimice el valor de la inteligencia financiera e investigación. Las jurisdicciones también deben considerar el valor de un recurso específico y especializado en ASVD, ESIF o ESIN en general, que trabaje para garantizar una respuesta estandarizada y comprehensiva.

● Desarrollar proactivamente alianzas internacionales

Según este informe, en muchos casos estos delitos tienen elementos internacionales, frecuentemente con países socios recurrentes. Los individuos y las autoridades pueden crear proactivamente relaciones con contrapartes y/o aprovechar los foros y grupos de trabajo multinacionales existentes, o desarrollar nuevos.

● Poderes de suspensión temporal

Las Normas del GAFI requieren que los países tengan el poder de suspender transacciones financieras. Estos poderes deben utilizarse en casos de transacciones financieras relacionadas con el lavado de los ingresos de la ESIN.

● Persecución de medidas de recuperación de activos

El GAFI alienta a los países a utilizar más frecuentemente las leyes de recuperación de activos como medio para combatir la ESIN. Los países podrían considerar usar sus redes interinstitucionales regionales de recuperación de activos o el Aviso Plata de INTERPOL para rastrear y recuperar activos criminales vinculados a la ESIN.

● Adoptar un enfoque multifacético

De este informe y de las presentaciones recibidas de los miembros de la Red Global del GAFI, es claro que para detectar, interrumpir, investigar y perseguir judicialmente la ESIN con éxito, es esencial adoptar una respuesta multifacética y global por parte de las partes interesadas. Esta respuesta debe abarcar la acción policial local e internacional, leyes contemporáneas y específicas sobre ESIN en todas las jurisdicciones, cooperación público-pública y público-privada, incorporación de la ESIN en las evaluaciones de riesgo nacional, e iniciativas específicas de prevención y educación.

Oportunidades

Disrupción del delito de contacto: Existe una tipología conocida de consumidores de ASVD que progresan desde el consumo en línea del abuso sexual transmitido en directo hacia el viaje a destinos para cometer abuso de contacto en persona (turismo sexual infantil). Detectar el consumo de ASVD e identificar y tomar las acciones apropiadas contra los consumidores es una oportunidad para interrumpir o prevenir esta escalada de comportamiento. Como se señala en este informe, la inteligencia financiera vinculada al ASVD puede ayudar a construir perfiles más precisos de posibles infractores, que pueden compartirse con las agencias nacionales de seguridad fronteriza.

Disrupción de otros delitos: Como se vio en la Operación Cazador (Operation Huntsman), las mulas bancarias involucradas en el lavado de pagos de rescate de la ESIF también fueron identificadas como facilitadoras de una amplia gama de delitos de fraude de alto valor económico. La acción de la Operación contra estas mulas por su participación en la ESIF comprometió su utilidad para permitir los delitos de mayor valor de los perpetradores. Esto, junto con la tipología conocida de perpetradores de la ESIF que también realizan otros fraudes y estafas, ofrece la oportunidad, a través de la identificación de perpetradores o actores asociados de la ESIF, de interrumpir la comisión de otros delitos.

Conclusión

La ESIN es un delito atroz que se aprovecha de las personas más vulnerables de la sociedad: los niños. No existen definiciones claras y coherentes que describan los tipos de delitos que la ESIN abarca. En consecuencia, no hay estimaciones aceptadas de los ingresos que estos delitos generan. Lo que sí es claro es que este tipo delictivo es masivo en su alcance y la trayectoria de sus instancias está aumentando a un ritmo alarmante.

Hay muchas incógnitas en la investigación sobre este tipo delictivo, pero lo que no está en cuestión es el costo significativo para las víctimas y sus familias. La ESIN tiene consecuencias devastadoras sobre las víctimas, consecuencias que son graves e impactan a las víctimas a lo largo de toda su vida. Algunas situaciones que involucran ESIN han incluso resultado en suicidios. El riesgo de LA no es simplemente una expresión del dinero que genera un delito. El riesgo de LA incluye la consideración de las consecuencias del delito, incluidas las consecuencias para la víctima y las sociedades que incurren en costos sociales adicionales. En el caso de la ESIN, estas consecuencias son enormes y superan cualquier consideración del valor de los ingresos que el tipo delictivo genera.

