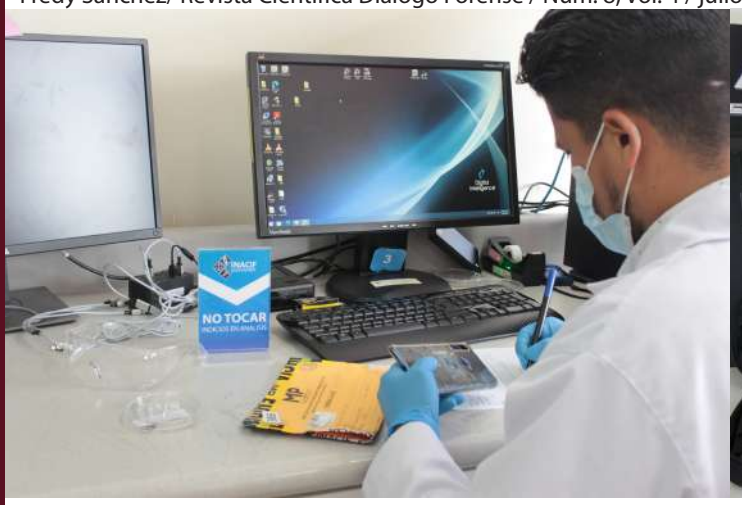
Fredy Sánchez/ Revista Científica Diálogo Forense / Núm. 8, Vol. 4 / julio-diciembre 2023/ pp. 1-9



Diálogo Forense
Núm. 8 , Vol. 4, 2023
ISSN: 2789-8458

CASOS DE ABUSO SEXUAL INFANTIL, DESDE LA PERSPECTIVA DEL PERITO EN INFORMÁTICA FORENSE

Fredy E. Sánchez Gálvez
Jefe del Laboratorio de Informática Forense
Instituto Nacional de Ciencias Forenses de Guatemala -INACIF-

frsanchez122@gmail.com

Recibido: 31/03/2023
Aceptado: 01/08/2023

Palabras clave: abuso sexual infantil, informática forense, perito, ciberdelito, pornografía infantil.
Keywords: child sexual abuse, computer forensics, expert witness, cybercrime, child pornography.

RESUMEN

El perito en informática forense es un profesional especializado en técnicas para tratar la evidencia digital con el fin de garantizar la autenticidad, identidad e integridad, cumpliendo así con los procesos forenses y la legislación en general. Por otro lado, las tecnologías informáticas han evolucionado en respuesta a la necesidad humana de automatizar procesos y hacerlos más ágiles, tal como la comunicación entre personas en distintos puntos geográficos. Aunque estas tecnologías son desarrolladas con fines benignos, desafortunadamente también son aprovechadas por personas que cometen actos ilícitos, como la captura de fotografías íntimas, la creación de documentos falsos, el almacenamiento de archivos ilícitos y la transmisión de datos e información sensible entre dispositivos. El abuso sexual infantil generalmente se cataloga como un ciberdelito, ya que muchos perpetradores recurren a la toma de fotografías para su distribución en redes de contactos, haciendo uso de dispositivos electrónicos e internet. Por lo tanto, es crucial que el perito en informática forense posea no solo aptitudes en técnicas avanzadas, sino el conocimiento de las terminologías adecuadas para definir este delito, la capacidad de distinguir signos o símbolos de identificación entre pedófilos, y comprender el objetivo de las palabras clave y mensajes ocultos de las imágenes de persuasión. Asimismo, debe tener dominio en el uso de herramientas forenses que permitan desarrollar un trabajo adecuado para descubrir evidencia latente.

ABSTRACT

The forensic computer expert is a professional specialized in techniques necessary to treat digital evidence in order to guarantee its authenticity, identity and integrity, thus complying with forensic processes and legislation in general. On the other hand, computer technologies have evolved in response to the human need to automate processes and make them more agile, such as communication between people in different geographical locations. Although these technologies are developed for benign purposes, unfortunately they are also exploited by people who commit illicit acts, such as capturing intimate photos, creating false documents, storing illicit files, and transmitting data and sensitive information between devices. Child sexual abuse is generally classified as a cybercrime, since many perpetrators resort to taking photographs and their subsequent distribution in contact networks, using electronic devices and the Internet. Therefore, it is crucial that the computer forensic expert possesses not only advanced technical skills, but also knowledge of the appropriate terminologies to define this crime, the ability to distinguish identifying signs or symbols between pedophiles, and understand the purpose of the words key and hidden messages of persuasive images. Likewise, you must have mastery in the use of forensic tools that allow you to develop an adequate job and discover latent evidence.

