APORTE DEL PERITO EN INFORMÁTICA FORENSE EN LA LUCHA CONTRA EL CIBERACOSO Y EL *GROOMING*

Diálogo Forense
Núm. 9 , Vol. 5, 2024
ISSN: 2789-8458

Mayra Alejandra Martínez Ralón
Informática Forense del Instituto Nacional de Ciencias Forenses de Guatemala -INACIF-

mmartinez@inacif.gob.gt

Recibido: 05/03/2024
Aceptado: 12/06/2024

Palabras clave: ciberacoso, *grooming*, brecha digital, supervisión parental, redes sociales.
Keywords: cyberbullying, grooming, gap, parental supervision, social networks.

RESUMEN

El ciberacoso, en particular el *grooming* en línea, plantea una grave amenaza para la seguridad de los menores de edad en la era digital. Este estudio presenta dos casos de ciberacoso en Guatemala, investigados mediante análisis forense de comunicaciones en aplicaciones como WhatsApp y Facebook Messenger. Los resultados revelan un patrón común: adultos que se contactan con menores de edad para ganar su confianza y eventualmente involucrarlos en actividades sexuales. Se destaca la necesidad de una supervisión activa de los padres y el uso de herramientas de control parental para proteger a los menores en línea. Además, se propone una mayor educación y concientización sobre los riesgos del ciberacoso.

ABSTRACT

Cyberbullying, particularly online grooming, poses a serious threat to the safety of minors in the digital age. This study presents two cases of cyberbullying in Guatemala, investigated through forensic analysis of communications on applications such as WhatsApp and Facebook Messenger. The results reveal a common pattern: adults contacting minors to gain their trust and eventually involve them in sexual activities. The need for active parental supervision and the use of parental control tools to protect minors online is emphasized. Furthermore, increased education and awareness about the risks of ciberbullying.

INTRODUCCIÓN

El *grooming* en línea, como forma de ciberacoso, representa un problema grave que se produce mediante la utilización de la tecnología con la finalidad de intimidar, acosar o amenazar a menores de edad. Es un acto delictivo que implica a un adulto que se pone en contacto con un niño, niña o adolescente con el objetivo de ganarse gradualmente su confianza para involucrarlos en actividades sexuales. Estas interacciones pueden variar en su grado de peligro, desde conversaciones con temática sexual hasta la obtención de material íntimo, e incluso llegar a encuentros físicos de naturaleza sexual (Save the Children, 2019).

La Real Academia Española (s.f., definición 1) define el *grooming* como "acoso sexual a menores de edad a través de medios informáticos o telemáticos, fundamentalmente mediante chats y redes sociales". Los menores de edad se enfrentan a ciberacosadores a través de las redes sociales y plataformas móviles o *web*, donde la interacción virtual en muchos casos se caracteriza por la ausencia de controles parentales o la supervisión de un adulto. Esta situación aumenta su vulnerabilidad y es cada vez más común y peligrosa.

En 2022, el Congreso de la República de Guatemala aprobó el Decreto 11-2022, que reforma el Código Penal, en relación con delitos cometidos contra la niñez y adolescencia a través de medios tecnológicos. Esta reforma establece penas de 6 a 12 años de prisión para aquellas personas que, valiéndose de estos medios, contacten a niños o adolescentes con fines sexuales, según lo indicado en el artículo 190 Bis:

> **Artículo 190 Bis.** Seducción de niños, niñas o adolescentes por el uso de las tecnologías de información. Quien, a través de todo tipo o clase de medios tecnológicos, valiéndose o no del anonimato, contacte a cualquier niño, niña o adolescente con el propósito de:
>
> A. Solicitar o recibir material con contenido sexual o pornográfico, propio o de terceras personas, ya sea que incluya o no medios audiovisuales;
> B. Tener o facilitar con tercera persona relaciones sexuales;
> C. Facilitar la comisión de cualquier otro delito contra la libertad o indemnidad sexual del niño, niña o adolescente contactado...(p.1).

La vulnerabilidad de los menores de edad se incrementa cuando utilizan aplicaciones de mensajería, redes sociales y juegos en línea sin la supervisión de un adulto (Cahanme López y García Ordinola, 2021). La falta de controles parentales los expone a ser contactados por personas con intenciones maliciosas. Por consiguiente, la gestión del contenido y la protección de la privacidad por medio de la función de "control parental" son cruciales para prevenir y restringir estas interacciones, mediante el bloqueo de aplicaciones, funciones y contenido al que los menores pueden acceder (ver figura 1).