Este impacto significa que es imperativo que todas las jurisdicciones trabajen juntas a nivel global para detectar, interrumpir e investigar la comisión de la ESIN. La inteligencia financiera y el despliegue de estrategias de investigación centradas en la víctima tienen un papel fundamental que desempeñar en esto, ofreciendo oportunidades para la detección y disrupción de la ESIN no posibles por otros medios y de una manera que puede reducir la dependencia del testimonio de la víctima. La utilización de la inteligencia financiera ha llevado directamente, como lo demuestran las contribuciones de las delegaciones, a la identificación y protección de víctimas del ASVD y a intervenciones de apoyo en tiempo real para víctimas de la ESIF, subrayando el poderoso impacto que puede tener el uso efectivo de la inteligencia financiera.

Anexo A:

Identificación de Transacciones Financieras Vinculadas a la Explotación Sexual Infantil en Línea

ANEXO A

Debe tenerse en cuenta que los indicadores que se detallan a continuación vinculados a la detección de la explotación sexual infantil en línea (ESIN) están en constante evolución, y las jurisdicciones deben continuar informando y fortaleciendo estos indicadores a través de la colaboración continua entre sus UIF, entidades obligadas, fuerzas del orden y otras partes interesadas.

Identificación de Transacciones Financieras Vinculadas al Abuso Sexual de Niños por Videotransmisión en Directo

Los consumidores que pagan por ver el abuso sexual de niños por videotransmisión en directo (ASVD) utilizan típicamente servicios de transferencia de moneda o valor (STMV) populares, predominantemente sistemas de pago en línea entre pares (P2P) como PayPal. Si bien menos común, algunos consumidores realizan depósitos bancarios directos o transfieren activos virtuales (AV) a través de proveedores de servicios de activos virtuales (PSAV). Las entidades obligadas que brindan o facilitan estos servicios financieros pueden detectar transacciones que puedan estar vinculadas a casos de ASVD utilizando una combinación de los indicadores que se detallan a continuación:

Indicadores Generales de Transacciones Relacionadas con el Abuso Sexual de Niños por Videotransmisión en Directo

- Transacciones desde países desarrollados hacia jurisdicciones de alto riesgo para la explotación sexual infantil.
- Diferencias de edad significativas entre remitentes y receptores.
- Transacciones de montos bajos (entre 10 y 200 EUR por instancia), en denominaciones exactas en moneda del país de origen o destino, o en el equivalente en activos virtuales de montos fiat exactos.
- Pagos realizados a receptores en otra jurisdicción con quienes el remitente no tiene una conexión legítima aparente.
- Transacciones realizadas a intervalos irregulares pero de forma repetida a cuentas el mismo día o en días sucesivos.
- Transacciones realizadas tarde en la noche o muy temprano en la mañana (señalando que el consumidor puede encontrarse en un huso horario diferente).
- El propósito de la transacción hace referencia a redes sociales o nombres de usuario, términos sexuales o pornográficos, o la fecha/hora en que se transmitió el material.

- Historial financiero extendido caracterizado por pagos durante un período prolongado, señalando que se ha formado una relación a largo plazo entre el consumidor y el facilitador.
- La transacción puede describirse como para gastos médicos o de subsistencia o referirse a relaciones entre el remitente y el receptor (p. ej., "apoyo familiar", "cuotas escolares", "asistencia", "apoyo", "facturas médicas", "alojamiento", "educación", "asistencia financiera", "regalo", "compra de ropa", "compra de juguetes", "uniforme", "amigo", "novio", "novia", "patrocinador").
- Compras en proveedores que ofrecen herramientas de cifrado en línea, servicios de VPN, software para borrar rastros en línea, u otras herramientas o servicios de privacidad y anonimato en línea.
- Cuentas o clientes con un alto volumen de transacciones hacia Facebook, Microsoft, Google Play, OnlyFans, TikTok, Instagram u otros sitios de redes sociales.
- Transacción vinculada a una persona incluida en un registro público de delincuentes sexuales.

Transacciones Realizadas por Consumidores

- Transacciones realizadas a cuentas ubicadas o accedidas en jurisdicciones de alto riesgo para el ASVD (p. ej., cuentas accedidas mediante retiros de ATM, o inicio de sesión en la cuenta a través de una dirección IP en una jurisdicción de preocupación).
- Compras en plataformas de citas o plataformas que ofrecen contenido de entretenimiento para adultos.
- Compras en plataformas de webcam/videotransmisión, incluidas las que ofrecen entretenimiento para adultos.
- Compras en plataformas de juegos en línea o tiendas de videojuegos.
- Compras de software de captura de video.
- Fondos enviados o recibidos de una persona acusada por delitos relacionados con la explotación sexual infantil (incluyendo cualquier delito de atracción) y/o fondos hacia o desde una contraparte común compartida con dicha persona.
- Transacciones vinculadas a una persona que es objeto de medios negativos relacionados con delitos de explotación sexual infantil.