INTRODUCCIÓN

En la actualidad se ha observado un aumento de ciberdelitos, entre los cuales se encuentra la pornografía infantil, que se define como la producción, distribución o posesión de material que muestra abuso sexual infantil. Se ha catalogado como ciberdelito porque las fotografías e imágenes de abuso sexual infantil se suelen transmitir de un dispositivo a otro mediante el uso de internet.

En el contexto de una investigación criminal, el Ministerio Público puede solicitar pruebas técnicas y científicas que le permitan tener una base para su acusación. Los peritos en informática forense deben tener ciertos conocimientos para identificar signos o símbolos que indiquen la necesidad de aplicar técnicas analíticas y científicas avanzadas para la localización de este tipo de archivos.

Estos peritos deben contar con una sólida formación en técnicas forenses, así como con habilidades especializadas en la identificación y análisis de evidencia digital. Además, deben estar al tanto de los avances tecnológicos y las nuevas formas en las que los delincuentes pueden ocultar o compartir material ilícito. De esta manera, los peritos en informática forense juegan un papel crucial en la lucha contra el abuso sexual infantil y otros ciberdelitos, pues recogen pruebas técnicas sólidas que respaldan los procesos judiciales y contribuyen a la protección de los derechos de la niñez.

CONTENIDO

El perito en informática forense

Según la Real Academia Española (s.f.), un perito es un "…profesional o especialista experto en un arte o ciencia cuya opinión técnica es necesaria para el cumplimiento de diversas obligaciones impuestas por el derecho." El Código Procesal Penal Guatemalteco menciona en el Artículo 226: "…los peritos deberán ser titulados en la materia al que pertenezca el punto sobre el que han de pronunciarse, siempre que la profesión, arte o técnica estén reglamentados."

Estas dos definiciones expresan claramente que un perito debe ser alguien con idoneidad, para brindar al juez la prueba científica sobre alguna materia en específico, que le permita tomar decisiones claras para una sentencia. Desde el punto de vista personal y en el ámbito de la informática forense, para alcanzar la idoneidad y calidad que se requiere, son necesarias algunas características además de los conocimientos académicos avanzados sobre informática:

a. Conocimiento y experiencia: Constantemente un perito en informática forense obtiene nuevo conocimiento, debido al cambio continuo de las tecnologías de información y comunicación. Esto implica estar al tanto del desarrollo y creación de nuevos dispositivos, marcas, modelos, sistemas de seguridad, métodos de evasión de bloqueos, artefactos forenses, entre otros elementos relevantes. El conocimiento se consigue a través del tiempo, mediante la experiencia obtenida durante procesos de capacitación y el acompañamiento en la resolución de casos.

b. Dedicación: La dedicación es esencial, ya que cada peritaje presenta variables únicas. Esto hace que los peritos dediquen largos periodos a la adquisición y procesamiento de evidencia en las estaciones forenses. La minuciosidad y meticulosidad son fundamentales en cada etapa del proceso para garantizar la integridad de los datos y asegurar la obtención de resultados que sean repetibles y reproducibles, generando así información de valor que se encuentra dentro de grandes cúmulos de datos.

c. Ser autodidacta: Para realizar un trabajo adecuado y de calidad, se necesita capacitación constante sobre el uso apropiado de herramientas forenses, actualización de los procesos de adquisición y análisis, y capacitaciones avanzadas y puntuales sobre la especialidad. Como se ha mencionado, la tecnología avanza sin dar tregua, lo cual obliga a los peritos a buscar información en *webinars*, videos, foros, libros, congresos, sitios *web* oficiales de herramientas forenses y realizar consultas directas con otros expertos, para tratar casos puntuales por la variabilidad estos, demostrando proactividad y un aprendizaje autodidacta.

d. Vocación: Todo perito, indistintamente de su especialidad, debe tener una sólida vocación de servicio, ya que enfrentará situaciones desafiantes y diversas. Por ejemplo, los peritos podrían encontrar archivos de todo tipo, como documentos con derechos de autor, documentación financiera, mensajes de extorsión, registros de llamadas, videos de asesinatos, fotografías íntimas o archivos de abuso sexual infantil, entre otros. En este contexto, es crucial que los peritos mantengan un alto nivel de profesionalismo, ética y responsabilidad.