Figura 1. *Funcionamiento de las aplicaciones de control parental en dispositivos conectados a internet. Las aplicaciones de control parental operan en dispositivos conectados a internet, permitiendo a los padres y cuidadores monitorear y gestionar el uso que los menores hacen de diversas plataformas y aplicaciones.*

Asimismo, esta función permite monitorear y delimitar los tiempos de navegación en dispositivos como teléfonos móviles, tabletas y ordenadores (Larreátegui y Sánchez, 2016). Se pueden encontrar diversas aplicaciones de control parental como, Family Link de Google y Control Parental de Apple. Además, la mayoría de aplicaciones, plataformas de *streaming* y juegos en línea ya ofrecen opciones para activar el control parental y así controlar el uso de estas.

No obstante, la brecha digital, que se refiere a la disparidad en el acceso y uso de tecnologías de la información y comunicación entre diferentes grupos, afecta la capacidad de supervisión que los padres y cuidadores pueden ejercer sobre el uso de internet por parte de los menores. Reducir esta brecha es esencial para garantizar una supervisión efectiva y proteger a los menores del *grooming* en línea.

PRESENTACIÓN DE LOS CASOS

Los nombres de las personas involucradas, edades y las fechas de los eventos que se describirán a continuación, fueron modificados para proteger la confidencialidad de los casos.

CASO 1

"Eva" es una adolescente de 13 años de edad que vive en una aldea de Jalapa junto a su madre y su hermano menor (Tony). Eva, durante el último trimestre del 2022 mantuvo comunicación mediante la aplicación de mensajería WhatsApp con el señor José Manuel, "don José" o "tío chepe", quien tiene 55 años de edad. José la conoce desde niña porque es su tío y son vecinos. Eva, Tony y los hijos de don José juegan juntos. La mamá de Eva confiaba plenamente en ella, sin embargo, no la dejaba salir sin la compañía de Tony.

Las conversaciones se inician en la segunda quincena de noviembre de 2022, en las cuales se evidencia que la niña visitaba el hogar de su tío Chepe, pues allí vivían sus primitos. Ella y Tony solían verse con los niños por las tardes para jugar, situación que aprovechó el abusador para contactarla de forma maliciosa y poder agregarla a su agenda telefónica y a la aplicación WhatsApp. Posteriormente, buscó saludarla por el chat, comenzó a ofrecerle regalos y a acosarla constantemente, puesto que la niña se negaba a visitarlo a solas, como él solía pedirle. Don José afirma estar enamorado de ella y sentirse en desventaja, pues la edad de él jamás le permitiría mantener una relación con la niña. Este se victimiza y le hace varias ofertas de índole económico con la intención de poderla atraer.

Sin embargo, a medida que pasan los días, y dada la negativa de la niña de "darle un beso", don José intensifica el tono de las conversaciones, recurriendo a frases figurativas con intenciones sexuales. Incluso llega al punto de amenazar con revelar a la madre de Eva la comunicación que mantenían, inventando una historia para presionar a la sobrina a continuar permitiendo el abuso y poder tener algún tipo de contacto físico con Eva. Finalmente, Eva decidió contarle a su mamá lo sucedido y pusieron la denuncia en el Ministerio Público contra el acosador.

CASO 2

"Arielle Vásquez" tiene 14 años de edad, vive en la ciudad capital de Guatemala junto a sus padres y hermanos. Ella mantuvo comunicación durante dos semanas por la aplicación Facebook Messenger con "Emanuel Orantes", de 23 años, quien le envió invitación a la red social. Ella lo aceptó, ya que es hermano de su amiga "Beberly" y conocido de la familia. Además, él trabaja por el sector que conduce a la escuela a la que ella asiste y se han saludado a la distancia en un par de ocasiones.

La primera interacción tuvo lugar el 12 de agosto de 2022, por el chat de Messenger. Emanuel la saludó y fue muy educado con Arielle, con la aparente intención de ganarse su confianza y conocer sus movimientos. Tres días después, el agresor incitaba a la menor para enviarle fotografías, y le realizaba solicitudes para reunirse solo los dos, con la excusa de que quería entregarle un regalo. A partir del quinto día, él comenzó a decirle que estaba enamorado de ella y le prometió que iban a vivir juntos para siempre.