Transacciones Realizadas por Facilitadores/Abusadores

- Las remesas de dinero generalmente se retiran de inmediato.
- Los receptores están bajo investigación policial por sospecha de ser parte de la facilitación de la explotación sexual infantil en línea.
- Pagos por funciones o servicios premium en plataformas de redes sociales.
- Compras de software de captura de video para uso en sitios web o redes sociales.
- Transacciones en plataformas de juegos en línea o tiendas de videojuegos.
- Adquisición de spyware o aplicaciones de vigilancia.
- Múltiples depósitos de montos similares rastreados a fuentes extranjeras, particularmente de países consumidores de alto riesgo de ASVD, incluidos depósitos de estas fuentes extranjeras al mismo tiempo o en un tiempo similar.
- Pagos a proveedores/plataformas de alojamiento de archivos en línea.
- Compras en sitios web de transmisión de contenido creativo (p. ej., membresías o suscripciones a estos sitios o pago de fondos a otros streamers en estos sitios).

Si bien uno de los indicadores anteriores aislado puede no necesariamente indicar pagos relacionados con posibles casos de ASVD, usar una combinación de indicadores y otros factores relevantes respecto de las transacciones y los clientes puede ayudar a las entidades obligadas a observar patrones que puedan señalar actividad sospechosa.

Identificación de la Extorsión Sexual e Infantil con Fines Financieros a través de Transacciones Financieras

La mayoría de las víctimas reportan haber pagado rescates a facilitadores a través de STMV (predominantemente sistemas de pago P2P en línea como PayPal), transferencias bancarias, AV a través de PSAV o tarjetas de regalo. Las entidades obligadas que brindan estos servicios tienen la capacidad de detectar transacciones que puedan ser indicativas de extorsión sexual e infantil con fines financieros (ESIF) utilizando una combinación de los indicadores que se enumeran a continuación:

Indicadores Generales de Transacciones Relacionadas con la Extorsión Sexual e Infantil con Fines Financieros

- Transacciones realizadas entre dos personas sin relación aparente (sin apellido común, sin propósito comercial claro).
- Transacciones generalmente inferiores a 500 EUR, pero a veces de hasta 1.500 EUR en denominaciones exactas.
- La transacción inicial entre remitente (víctima) y receptor (perpetrador) generalmente inferior a 250 EUR.
- Múltiples transacciones de un remitente a un receptor en un corto período de tiempo que luego cesan completamente.
- Transacciones realizadas a un país de operación común de perpetradores de ESIF (p. ej., Côte d'Ivoire, Nigeria, Filipinas). Las entidades obligadas deben tener en cuenta la tendencia cambiante de los países donde esto predominantemente ocurre con el tiempo.
- El propósito de la transacción hace referencia a redes sociales o nombres de usuario, términos sexuales o pornográficos, lenguaje amenazante/suplicante o la fecha/hora en que se recibió el material.
- El receptor de la transacción no es local al remitente.
- Los detalles del pago parecen una donación benéfica.
- Transacción vinculada a una persona incluida en un registro público de delincuentes sexuales.

Transacciones Realizadas por Víctimas

- Transacciones realizadas por un adolescente o joven adulto varón y, en menor medida, adolescente o joven adulta mujer.
- Transacciones originadas en países predominantemente de habla inglesa, si son internacionales. Las entidades obligadas deben tener en cuenta que esto se convertirá en un marcador menos relevante con el tiempo a medida que los facilitadores se vuelvan más sofisticados.
- Recepción de denuncias de personas sobre vínculos de transacciones con extorsión sexual.
- Pagos que ocurren típicamente entre las 19 hs. y las 7 hs. (generalmente mientras la extorsión sexual está ocurriendo en tiempo real).

- El remitente (víctima) no ingresa el nombre del beneficiario (es decir, solo ingresa una etiqueta general para el destinatario) o ingresa un nombre de beneficiario que no coincide con el titular real de la cuenta.
- Reducción de fondos en las cuentas del remitente en pocas horas (generalmente menos de 24 horas).
- Compra no característica de tarjetas de regalo digitales o créditos de juegos.
- Usos no característicos de cuentas de plataformas P2P del individuo.
- Compra no característica de activos virtuales.
- Cuando el personal bancario le hace preguntas, el remitente es evasivo u ofrece una explicación implausible de la actividad.
- Cliente comprando múltiples tarjetas de regalo (p. ej., Amazon, PlayStation u otros proveedores de juegos).