e. Ser ético: Según el Código de Ética del Instituto Nacional de Ciencias Forenses de Guatemala -INACIF- (2021) "La ética es aquel conjunto de virtudes que nos hacen ser mejores personas y, en consecuencia, a quienes desempeñamos una función pública, nos hace ser mejores servidores." (p. 5). El perfil de todo perito de cualquier especialidad, debe inspirar confianza y credibilidad, a través de la aplicación de integridad, independencia, imparcialidad, objetividad y confidencialidad, respetando en todo momento la dignidad de las víctimas.

Para tratar casos puntuales que contienen archivos de abuso sexual infantil, un perito en informática forense debe contar con las características mencionadas, además de otras habilidades técnicas para realizar su trabajo adecuadamente, siguiendo los lineamientos y procesos requeridos por las buenas prácticas forenses.

Es importante resaltar que el análisis informático forense comprende técnicas científicas y analíticas para extraer e interpretar datos e información en dispositivos de procesamiento y almacenamiento digitales. Estos procesos forenses buscan evitar alteraciones sobre la evidencia digital, garantizando la identidad e integridad. Por lo tanto, un perito en informática forense debe manejar adecuadamente las distintas fuentes de datos en la evidencia digital, en especial en casos que involucran archivos de abuso sexual infantil. Esto implica considerar aspectos técnicos y legales, siguiendo las normativas nacionales y las buenas prácticas del ámbito internacional.

Para abordar casos de este tipo, los peritos en informática forense deben tener un conocimiento adecuado de la terminología utilizada, estar familiarizados con los ciberdelitos, conocer los métodos de transmisión de archivos, y reconocer los signos o símbolos utilizados por pedófilos. También deben comprender el propósito de las imágenes de persuasión y conocer la relación que tienen las palabras clave con este delito.

Es posible que durante el análisis de los indicios iniciales que se clasifican como un delito diferente, el perito en informática forense encuentre imágenes de persuasión que generen sospechas de la existencia de archivos de abuso sexual infantil. Durante el análisis, el perito puede considerar prudente etiquetar dicho material relevante y, como resultado de la pericia se puede informar el hallazgo de archivos de posible abuso sexual infantil de acuerdo con el Decreto 21 de 2006 [con fuerza de ley]. Este hallazgo se reporta a la fiscalía para que proceda como corresponde, según sus criterios de investigación. Debe destacarse que el perito utiliza el término "posible", ya que no es parte de sus competencias establecer en el dictamen si la persona que aparece en las imágenes o videos es un niño, niña o adolescente, debido a que este extremo debe ser dictaminado por un médico forense.

Etimología del término "pornografía infantil"

En algunos países, como en Guatemala, aún se utiliza erróneamente el término "pornografía de personas menores de edad", o incluso "pornografía infantil" en referencia a la explotación sexual de niños, niñas y adolescentes. Sin embargo, organismos internacionales como la Organización Internacional de Policía Criminal -INTERPOL- el Fondo de las Naciones Unidas para la Infancia -UNICEF- (por sus siglas en inglés), el Centro Internacional para Niños Desaparecidos y Explotados -ICMEC- (por sus siglas en inglés) y *End child prostitution,*

child pornography and trafficking of children for sexual purposes -ECPAT- (por sus siglas en inglés), que trabajan para proteger a niños, niñas y adolescentes y poner fin a la explotación sexual, recomiendan no utilizarlo y en su lugar emplear una terminología adecuada basada en las orientaciones de Luxemburgo.

Las Orientaciones de Luxemburgo proporcionan directrices claras sobre cómo utilizar un lenguaje estandarizado al hablar de explotación y abuso sexual de menores. Estas directrices buscan evitar la victimización adicional de los niños, niñas y adolescentes al utilizar términos inapropiados que puedan minimizar la gravedad de los delitos o estigmatizar a las víctimas (Grupo de Trabajo Interinstitucional en Luxemburgo, 2016).