De acuerdo con los reportes de llamadas, contenido de las conversaciones y al historial de geolocalización almacenados en Google Maps, se pudo determinar que el

primer intento de abuso físico fue el 21 de agosto, cuando Emanuel ingresó en la vivienda de la menor. No obstante, ella se asustó y el individuo optó por abandonar el hogar de la niña a los pocos minutos de haber entrado. Luego de esto, continuaron las conversaciones y bajo manipulación consiguió que Arielle aceptara que la visitara en su dormitorio un sábado por la noche, a escondidas de la familia de la niña. El abuso sexual físico hacia la menor se perpetró el 27 del mismo mes, según el material extraído del dispositivo.

Extractos de la conversación entre ambos documentan dos semanas en las cuales el agresor realiza el primer contacto con la menor por el chat de Facebook Messenger. Luego de varios días de comunicación logra ganarse su confianza, evidenciando cómo de forma gradual va aumentando el tono de la conversación hasta el punto de que el agresor le hace invitaciones a su casa, le pide que use cierto tipo de ropa y busca la manera de verla a solas, visitándola inclusive en su cuarto.

Según lo establecido en la línea de tiempo de este caso, las conversaciones se hacían regularmente por la noche, ya que en el día la joven se encontraba en compañía de su familia o estudiando y el agresor trabajaba. Adicionalmente, se pudo constatar que Emanuel mantenía comunicación con varias mujeres al mismo tiempo. Las conversaciones finalizaron hasta que la mamá de la menor revisó el teléfono y se percató del contenido de dicha conversación.

DISCUSIÓN

La labor del Laboratorio de Informática Forense es crucial para combatir el *grooming*, ya que permite obtener y analizar pruebas digitales esenciales para las investigaciones de este tipo de acoso. Por ejemplo, se pueden generar líneas de tiempo a partir de los registros contenidos en los distintos dispositivos telefónicos proporcionados, analizando comunicaciones y contenido multimedia según lo requerido en las solicitudes de peritaje.

En el primer caso, el laboratorio efectúo la extracción de datos de los dispositivos móviles, incluyendo chats, historial de geolocalización, registros de llamadas, imágenes, videos y audios. La información extraída reveló un patrón de *grooming* a través de diversas frases, desde la selección de la víctima hasta la realización de peticiones de naturaleza sexual (ver figura 3). La representación basada en la conversación extraída del dispositivo móvil ilustra cómo el agresor estableció contacto con la menor, ofreciéndo regalos y acosándola con intenciones sexuales. La figura muestra cómo las interacciones iniciales inofensivas se transformaron en manipulación, culminando en amenazas.

Para llevar a cabo el análisis forense de los dispositivos móviles, se utilizó la herramienta Cellebrite UFED 4PC, una solución avanzada en el campo de la informática forense. Cellebrite UFED 4PC permite realizar tres tipos principales de extracciones de datos, como lo describe Di Lorio (2013):

Extracciones Físicas: Este método posibilita la obtención de una copia completa de todos los datos almacenados en el dispositivo, incluyendo información eliminada y oculta. Requiere permisos especiales y puede ser un proceso complejo y prolongado, pero ofrece una visión exhaustiva de los datos.

Extracciones del Sistema de Archivos: Este enfoque se centra en recuperar datos directamente desde el sistema de archivos del dispositivo, incluyendo la estructura de carpetas y archivos visibles. Aunque no proporciona una copia completa bit a bit del almacenamiento, es menos invasivo y puede ser suficiente para muchas investigaciones.

Extracciones Lógicas: Esta técnica menos invasiva se basa en obtener datos accesibles a través del sistema operativo del dispositivo, como contactos, mensajes y registros de llamadas. Aunque no permite recuperar información eliminada, es compatible con la mayoría de los dispositivos y es más rápida de ejecutar.

Estos métodos hicieron posible obtener una amplia variedad de datos, incluso en aplicaciones móviles

protegidas, permitiendo obtener una copia descifrada de la información. Posteriormente, la información extraída fue procesada utilizando un programa forense especializado en análisis y decodificación, que también propicia la generación de informes en diferentes formatos. Estos informes facilitan la visualización y comprensión del contenido extraído, lo cual es esencial para la presentación clara y detallada de las pruebas.

