Vol.8 No.3 (2024): Journal Scientific Investigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.8.3.2024.4076-4097

Forensic Analysis on Android Mobile Devices for Cyberextortion Cases, Systematic Literature Review

Análisis Forense en Dispositivos Móviles Android para Casos de Ciberextorsión, Revisión Sistemática de Literatura

Autores:

Banegas-Crespo, Danilo Adrián
UNIVERSIDAD CATÓLICA DE CUENCA
Maestrante
Cuenca – Ecuador

danilo.banegas.35@est.ucacue.edu.ec

https://orcid.org/0009-0001-6413-8370

Andrade-Pesantez, Daniel Jacobo
UNIVERSIDAD CATÓLICA DE CUENCA
Docente Tutor del área
Cuenca – Ecuador

dandradep@ucacue.edu.ec

https://orcid.org/0000-0003-0586-4038

Fechas de recepción: 20-JUL-2024 aceptación: 27-AGO-2024 publicación:15-SEP-2024

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

El documento aborda el análisis forense de dispositivos móviles Android en casos de ciberextorsión, destacando la necesidad de un procedimiento actualizado debido al aumento de estos delitos en América Latina y Ecuador. El objetivo principal es desarrollar un procedimiento forense basado en la norma ISO/IEC 27037:2012, que permita la identificación, recolección, preservación y análisis de evidencia digital de manera eficaz y legalmente admisible. La metodología incluye una revisión de la literatura y el desarrollo de un procedimiento forense siguiendo estándares y normas internacionales. El estudio concluye enfatizando la importancia de adoptar estándares internacionales y la formación continua de los profesionales en el campo para contribuir significativamente a la resolución de casos de ciberextorsión que involucren dispositivos móviles Android. Se subraya que un procedimiento forense bien estructurado puede mejorar la eficacia de las investigaciones y la confiabilidad de la evidencia, destacando la necesidad de una capacitación constante para los profesionales involucrados en estas investigaciones.

Palabras clave: Ciberextorsión; análisis forense; dispositivos Android; evidencia digital; ISO/IEC 27037:2012

Abstract

The document addresses the forensic analysis of Android mobile devices in cases of cyber extortion, highlighting the need for an updated procedure due to the increase in these crimes in Latin America and Ecuador. The main objective is to develop a forensic procedure based on the ISO/IEC 27037:2012 standard, allowing for the identification, collection, preservation, and analysis of digital evidence in an effective and legally admissible manner. The methodology includes a literature review and the development of a forensic procedure following international standards and norms. The study concludes by emphasizing the importance of adopting international standards and the continuous training of professionals in the field to significantly contribute to the resolution of cyber extortion cases involving Android mobile devices. It underscores that a well-structured forensic procedure can enhance the effectiveness of investigations and the reliability of evidence, highlighting the need for constant training for professionals involved in these investigations.Resumen del artículo, en idioma inglés.

Keywords: Cyber extortion; forensic analysis; Android devices; digital evidence; ISO/IEC 27037:2012

Introducción

En los últimos años, América Latina ha experimentado un aumento significativo de ciberataques, destacando la ciberextorsión como una de sus derivaciones más preocupantes. En 2021, se registró un aumento del 600% de ataques informáticos en América Latina y el Caribe, con 289.000 millones de intentos de ciberataques, siendo México el país más afectado con el 53,9% de los intentos, seguido por Brasil con el 30,6% (Vera, 2022). En 2023, los ataques de phishing, ransomware y troyanos incrementaron un 617% con más de 286 millones de intentos (Rivera, 2023). Ecuador ha sido particularmente afectado, situándose como el tercer país en América Latina con mayor número de incidencias en 2024 (El Universo, 2024). Entre enero y septiembre de 2023, la Policía Nacional del Ecuador registró 5.930 denuncias de extorsión, un aumento significativo respecto al año anterior (La Hora, 2023b), y con la "extorsión virtual" representando el 57% de los casos, donde se utilizan medios digitales para chantajear a las víctimas (Primicias, 2023).