Transacciones Realizadas por Perpetradores

- Una cuenta que recibe múltiples transacciones aparentemente no vinculadas entre sí.
- La cuenta receptora tiene múltiples motivos no relacionados identificados para las transacciones recibidas.
- Los montos recibidos son retirados rápidamente de la cuenta.
- Pagos a servicios en línea que ofrecen privacidad y/o anonimato (p. ej., cifrado, VPN, números de teléfono virtuales).
- Pagos asociados a múltiples tarjetas de crédito prepagadas o tarjetas de regalo.
- Recepción de fondos de múltiples servicios de comercialización de alojamiento de archivos en línea (p. ej., modelos de pago por descarga) en diferentes jurisdicciones.
- Compra de bienes (vehículos, bienes raíces, electrodomésticos) en un corto período de tiempo, sin justificación para los medios utilizados.
- Personas con un estilo de vida y consumo inconsistente con los ingresos de su actividad laboral.

Es importante señalar que cualquiera de los indicadores enumerados anteriormente es insuficiente por sí solo para generar sospecha de un posible intento de extorsión sexual con motivación financiera, sino que las entidades obligadas deben considerar todos los factores que rodean una transacción y si la transacción cumple con varios de los indicadores descritos anteriormente.

Exención de responsabilidad: Este documento y/o cualquier mapa incluido en él se presentan sin perjuicio del estatus o la soberanía sobre cualquier territorio, de la delimitación de fronteras y límites internacionales y del nombre de cualquier territorio, ciudad o área.

Grupo de Acción Financiera Internacional (GAFI) | www.fatf-gafi.org

Nota del Traductor:

Decisiones Terminológicas

NOTA DEL TRADUCTOR – DECISIONES TERMINOLÓGICAS

La presente traducción tiene por objeto trasladar fielmente al español el contenido del informe original en inglés. A continuación se explicitan las principales decisiones adoptadas respecto de siglas, denominaciones y nombres propios. Las justificaciones se limitan estrictamente a criterios de traducción; no se agrega información normativa ni de contexto externas al documento original.

1. Siglas y denominaciones institucionales

Las siglas en inglés del documento original fueron traducidas al español. Se adoptó en todos los casos la traducción literal del nombre completo y se construyó la sigla en español correspondiente. Las siglas ESIN, ASVD y ESIF no son siglas oficiales preexistentes: fueron construidas exclusivamente para mantener coherencia interna a lo largo de esta traducción.

Financial Action Task Force (FATF)	Grupo de Acción Financiera Internacional	GAFI	El propio organismo utiliza esta denominación y sigla en sus documentos oficiales en español.
Online Child Sexual Exploitation (OCSE)	Explotación Sexual Infantil en Línea	ESIN	Traducción literal del nombre completo. Sigla construida para esta traducción; no es una sigla oficial preexistente.
Live-streamed Sexual Abuse of Children (LSAC)	Abuso Sexual de Niños por Videotransmisión en Directo	ASVD	Traducción literal del nombre completo. Sigla construida para esta traducción; no es una sigla oficial preexistente.
Financial Sexual Extortion of Children (FSEC)	Extorsión Sexual e Infantil con Fines Financieros	ESIF	Traducción que preserva los tres elementos del término original: dimensión sexual, víctima infantil y móvil financiero. Sigla construida para esta traducción; no es una sigla oficial preexistente.
Child Sexual Abuse Material (CSAM)	Material de Abuso Sexual Infantil	MASI	Traducción literal del nombre completo tal como lo define el propio documento original en su sección de Definiciones.
Money or Value Transfer Services (MVTs)	Servicios de Transferencia de Moneda o Valor	STMV	Traducción literal del término tal como figura en el Glosario del GAFI, según se define en el propio documento.

Virtual Asset Service Provider (VASP)	Proveedor de Servicios de Activos Virtuales	PSAV	Traducción literal del término tal como figura en el Glosario del GAFI, según se define en el propio documento.
Financial Intelligence Unit (FIU)	Unidad de Inteligencia Financiera	UIF	Traducción literal del nombre completo.
Virtual Assets (VA)	Activos Virtuales	AV	Traducción literal del término tal como figura en el Glosario del GAFI, según se define en el propio documento.
Peer-to-Peer (P2P)	Entre Pares	P2P	Se conserva la sigla P2P en tanto designador técnico de uso universal. El nombre completo se traduce en primera mención.
Virtual Private Network (VPN)	Red Privada Virtual	VPN	Se conserva la sigla VPN en tanto designador técnico de uso universal. El nombre completo se traduce en primera mención.