En el segundo caso, se recibió un teléfono bloqueado con un PIN de 6 dígitos. Dada la negativa de la menor de proporcionar las credenciales de acceso, se recurrió a un ataque de fuerza bruta, importando diccionarios de contraseñas personalizados en el programa Oxygen Forensic Detective. Este proceso permitió obtener los dígitos necesarios para desbloquear el dispositivo, que tenía el sistema operativo Android. Tras dos semanas de intentos se logró acceder a la información de las bases de datos de la aplicación de chat de Facebook. El análisis de los chats mostró cómo el agresor estableció contacto y en un periodo de casi dos semanas, incrementó gradualmente la intensidad de la conversación, resultando en un abuso físico (ver figura 4).

Ambos casos son paradigmáticos de *grooming*. Los resultados de los análisis realizados en el Laboratorio de Informática Forense condujeron a identificar acosadores en línea que establecieron relaciones engañosas con menores de edad con el objetivo de abusar físicamente y obtener material con contenido sexual. Además de facilitar la extracción de contenido y la creación de una línea de tiempo de los eventos, estos análisis permitieron identificar similitudes entre ambos casos al examinar las fases del *grooming*.

Figura 2. *Las principales fases del grooming. El número de fases descritas pueden variar dependiendo del autor; sin embargo, finalmente estas engloban siempre las mismas características.*

A pesar de que varios autores, como Pasca et al. (2022), Winters et al. (2020), y Lanning y Dietz (2014), han descrito diversas fases del *grooming* que varían de tres a ocho pasos (ver figura 2), el análisis de varios casos de acoso hacia menores de edad trabajados en el laboratorio ha evidenciado seis fases comunes:

Selección de la víctima: El agresor inicia el contacto con el menor, agregándolo a una red social o chat de WhatsApp.

Rastreo de su entorno familiar y de confianza: El agresor busca ganarse la confianza del menor, conociendo sus rutinas y detalles personales, ofreciendo regalos para volverse cercano a la víctima.

Aislamiento de la víctima: El agresor intenta mantener la relación en secreto, identificando quién tiene acceso a las cuentas o al teléfono móvil del menor.

Desarrollo de confianza: El agresor busca obtener confesiones personales o íntimas del menor.

Desensibilización al contenido sexual y al contacto físico: El abusador introduce temas sexuales mediante persuasión, buscando familiarizar al menor con actos sexuales.

Realización de peticiones de naturaleza sexual: El agresor manipula al menor para encuentros físicos o para obtener material sexual, utilizando técnicas de chantaje o manipulación.

Una observación relevante en la experiencia, como perito del Laboratorio de Informática Forense, es que en 1 de cada 10 casos de *grooming* analizados no se tenía activado ningún control parental en los dispositivos utilizados por los menores. Esto destaca la importancia de que los padres y tutores implementen medidas de control parental para proteger a los menores de los riesgos en línea.

Las estadísticas sobre el uso de controles parentales indican que un porcentaje significativo de padres no implementa estas medidas adecuadamente. Por ejemplo, según un comunicado del Instituto Federal de Telecomunicaciones de México (2022), aunque el 62.7 % de los padres han implementado algún tipo de

control en sus redes móviles (como control del tiempo de uso), solo el 12.5 % utiliza herramientas específicas como Google Family Link para un control parental más completo. Estos datos reflejan una notable discrepancia entre la conciencia de los riesgos en línea y la utilización efectiva de medidas preventivas. La supervisión parental y el uso de herramientas de control parental son fundamentales para proteger a los menores de peligros como el ciberacoso y el *grooming*. Promover el uso efectivo de estas herramientas y educar a los padres sobre su importancia podría significativamente aumentar la protección de los niños en el entorno