Con respecto a los dispositivos móviles, especialmente aquellos con sistema operativo Android, han sido blancos de ciberdelincuentes que buscan robar, manipular o extorsionar a los usuarios (Manrique, 2019). Un ejemplo de ciberextorsión en Quito involucró a una banda que creaba perfiles falsos en redes sociales para reclutar jóvenes, obtener fotos y videos íntimos y luego exigir dinero a cambio de no revelar el material (La Hora, 2023a). La informática forense fue crucial en este caso para recopilar, analizar y presentar pruebas digitales en un contexto legal. Los resultados del análisis forense pueden utilizarse en procedimientos judiciales o a petición de organizaciones para identificar violaciones de seguridad, y los investigadores forenses pueden ser responsables civil y penalmente por errores o pérdida de pruebas (Corredera, 2023).

Por ello, es necesario tener presente a la Ley Orgánica de Protección de Datos Personales, promulgada en Ecuador el 26 de mayo de 2021, ya que es un marco legal destinado para proteger los derechos a la privacidad y la dignidad humana. Esta ley define información personal como "cualquier dato que directa o indirectamente identifique o haga identificable a una persona física". Además, la ley establece que la protección de datos personales es un derecho inherente a la dignidad humana (Niubox, 2021). Se debe tener presente que los datos personales deben ser tratados de manera transparente y segura y con el consentimiento explícito del titular de los datos. Esto significa que los profesionales en análisis forense deben cumplir con los estándares de seguridad y privacidad al recopilar, analizar y almacenar información relacionada con casos judiciales.

Además, el Código Orgánico Integral Penal (COIP) de Ecuador, en su artículo 190, tipifica el delito de "Acceso no consentido a un sistema informático, telemático o de telecomunicaciones", proporcionando un marco legal relevante para la investigación de delitos informáticos en el contexto del análisis forense digital. Asimismo, el COIP define el contenido digital como “todo acto informático que representa información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático”, que pueden ser utilizados como evidencia en procesos judiciales. Por ello, la cadena de custodia es

fundamental para garantizar la integridad de la evidencia digital, asegurando que el contenido digital presentado como prueba no haya sido alterado durante la investigación (Código Orgánico Integral Penal (COIP), 2014).

Con base a lo antes indicado, y debido al incremento de incidencias relacionadas a la ciberextorsión en América Latina y Ecuador, y a esto sumado, el uso frecuente de dispositivos móviles Android en estos delitos, es fundamental contar con un procedimiento actualizado de análisis forense para este tipo de equipos; lo que permitirá a los expertos recopilar, analizar y presentar pruebas digitales efectivas en un contexto legal y estar al tanto de las metodologías y técnicas que aporten significativamente a la investigación de los casos judiciales.

En otro ámbito, se menciona que existen diversos estudios sobre el análisis forense de dispositivos móviles Android, como el realizado en la Universidad Nacional de Loja, Ecuador, que se han centrado en identificar, analizar y clasificar metodologías y herramientas forenses (Pozo et al., 2020). Otra investigación en la Universidad Católica de Cuenca desarrolló un framework y herramientas para el análisis forense en casos de cibergrooming, identificando metodologías como NIST, adquisición física y lógica, y DFRW, y herramientas como UFED, XRY, Oxygen Forensic y FTK Imager (Murudumbay, 2022). Estos estudios resaltan la necesidad de actualizar metodologías y herramientas debido a los rápidos cambios tecnológicos y las tácticas de los ciberdelincuentes, propiciando así la estandarización de procedimientos para garantizar su aceptación legal.

Para abordar las brechas de conocimiento identificadas, se propone el objetivo general de desarrollar un procedimiento de análisis forense para dispositivos móviles Android en casos de ciberextorsión, utilizando metodologías y técnicas adecuadas para obtener resultados que contribuyan significativamente a la investigación de estos delitos.

En resumen, este trabajo representará un aporte importante para la línea dedicada a la informática forense y tendrá un impacto positivo en la lucha contra la ciberextorsión. Se espera que los resultados de esta investigación sean de interés para los investigadores, profesionales y organismos encargados de hacer cumplir la ley y que trabajan en el campo de la informática forense y la ciberseguridad.