2. Nombres de operaciones, proyectos y programas

Se adoptó como criterio general la traducción semántica al español de todos los nombres de operaciones y programas, conforme a la instrucción recibida. En los casos en que el nombre original es un designador alfanumérico, un nombre propio sin contenido semántico traducible, o el nombre institucional propio de un organismo externo, se conservó en inglés. En todos los casos se consigna el nombre original entre paréntesis en la primera mención dentro del documento.

Operation Huntsman	Operación Cazador	Traducción semántica: 'huntsman' significa cazador/montero en inglés.
Project SHADOW	Proyecto Sombra	Traducción semántica directa.
Operation Cyber Guardian	Operación Guardián Cibernético	Traducción semántica directa.
Lantern Coalition	Coalición Linterna	Traducción semántica directa.
1930 Take Down System	Sistema de Eliminación 1930	El número 1930 es la línea de ayuda mencionada en el documento y se conserva. 'Take Down' se traduce como 'Eliminación' en tanto el documento lo describe como un sistema para eliminar contenido dañino en línea.

Operation O (NCA, UK)	Operación O	Se conserva: es un designador alfanumérico sin contenido semántico traducible.
Operation Narsil (INTERPOL)	Operación Narsil	Se conserva: es un nombre de código propio de INTERPOL sin contenido semántico traducible al español.
CyberTipline (NCMEC)	CyberTipline (conservado)	Se conserva: es el nombre propio de un sistema institucional específico del NCMEC. Su función se describe en el texto.
ThinkUKnow Australia	ThinkUKnow (conservado) Australia	Se conserva: es el nombre propio de un programa institucional específico mencionado en el documento.
Hydrant Program (UK)	Programa (conservado) Hydrant	Se conserva: es el nombre de código propio de un programa institucional del Reino Unido mencionado en el documento.

3. Términos con decisión de traducción no evidente

Los términos a continuación presentaban más de una opción de traducción posible. Se explica el criterio adoptado en cada caso.

Original: *Catfishing* **Traducción:** Ciberengaño (catfishing)

El documento original define este término en su sección de Definiciones como el proceso de atraer a alguien mediante una persona ficticia en línea. Se optó por 'ciberengaño' como traducción descriptiva, conservando el original entre paréntesis por ser un término técnico reconocible en el ámbito de los delitos informáticos.

Original: *Capping* **Traducción:** Captura (capping)

El documento original define este término en su sección de Definiciones como la grabación del material de abuso sexual infantil transmitido en directo. Se optó por 'captura' como traducción funcional del concepto, conservando el original entre paréntesis.

Original: *Ransom* **Traducción:** Rescate

El documento usa 'ransom' para referirse al monto exigido a la víctima bajo amenaza. Se optó por 'rescate' por ser la traducción más directa y la que mejor refleja el contexto descrito en el documento.

Original: *Money mule* **Traducción:** Mula de dinero

El documento usa este término en el contexto de tipologías de lavado de activos. Se adoptó la traducción literal 'mula de dinero', que es la misma denominación utilizada en las tipologías del GAFI citadas en el propio documento.

Original:	<i>Grooming</i>	Traducción:	Grooming (conservado)
------------------	-----------------	--------------------	-----------------------

El documento usa este término para referirse a técnicas de manipulación de largo plazo previas al abuso. Se conservó en inglés porque el documento lo usa como término técnico diferenciado de las técnicas de la ESIF, y porque su conservación permite identificarlo con precisión en el contexto del informe.

Original:	<i>Suspicious Activity Report / Suspicious Transaction Report (SAR/STR)</i>	Traducción:	Reporte de Operaciones Sospechosas (ROS)
------------------	---	--------------------	--

El documento refiere a estos reportes como instrumentos del sistema antilavado. Se adoptó la denominación 'Reporte de Operaciones Sospechosas' por ser la traducción que el propio GAFI utiliza en sus documentos en español.

Original:	<i>Proceeds of crime / asset recovery</i>	Traducción:	Producto del delito / recuperación de activos
------------------	---	--------------------	---

Traducciones literales adoptadas por el GAFI en sus documentos oficiales en español, tal como se desprende del Glosario del GAFI citado en el propio informe.

Original:	<i>Designated categories of offences</i>	Traducción:	Categorías designadas de delitos
------------------	--	--------------------	----------------------------------

Término del Glosario del GAFI. Se traduce literalmente conforme a la versión en español del mismo Glosario al que el documento hace referencia explícita.

Nota sobre el alcance de esta traducción: La presente traducción reproduce el contenido textual del informe original. El documento original en inglés contiene además elementos visuales (fotografías a página completa, gráficos y diagramas) que no son texto y por lo tanto no han sido incorporados. El texto en inglés del informe original prevalece en caso de discrepancia con esta traducción.