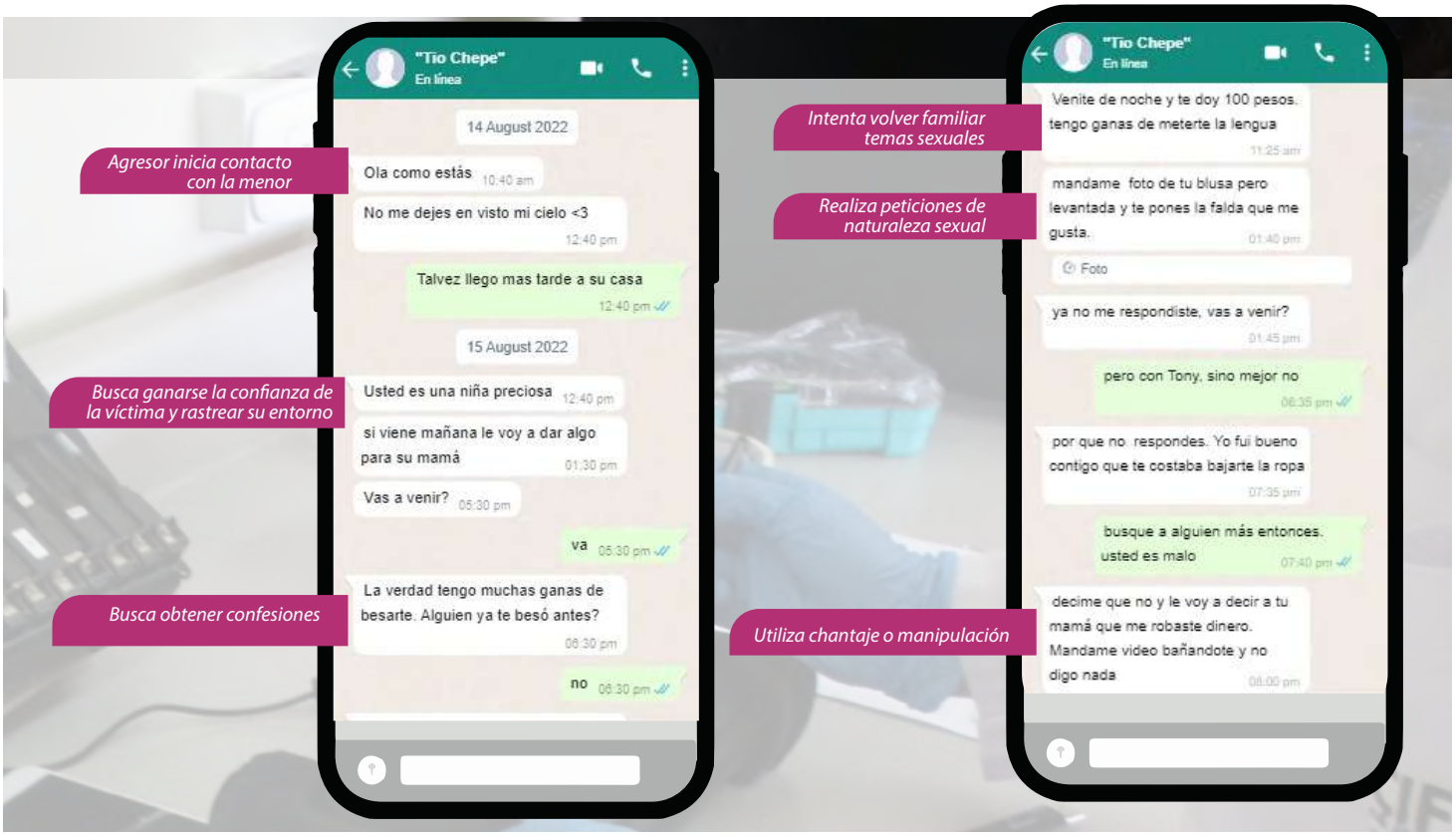

Figura 3. Fases del *grooming* en el caso 1. Se muestra una representación basada en la conversación extraída del dispositivo móvil del caso 1. Las imágenes presentadas no son reales; han sido recreadas utilizando una aplicación para fines ilustrativos. El diálogo exhibido no reproduce textualmente la conversación original, ya que se han realizado modificaciones en las palabras, aunque se ha mantenido el sentido y la esencia de lo discutido.

Figura 4. Ejemplificación del caso 2. La figura muestra una representación basada en una conversación en Facebook Messenger. Las imágenes no son reales; han sido recreadas con una aplicación con fines ilustrativos. El diálogo presentado no es una reproducción textual de la conversación original, ya que las palabras han sido modificadas, pero se ha conservado el sentido y la esencia de lo discutido.