Se menciona que el presente artículo dispone de una estructura de información que inicia con la descripción de la metodología de investigación, mediante la cual se basó todo el proceso investigativo. Como siguiente punto, se dispone de la presentación de los resultados, los cuales están presentados de la siguiente manera: Directrices y normas aplicables a la informática forense en dispositivos móviles, Lineamientos y desafíos para el análisis forense de dispositivos móviles Android basado en la norma ISO 27037:2012, Procedimiento de análisis forense de dispositivos móviles Android, basado en la norma ISO 27037:2012 y Recomendaciones técnicas para el apoyo a casos comunes de ciberextorsión; luego se entabla un espacio de discusión con el análisis de resultado y finalmente la presentación de las conclusiones obtenidas de la presente investigación

Metodología

La investigación se basó en el método cualitativo para entender y categorizar las técnicas y metodologías, ejecutando dos etapas clave. La primera etapa fue una revisión de la literatura para comprender y categorizar las técnicas y metodologías disponibles dirigidas al análisis forense de dispositivos móviles Android. La segunda etapa consistió en el desarrollo de un procedimiento de análisis forense, basado en la norma ISO 27037:2012, para identificar métodos adecuados para casos de ciberextorsión.

Para cumplir con lo anterior, se siguieron varios pasos. Primero, se revisó el marco jurídico relacionado con la informática forense y la ciberextorsión, incluyendo la Ley Orgánica de Protección de Datos Personales (LOPDP), el COIP y regulaciones internacionales aplicables. Luego, se revisó la literatura publicada en los últimos 5 años sobre normas y estándares internacionales aplicables a la informática forense en dispositivos móviles, y se identificaron las técnicas y metodologías actuales en el análisis forense de dispositivos móviles Android; las mismas que están basadas en criterios con conformidad con la norma ISO 27037:2012, y se realizaron búsquedas en bases de datos como IEEE Xplore, ScienceDirect, Biblioteca Virtual Ucacue, Scielo.org, Google Scholar, etc.; utilizando palabras clave como “análisis forense digital”, “dispositivos móviles”, “Android”, “ciberextorsión“, “ISO 27037:2012”, entre otras.

Luego, se desarrolló un procedimiento de análisis forense de dispositivos móviles Android basado en normas y estándares reconocidos. Este procedimiento incluyó instrucciones detalladas para identificar, adquirir, analizar y presentar evidencia digital, siendo diseñado específicamente para procesos legales de ciberextorsión sobre dispositivos móviles Android. Además, se hicieron recomendaciones técnicas para identificar casos comunes de estudio y ajustar el procedimiento según las necesidades.

La metodología se enfocó en la hipótesis de que un procedimiento de análisis forense adecuado y actualizado para dispositivos móviles Android en casos de ciberextorsión permitiría obtener resultados significativos para las investigaciones. Con base a ello, las variables independientes incluyeron las metodologías y técnicas de análisis forense, los procedimientos a seguir y las herramientas forenses de software utilizadas, mientras que la variable dependiente fue la evidencia digital recuperada y analizada.

Finalmente, en términos de fuentes de información primaria, se utilizaron: Directrices Globales para Laboratorios de Forense Digital de INTERPOL, Requisitos Mínimos para la Evidencia Digital y Multimedia de la Alianza Estratégica Internacional Forense (IFSA), Reglamento General de Protección de Datos (RGPD), ISO/IEC 27037:2012, NIST Special Publication 800-86 y otras normas ISO relevantes. La recolección secundaria de datos incluyó la Ley Orgánica de Protección de Datos Personales (LOPDP), el Código Integral Penal (COIP) y diversas regulaciones internacionales relevantes para la informática forense y la ciberextorsión.