Para comprender mejor este error, es importante analizar la etimología de la palabra "pornografía". Esta proviene de la combinación de dos términos que se describen a continuación: "porno", que deriva del griego *porne* y significa "prostituta", y "grafía", que proviene del griego *grapho*, y se refiere a "escribir" o "representar gráficamente" (Mazo, 2019). Por lo tanto, se puede concluir que la pornografía se refiere a la representación visual de la prostitución.

Por lo tanto, es fundamental comprender que "si hay niños implicados, no es porno. Es un delito. Es Abuso" (INTERPOL, s.f, "Delito grave, definición acorde", párrafo 4). Por estos motivos, el término correcto para describir este tipo de delito es material de abuso sexual infantil. Con esto también se tiene el objetivo de generar una conciencia mundial sobre la gravedad de este delito y proteger adecuadamente a los niños niñas y adolescentes contra cualquier forma de abuso sexual infantil.

El Ciberdelito

Según Peña y Almaza (2010), un delito se define como una acción típica antijurídica y culpable. Por otra parte, Córdova (2020) afirma que un delito es una acción u omisión que ocasiona un resultado (p. 41).

Cuando hablamos de ciberdelito nos referimos esencialmente a acciones antijurídicas que se llevan a cabo mediante el uso de dispositivos informáticos o a través del uso de internet. Alaminos y Maza (2019) en su página *web*, describen el ciberdelito como un término genérico que engloba actividades delictivas de las acciones en internet o relacionadas, llevadas a cabo mediante equipos informáticos o a través del mismo internet.

Existen diferentes tipos de ciberdelitos, por ejemplo, el *hacking* que busca vulnerar sistemas y acceder a ellos sin ningún tipo de autorización; extorsión sexual, que consiste en exigir a las personas dinero o algún beneficio para no publicar fotografías íntimas; *ciberbullying* que consiste en acoso masivo en redes sociales; la piratería digital que infringe derechos de autor; el *sexting* que no es catalogado como ciberdelito, sin embargo, si participa un menor de edad, se puede clasificar como acoso a menores de edad; y la producción de material de abuso sexual infantil, que abarca la producción, consumo, distribución y posesión de archivos digitales relacionados.

Métodos de envío de archivos con contenido de abuso sexual infantil

El uso de las tecnologías de información y comunicación ha revolucionado la forma en que nos conectamos con otras personas en todo el mundo. Estas tecnologías nos permiten comunicarnos de manera instantánea. Además, han facilitado la transmisión de datos y archivos en tiempo real.

Sin embargo, se debe reconocer que el uso inapropiado de estas tecnologías, puede tener graves consecuencias, especialmente cuando se trata de transmisión de archivos con contenido de abuso sexual infantil. Este tipo de contenido se refiere a fotografías y videos en donde se observan a menores de edad mostrando sus partes genitales o se ven involucrados en actividades sexuales explícitas reales o simuladas (ICMEC, 2016).

Es importante mencionar que existen muchas formas de transmisión de archivos y para ello se describirán algunos métodos. Entre ellos se encuentran las redes *peer-to-peer* -P2P- (por sus siglas en inglés), también denominadas como redes de igual a igual. Estas redes se establecen mediante la instalación de programas como Ares, Torrent, Bit Torrent, UTorrent, Emule, entre otras.

En una red P2P, cada computadora que instala uno de estos programas se convierte en un nodo dentro de una red más grande de computadoras. El objetivo de esta red es compartir información entre los usuarios, aprovechando las características particulares de este tipo de redes. Según Millán (2006); algunas de estas características son:

a.

b. Ausencia de un servidor centralizado: en una red P2P no se necesita de un servidor centralizado para gestionar las transferencias, por lo que los archivos para compartir están a disposición de todos los usuarios de la red.

c. Distribución de costos entre los usuarios: en este tipo de red, los usuarios pueden solicitar archivos de otras computadoras, pero a cambio deben brindar otros

Otros medios de envío comunes son las aplicaciones de mensajería instantánea como *WhatsApp, Facebook Messenger, Telegram, Instagram*, entre otras, que son utilizadas para transmitir archivos de distinto tipo. Se debe resaltar que dichas aplicaciones han sido utilizadas por muchas personas, en particular adolescentes, para practicar *sexting*.