CONCLUSIONES

La protección de los menores de edad en línea es una prioridad crucial para prevenir casos de ciberacoso y *grooming,* como los documentados en este artículo. La supervisión activa de los padres y el uso de herramientas de control parental son fundamentales para protegerlos en el entorno digital. De acuerdo con los datos registrados, se destaca la necesidad de una mayor concienciación y aplicación de estas medidas de protección.

Es esencial establecer límites de tiempo para la navegación en línea, deshabilitar las opciones de chat por defecto en las plataformas de juegos en línea, y revisar constantemente el contenido de las conversaciones activas. Estas prácticas no solo reducen la exposición de los menores a posibles acosadores, sino que también permiten a los padres identificar comportamientos sospechosos de manera temprana. Además, las campañas de concienciación dirigidas tanto a adultos como a menores son vitales para educar a todos sobre los riesgos del ciberacoso y cómo manejar los servicios en línea de manera segura. Estas campañas deben enfatizar la importancia de un ambiente de confianza, donde los menores se sientan seguros para comunicar cualquier situación de peligro o acoso que enfrenten.

Asimismo, la labor del Laboratorio de Informática Forense es crucial en la lucha contra el *grooming*. La capacidad de este laboratorio para extraer y analizar datos de dispositivos móviles es capaz de proporcionar pruebas fundamentales en las investigaciones de acoso en línea. Estas herramientas avanzadas permiten obtener una comprensión detallada de las tácticas utilizadas por los acosadores y ayudan a las autoridades a intervenir de manera efectiva. La tecnología forense, combinada con la supervisión parental y la educación, constituye una estrategia integral para proteger a los menores en la era digital.

BIBLIOGRAFÍA

Chaname Lopez, A., y García Ordinola, S. (2021). El Sexting como conducta de riesgo asociada a la violencia: una revisión sistemática [Tesis de licenciatura, Universidad César Vallejo]. Repositorio Digital Institucional.

Decreto número 11-2022, Código Penal (2022).
https://www.congreso.gob.gt/assets/uploads/info_legislativo/decretos/2d60f-11-2022.pdf

Save the Children. *Grooming, qué es, cómo detectarlo y prevenirlo*. (1 de julio de 2019).
https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

Grupo de Trabajo Interinstitucional en Luxemburgo. (28 de enero de 2016). *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.* Recuperado el 24 de marzo de 2023.
https://www.interpol.int/es/content/download/9373/file/Terminology-guidelines_Spanish_version-electronica_FINAL.pdf

Larreátegui, G. B., y Sánchez, M. S. (2016). Implementación de una aplicación para control parental en dispositivos inteligentes. *Investigatio*, (7), 101-115. https://doi.org/10.31095/investigatio.2016.7.6

Di Iorio, A. (2013). La Informática Forense y el proceso de recuperación de información digital. *Reposiutorio Insittucional Universidad Fasta.*

Instituto Nacional de Ciencias Forenses de Guatemala (INACIF). (2024). *Base de datos del Laboratorio de Informática Forense* (BASE INFOR).

Organismo Judicial. (s. f.). *Código Penal.* CENADOJ. Recuperado 24 de marzo de 2024,de http://ww2.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20compilaciones/Compilacion%20Leyes%20Penales/

Real Academia Española. (s.f.). Cultura. *En Diccionario de la lengua española.* Recuperado en 6 de junio de 2023, de https://dle.rae.es/grooming?m=form

UNICEF. (s/f). *Ciberacoso: Qué es y cómo detenerlo.* www.unicef.org. Recuperado el 2 de 2024, de https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

UNODC. (2024). *Mini guía de seguridad informática.*
https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Safety_Guide_Spanish.pdf

Pasca, P., Signore, F., Tralci, C., Del Gottardo, D., Longo, M., Preite, G., y Ciavolino, E. (2022). Detecting online grooming at its earliest stages: development and validation of the Online Grooming Risk Scale. *Mediterranean Journal of Clinical Psychology*, 10, 1-24.

Winters, G. M., Jeglic, E. L., y Kaylor, L. E. (2020). Validation of the sexual grooming model of child sexual abusers. *Journal of child sexual abuse,* 29(7), 855-875.

Lanning, K. V., y Dietz, P. (2014). Acquaintance molestation and youth-serving organizations. *Journal of Interpersonal Violence*, 29(15), 2815–2838. https://doi.org/10.1177/
0886260514532360