Resultados

En el presente estudio se consideraron los contenidos relacionados a la: Identificación, preservación, análisis y presentación de evidencia; además de la descripción detallada de las actividades y procedimientos involucrados en cada etapa. Cabe destacar que los conceptos antes mencionados, estuvieron enmarcados en las bases legales que rigen en el Ecuador, acerca del manejo de información y presentación de resultados, posterior a su análisis. Con base a lo mencionado, se presentan los siguientes resultados:

a. Directrices y normas aplicables a la informática forense en dispositivos móviles

En la actualidad, existen distintas directrices a nivel internacional que aportan significativamente a los procesos relacionados a la informática forense, estableciendo reglas sobre los cuales se apoyan las regulaciones que adopta cada país, que son mencionadas en la Tabla 1:

Tabla 1
Tabla Comparativa de Directrices Internacionales para la Informática Forense

Directriz	Descripción	Aplicación
Directrices Globales para Laboratorios de Forense Digital de INTERPOL	Proporcionan información de gestión de casos relacionados a dicho ámbito (Interpol, 2019).	Recibir solicitudes, registrar pruebas, fotografiar pruebas, realizar análisis, devolver pruebas y cerrar casos.
Requisitos Mínimos para la Evidencia Digital y Multimedia de la Alianza Estratégica Internacional Forense (IFSA)	Establecen requisitos mínimos para que los proveedores forenses emergentes brinden servicios científicos al sistema de justicia penal (IFSA, 2023).	Marco de competencias para el personal, equipos y suministros, recolección, análisis, interpretación, informes, procedimientos, protocolos, validación y control de calidad.
Reglamento General de Protección de Datos (RGPD)	Establece los principios de protección de datos personales en la Unión Europea (REGLAMENTO (UE) 2016/ 679, 2016). Base de conocimiento para la definición de Leyes de Protección de Datos Personales para otros países.	Aplica a las organizaciones que procesan datos sobre personas en la UE en la recopilación, almacenamiento, uso y eliminación de datos. Establece obligaciones de protección de datos, el consentimiento explícito para el procesamiento de datos personales y mantención de la confidencialidad.

Se debe tener presente que la informática forense de dispositivos móviles se basa en la aplicación de métodos científicos y analíticos para recopilar y preservar evidencia digital; por lo tanto, se insta en observar atentamente las reglas y regulaciones aplicables. Sin embargo, la utilización de estas regulaciones puede variar según la jurisdicción y el tipo específico de análisis forense realizado.

Complementando el análisis anterior, se realiza la comparación de las normas (marcos de referencia) internacionalmente reconocidas, que son relevantes en el ámbito del análisis forense de dispositivos móviles, como indica la Tabla 2:

Tabla 2
Tabla Comparativa de Normas Aplicables a la Informática Forense

Norma	Descripción	Aplicabilidad
ISO/IEC 27037:2012	Establece lineamientos para identificar, recolectar, recuperar y preservar evidencia digital. Confirmada en el 2018 por el Comité Técnico Conjunto ISO/IEC JTC 1.	Amplia, cubre una variedad de dispositivos y actividades. Asegura la integridad y admisibilidad de la evidencia digital.
NIST Special Publication 800-86	Proporciona pautas para integrar la tecnología forense en la respuesta a incidentes.	Específica para incidentes de ciberseguridad.
ISO/IEC 27041:2015	Proporciona guías de cómo un perito en informática y telemática debe analizar e interpretar evidencias digitales.	Específica para el análisis e interpretación de evidencias digitales.
ISO/IEC 27042:2015	Establece lineamientos para el análisis e interpretación de evidencias digitales.	Similar a la 27041:2015.
ISO/IEC 27043:2015	Especifica los principios y procesos para la investigación de incidentes.	Específica para la investigación de incidentes.
RFC 4998	Define estándares para la preservación de la información.	Específica para la preservación de la información.
RFC 6283	Define la sintaxis del lenguaje XML y las reglas de procesamiento que se deben seguir para crear una prueba de información completa.	Específica para la creación de pruebas de información.

Luego de un análisis comparativo de las normas antes citadas, se opta por la norma “ISO/IEC 27037:2012” basado en las siguientes razones:

- Amplitud de Aplicación: Proporciona directrices específicas de gestión y análisis de la evidencia digital, cubriendo una amplia gama de actividades aplicables.
- Integridad y Admisibilidad: Garantiza la integridad y admisibilidad de la evidencia digital; para que sea procesada de una manera aceptable en los tribunales de justicia.
- Aplicabilidad a Diversos Dispositivos: Se puede emplear en una amplia gama de dispositivos, entre ellos los teléfonos móviles con sistema operativo Android.
- Revisión y Actualización Regular: La norma ISO/IEC 27037:2012 fue revisada y validada en el año 2018, lo que indica que está acorde con los avances tecnológicos y las mejores prácticas en el campo de la informática forense.