Una característica de la aplicación de mensajería instantánea *WhatsApp* es que se pueden generar grupos de hasta 256 usuarios, en los cuales se pueden enviar todo tipo de archivos, incluyendo los que infringen los derechos de autor, archivos de audio, archivos de video entre otros. Se debe tener cuidado con estas aplicaciones, pues de tener por defecto la opción de descarga automática de archivos, se puede generar un problema grave para los usuarios. Si algún miembro del grupo envía archivos con contenido de abuso sexual de menores de edad, de manera automática estará almacenándose en el dispositivo y puede ser en algún momento parte del delito de tenencia, posesión o distribución de material de abuso sexual infantil (Sánchez, 2020).

Signos de identificación, palabras clave e imágenes de persuasión

El astrofísico Sagan (1980, como se citó en Díaz, 2019) hizo mención de una frase muy interesante, "la ausencia de evidencia, no es evidencia de ausencia", la cual nos indica que aun cuando no hubiera evidencia visible, no significa que no exista. A todos los que somos forenses, esta frase nos hace mucho sentido y nos reta, ya que es importante realizar y aplicar metodologías validadas previamente, para la obtención de evidencia latente.

En un análisis informático forense se tiene como objetivo recoger información mediante métodos de restauración de archivos eliminados, búsqueda, localización y obtención de datos o información que sea útil y tenga valor para la investigación y resolución de casos que investiga el Ministerio Público. Como se ha indicado, es importante tener una capacitación constante para tener conocimiento de signos, símbolos, y palabras clave que puedan despertar alertas de posibles actividades ilícitas ocultas.

Entre estos signos se encuentran figuras o imágenes utilizadas para la identificación de pedófilos en la *web*, con el propósito de compartir información dentro de su red de contactos. Generalmente, en casos de abuso sexual infantil hay signos y símbolos que indican la necesidad de aplicar métodos de restauración profunda sobre los dispositivos de almacenamiento digital. A continuación, se describen algunos de estos:

a. Símbolos pedófilos: en 2007, según el boletín de la Buró Federal de Investigaciones -FBI- (por sus siglas en inglés), existen símbolos e isotipos que utilizan los pedófilos para identificarse entre ellos. Estos símbolos regularmente se muestran como dos figuras; una pequeña, que representa al niño, dentro de una de mayor tamaño que representa al adulto. Por ejemplo, dos figuras triangulares en las posiciones descritas pueden representar a un adulto con interés en niños varones (ver figura 1). Asimismo, otras figuras como un corazón pequeño y otro grande pueden representar a un adulto con interés en niñas. Además, una mariposa formada por corazones puede representar a adultos que no tienen preferencia en cuanto a si son niños o niñas.

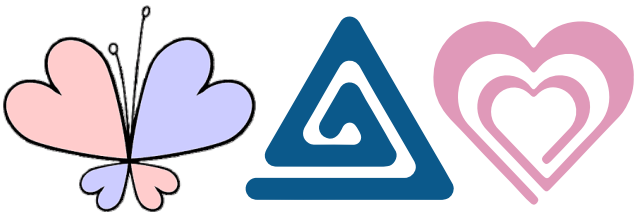


Figura 1. Símbolos que pueden ser utilizados por pedófilos. Adaptado de *Todos los símbolos que utilizan los pedófilos para identificarse que deberíamos conocer* [Fotografía], por La Vanguardia, 2020, https://n9.cl/1j5y0

b. Pedobear: el oso pedófilo es una caricatura que fue creada presuntamente en un sitio de humor negro en 1996. Dicha caricatura fue adoptada por pedófilos como símbolo de identificación. Este oso se muestra en fotografías junto a niños y niñas en distintas situaciones, dando la impresión de que este está acechándolos. Es curioso que este oso se haya convertido en un sello de aprobación (ver figuras 2 y 3), lo que plantea la pregunta ¿aprobación de qué? La respuesta es la aprobación de artículos sexuales, que, por llevar dicho sello, en teoría pueden ser utilizados con niños como se muestra en la figura 4.

Figura 2. Sello de aprobación Pedobear. Adaptado de *Pedobear's seal of approval* [Figura], por Rage Comics, s.f. https://n9.cl/0y9ex

Figura 3. Calcomanía de Pedobear captado en un vehículo particular. La fotografía fue tomada en la Ciudad de Guatemala.

Figura 4. Artículos sexuales con sello Pedobear. Adaptado de *So many things are wrong with this picture let me begin* [Fotografía] por foro JoyReactor, s.f. http://joyreactor.com/post/529018

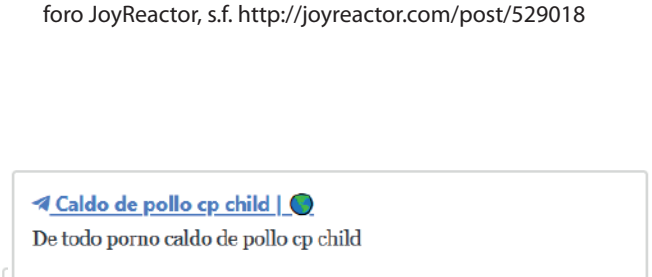


Figura 5. Capturas de pantalla de *Telegram* publicadas en la *web*. Se observan dos grupos de *Telegram* con mensajes ocultos.

Figura 6. Anuncio por medio del que se sugiere potencial distribución de material de abuso sexual infantil publicado en un libro de cupones. Se observa el uso de las siglas CP y la figura de Pedobear. Adaptado de *Bear meme ad por Farquhar,* 2011, https://n9.cl/dgufa

c. Palabras Clave: cuando nos referimos a palabras clave hacemos referencia a un juego de palabras que se inician con las mismas letras para aparentar otra cosa. Entre las más comunes se mencionan, por ejemplo: "Caldo de Pollo", "Camión Pesado", *"Cheese Pizza" "Club Penguin"*, las cuales comienzan con las siglas CP, que en inglés se refieren a *Child Pornography*, que se traduce como pornografía infantil (Trujillo, 2019). Estas palabras denotan que es necesario realizar, mediante la aplicación de *software* forense, procesos de parsing que consisten en la lectura de palabra por palabra, dentro de un gran conjunto de datos, contenidos en un medio de almacenamiento digital, lo que permite localizar conversaciones, archivos y otro tipo de información referente al CP (ver figuras 5 y 6).

d. Imágenes de persuasión: estas son en las que se muestra a personajes de dibujos animados en actos sexuales explícitos. Según la doctora Dupuy (2020), fiscal especializada en delitos y contravenciones Informáticas del Ministerio Público de Argentina, son utilizadas por los pederastas para hacer creer al niño o niña que es normal la actividad que realizan dichos personajes. El objetivo para ellos es que el menor observe pornografía animada y de esa manera aprovecharse de su víctima (ver figura 6).

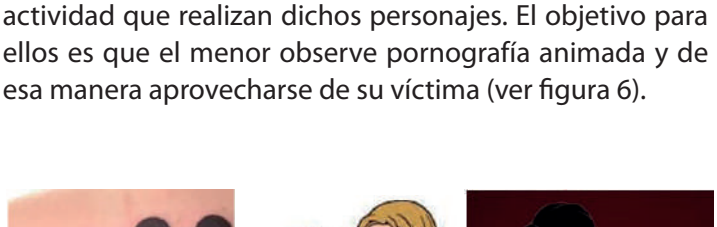


Figura 7. Imágenes de persuasión localizadas en caso real. Obtenido de computadora analizada en el Laboratorio de Informática Forense, durante 2020.

Herramientas Forenses

Usualmente, para una pericia informática se requiere de *hardware* y *software* especializado capaz de realizar las tareas de recolección, análisis y asistencia de la interpretación de los diversos artefactos forenses que requiere la experticia (Pressman y Pallazi, 2016). Estas herramientas son fundamentales para efectuar procesos de adquisición, preservación y análisis de datos, al tiempo que garantizan la autenticidad, identidad e integridad de la evidencia digital.

Existen diferentes herramientas forenses para la protección contra escritura del dispositivo, lo que facilita la creación de copias forenses y aseguran que la evidencia digital original no será alterada accidental o intencionalmente. Además, se emplean programas de recuperación de archivos borrados, que examinan dentro de cada sector de la unidad de almacenamiento, lo que permite localizar evidencia latente que puede ser de valor para la investigación.

También se hace mención de programas de análisis de información que aplican filtros, realizan el despliegue de llamadas y mensajes, permiten visualizar imágenes previas, hacen el *parsing* de palabras, examinan bases de datos, abren y analizan registros del sistema, analizan correos electrónicos y decodifican datos hexadecimales, entre otras funciones.