En comparación con las normas antes mencionadas, la norma ISO/IEC 27037:2012 ofrece una cobertura más completa y actualizada de las actividades relacionadas con la evidencia digital.

b. Lineamientos y desafíos para el análisis forense de dispositivos móviles Android basado en la norma ISO 27037:2012

La norma ISO/IEC 27037:2012 establece lineamientos para el manejo adecuado de la evidencia digital en procesos forenses y se centra en la identificación, recopilación, obtención y preservación de esta evidencia. Es la base para el análisis forense de dispositivos móviles Android, y proporciona un marco metodológico que garantiza la integridad y admisibilidad de la evidencia digital en procedimientos judiciales (Zambrano, 2022). Se basa en los siguientes principios básicos: Aplicación de Métodos, Proceso Auditable y Proceso Reproducible.

Además, se mencionan en la tabla 3 los desafíos del análisis forense según (Martínez, 2016):

Tabla 3
Desafío en el análisis forense de dispositivos móviles Android

Desafío	Descripción
Diversidad de dispositivos	Gran variedad de dispositivos Android con diferentes versiones de sistema operativo y personalizaciones del fabricante.
Protección de datos	Dispositivos Android modernos tienen medidas robustas de seguridad, como el cifrado de datos, entre otros.
Recuperación de datos eliminados	Es posible recuperar cierta información eliminada, este proceso puede ser complejo y no siempre garantiza resultados.
Información volátil	Datos importantes pueden ser volátiles, es decir, pueden perderse o modificarse, como la información en la memoria RAM.
Legalidad y privacidad	Es fundamental respetar las leyes y regulaciones vigentes en cuanto a la privacidad y protección de datos personales.
Necesidad de herramientas especializadas	El análisis forense requiere de herramientas y técnicas especializadas, y de personal con la formación adecuada.

c. Procedimiento de análisis forense de dispositivos móviles Android, basado en la norma ISO 27037:2012 (Tabla 4)

Tabla 4
Procedimiento de análisis forense de dispositivos móviles Android, basado en la norma ISO 27037:2012

Etapa	Procedimiento	Recomendaciones	Correspondencia ISO 27037:2012
Identificación y Aseguramiento de la Evidencia Digital			
Identificación de Dispositivos	**Identificar** todos los dispositivos relacionados con el caso.	• Reconocer y diferenciar la información relevante para la investigación. • Asegurar que la evidencia no se altere, dañe o destruya durante la recolección, el transporte, el almacenamiento; presencial o a distancia. • Recoger la evidencia de tal manera que sea aceptada en procesos legales, lo que implica seguir una metodología rigurosa y documentada. • Tener personal con la formación adecuada para manejar la evidencia sin comprometer su validez. • Adaptarse a la variedad de dispositivos y tecnologías existentes. • Evitar la introducción de datos o metadatos. • Prevenir la alteración remota de la evidencia en dispositivos conectados. • Implementar herramientas que impidan la modificación de la evidencia durante su análisis.	**Cláusula 5.3 - Identificación:** Destaca la importancia de identificar de manera precisa y documentar todos los dispositivos que pueden contener evidencia digital relevante
Aseguramiento del Dispositivo	**Aislar los dispositivos** de toda red (modo avión), para evitar la activación de mecanismos de seguridad. - Si está encendido o pagado, mantenerlo en ese estado.		
Documentación	**Registrar estado del dispositivo** y características observables, (encendido, apagado, bloqueado, daños, etc.). - Fotografiar el dispositivo y anotar detalles como número de serie, marca, modelo y condiciones físicas.		