Entre todas estas bondades, también encontramos la categorización de archivos que consiste en la aplicación de algoritmos de analítica de contenido, mediante inteligencia artificial, que permiten identificar y clasificar entre imágenes y videos, similitud de rostros, vehículos, dinero, drogas, armas de fuego, desnudez y posible abuso sexual infantil, entre otros. Todo esto es fundamental desde el punto de vista del perito en informática forense, ya que contar con herramientas forenses de *hardware* y *software*, propician la aplicación de los procesos forenses que exigen las buenas prácticas y el fortalecimiento del sistema de justicia.

CONCLUSIONES

El perito en informática forense debe ser un profesional o especialista en técnicas necesarias para el cumplimiento de su deber, lo que conlleva tener un perfil adecuado, que incluye conocimientos académicos sobre la especialidad, capacidad de ser autodidacta, tener experiencia, dedicación, vocación y contar con principios éticos sólidos.

El término "pornografía infantil" o "pornografía de personas menores de edad" no es una definición apropiada, debido a que la pornografía es un término utilizado para referirse a adultos que realizan actos sexuales consentidos. Para los casos de menores de edad, el término correcto es "material de abuso sexual infantil".

Existen signos, símbolos y palabras clave que son utilizadas por los pedófilos, como un método que les permite encontrarse e identificarse en la *web,* con el fin de establecer contactos o grupos para solicitar o compartir material de abuso sexual infantil.

El análisis informático forense comprende técnicas científicas y analíticas que permiten la extracción e interpretación de datos o información contenida en dispositivos de procesamiento y almacenamiento digital. Estos procesos forenses buscan evitar alteraciones en la evidencia digital, garantizando su identidad e integridad.

En cuanto a los archivos obtenidos en la pericia, que corresponden a material de abuso sexual infantil, el perito en informática forense no puede determinar si las personas que aparecen en las imágenes o videos son niños, niñas o adolescentes, debido a que este extremo debe ser dictaminado por un médico forense.

BIBLIOGRAFÍA

Alaminos, M. y Maza, P. (4 de marzo de 2019). *¿Qué es el Ciberdelito?* . Intelectual Abogados. Recuperado el 25 de marzo de 2023, de https://intelectualabogados.com/delitos-informaticos-ciberdelitos-y-delitos-en-redes-sociales/que-es-el-ciberdelito/

Centro Internacional para Niños Desaparecidos y Explotados. (2016). *Abuso y Explotación Sexual Infantil en Línea.* https://cdn.icmec.org/wp-content/uploads/2020/09/Estudo-Legislativo-ICMEC_UNICEF-ES.pdf

Córdova, W. (2020). La Teoría de la Imputación Objetiva. *Revista la Teoría del Delito en el Proceso Penal,* 179, 41-49.

Instituto Nacional de Ciencias Forenses. (2021). Código de Ética Institucional. https://inacif.gob.gt/docs/uip/codigo_de_etica.pdf

Decreto 21-2006 [con fuerza de ley]. Ley Contra la Delincuencia Organizada. (19 de julio de 2006). Artículo 63. D.O. No. 90. Guatemala.

Decreto 51-92: Código Procesal Penal Guatemalteco. (s.f.). Recuperado el 25 de marzo de 2023

Díaz, J. (19 de julio de 2019). *Los grandes pensamientos de Carl Sagan.* Catalunyapress. Recuperado el 24 de marzo de 2023, de https://www.catalunyapress.es/texto-diario/mostrar/1484245/grandes-pensamientos-carl-sagan

Dupuy, D. (2020). Webinar: *Nuevas Herramientas en Investigaciones Criminales.* Centro de Capacitación Judicial Misiones. https://www.youtube.com/watch?v=DS9r8nf1Hhg

Farquhar, P. (22 de marzo de 2011). *Bear meme ad.* News.com.au . https://n9.cl/dgufa

Federal Bureau Of Investigation Intelligence. (31 de enero de 2007). *Symbols and Logos Used by Pedophiles to Identify Sexual Preferences.* https://wikileaks.org/w/images/a/a1/FBI-pedophile-symbols-page1.jpg

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

Instituto Nacional de Clencias Forenses. (28 de septiembre de 2021). *Código de Ética Institucional.* Obtenido de Código de Ética Institucional: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj6gKDdnYb-AhUUVTABHX_PCh8QFnoECBIQAQ&url=https%3A%2F%2Finacif.gob.gt%2Fdocs%2Fuip%2Fcodigo_de_etica.pdf&usg=AOvVaw01tjRczSOFQOLvDN4ds_mD

Instituto de la Defensa Pública Penal de Guatemala. (agosto de 2018). *Teoría del Delito.* Recuperado el 24 de marzo de 2023, de http://biblioteca.oj.gob.gt/digitales/45580.pdf

Jonhnson, T. (2006). *Forensic Computer Crime Investigation.* New York: Taylor & Francis Group.

Martínez, M. (23 de septiembre de 2022). *El Código Deontológico del Perito Informático.* JDG peritajes informáticos. Recuperado el 29 de marzo de 2023, de https://jdgperitajesinformaticos.es/el-codigo-deontologico-del-perito-informatico/

Mazo, I. (2019). *Estudio de la narrativa pornográfica: la evolución del porno comercial* [Tesis de doctorado, Universitat Politècnica de València]. Repositorio Institucional UPV.

Millán, R. (abril de 2006). *Características de las Redes P2P.* Consultoría estratégica en tecnologías de la información y comunicaciones Recuperado el 2023 de marzo de 23, de https://www.ramonmillan.com/libros/librodistribucionlibrosredesp2p/distribucionlibrosredesp2p_caracteristicasp2p.php#beneficiosp2p

Naciones Unidas. (2011). *Observación General 13*: *Derecho del niño a no ser objeto de ninguna forma de violencia.* Convención sobre los Derechos del Niño.

Newman, R.(2007). Computer Forensics: *Evidence Collection and Management.* New York, United States of America: Auerbach Publications.

Organización Internacional de Policía. (s.f.). *Terminología Apropiada.* Recuperado el 2023 de marzo de 23, de https://www.interpol.int/es/Delitos/Delitos-contra-menores/Terminologia-apropiada

Pedobear's seal of approval (s.f.). Rage Comic. https://n9.cl/0y9ex

Peña, O. y Almanza, F. (2010). *Teoría del Delito.*
https://static.legis.pe/wp-content/uploads/2019/06/Teoria-del-delito.pdf

Pressman, G., y Pallazi, P. (2016). El uso de Software abierto para el análisis de la evidencia digital. El Derecho, 13.932. https://docplayer.es/90297795-El-uso-de-software-abierto-para-el-analisis-de-la-evidencia-digital.html

Real Academia Española. (s.f.). Cultura. En Diccionario de la lengua española. Recuperado el 24 de marzo de 2023, de https://dle.rae.es/perito?m=form

Rubio Alamillo, J. (28 de mayo de 2020). *Diferencias entre la respuesta ante incidentes (DFIR) y el peritaje informático.* Perito Informático.
https://peritoinformaticocolegiado.es/blog/diferencias-entre-la-respuesta-ante-incidentes-dfir-y-el-peritaje-informatico/

Sánchez, F. (2020). Conversaciones de la aplicación WhatsApp y ejemplos de su valor probatorio como evidencia digital en la legislación guatemalteca. *Diálogo Forense,* 2(2), 59.

Secretaría contra la Violencia Sexual Explotación y Trata de Personas. (2019). Guía Educa-VET. https://svet.gob.gt/wp-content/uploads/2022/08/GUIA-EDUCAVET-2021.pdf

So many things are wrong with this picture let me begin. (s.f.) foro JoyReactor. http://joyreactor.com/post/529018

Todos los símbolos que utilizan los pedófilos para identificarse que deberíamos conocer. (16 de octubre de 2020). La Vanguardia. https://n9.cl/1j5y0

Trujillo, S. (19 de septiembre de 2019). *La perturbadora palabra clave que usan los pedófilos para buscar pornografía infantil en internet.* Fayer Wayer. Recuperado el 26 de marzo de 2023, de https://www.fayerwayer.com/2019/09/pornografia-infantil-caldo-de-pollo/

Tusla, Police Department. (s.f.). An Introduction to Pedo Bear. *A Public Information Bulletin.* oklahoma, Tusla, United States. Recuperado el 29 de marzo de 2023, de A Public Safety Information Bulletin: https://www.yumpu.com/en/document/read/16878989/an-introduction-to-pedo-bear-a-public-safety-worldnow