Etapa	Procedimiento	Recomendaciones	Correspondencia ISO 27037:2012
Recolección de Evidencia Digital			
Adquisición Lógica	**Capturar datos en vivo** de sistemas en funcionamiento, si es necesario. **Copiar los objetos almacenados** en el dispositivo utilizando mecanismos nativos. **Preservar el estado** del dispositivo y sus datos **Acceder a todos los ficheros** visibles y potencialmente a información eliminada.	• Utilizar herramientas forenses para extraer datos del sistema de archivos, aplicaciones y bases de datos, adecuadas para cada dispositivo. • Evitar el uso del dispositivo hasta que se haya realizado la copia forense. • Capturar datos de la memoria interna y de cualquier almacenamiento externo. • Incluir datos almacenados en la nube. • Seguir procedimientos para manejar grandes cantidades de datos • Disponer de técnicas para el acceso a datos protegidos por encriptación y contraseñas. • Capacitación continua de los profesionales sobre técnicas forenses y herramientas	**Cláusula 6.3 - Recolección:** resalta la importancia de recolectar la evidencia digital de una manera que preserve su integridad, lo cual incluye hacer copias forenses para evitar la alteración de datos
Adquisición Física	**Realizar una copia forense** bit a bit de los dispositivos. **Extraer el chip de memoria** para acceder a los datos directamente. **Usar JTAG (Joint Test Action Group)** para desbloquear y acceder a los datos almacenados en bruto en el chip de memoria (optativo).	• Se pone en consideración herramientas que cumplen con los objetivos (existe variedad en el mercado con características similares): **Adquisición Lógica:** Cellebrite UFED, Oxygen Forensic Detective, MSAB XRY, Elcomsoft Mobile Forensic Bundle, etc. **Adquisición Física:** Cellebrite UFED, Magnet AXIOM, Belkasoft Evidence Center, MSAB XRY, Android Data Extraction via Recovery (ADER), etc.	**Cláusula 6.4 - Adquisición:** especifica que la adquisición debe realizarse usando métodos que aseguren la precisión y la integridad de los datos, lo cual se logra utilizando herramientas y procedimientos forenses reconocidos

Etapa	Procedimiento	Recomendaciones	Correspondencia ISO 27037:2012
Preservación de Evidencia Digital			
Preservación de Evidencia Digital	**Guardar la copia forense** en un entorno seguro y protegido contra alteraciones.	• Seguir procedimientos rigurosos para garantizar el almacenamiento de la evidencia, considerando: * Etiquetado y Registro * Contenedor Adecuado * Control de Acceso * Ambiente Adecuado * Registro Digital * Documentación Detallada	**Cláusula 6.5 - Preservación:** enfatiza la importancia de preservar la evidencia digital de manera que su integridad no se vea comprometida, manteniendo registros detallados de la cadena de custodia
Cadena de Custodia	**Documentar cada acceso** y cambio de custodia de la evidencia para asegurar la trazabilidad.	• Mantener un registro riguroso de la cadena de custodia del dispositivo desde su incautación hasta su análisis y almacenamiento; es crucial para garantizar la integridad de la evidencia.	
Análisis de Evidencia Digital			
Análisis de Datos Recolectados	**Extraer información relevante** como mensajes de texto, correos electrónicos, registros de llamadas, ubicaciones GPS y cualquier otra información relevante.	• Reconocer y analizar adecuadamente la evidencia digital potencial, y que sea relevante, confiable y suficiente. • Mantener actualizadas las técnicas y herramientas de análisis forense, para evitar la obsolescencia. • Calificar a los profesionales que intervienen en el análisis forense, para brindar credibilidad de la investigación.	**Cláusula 7 - Análisis:** Aunque esta norma no se enfoca directamente en el análisis, el proceso debe seguir principios que aseguren la validez de los hallazgos, apoyándose en técnicas forenses
Detección de Aplicaciones Maliciosas	**Identificar software instalado** por parte del usuario o de manera automática.		
Recuperación de Datos Borrados	**Usar herramientas forenses para recuperar datos** de archivos		

Etapa	Procedimiento	Recomendaciones	Correspondencia ISO 27037:2012
	eliminados, mensajes y otras comunicaciones borradas.	• Considerar la existencia de la amplia gama de dispositivos, lo que requiere disponer de conocimientos especializados para cada tipo. • Proteger mediante el cumplimiento de procedimientos adecuados a la evidencia digital, que puede ser: alterada, dañada o destruida. • Considerar que la evidencia digital puede cruzar fronteras jurisdiccionales rápidamente y sin esfuerzo, lo que plantea desafíos legales y de cooperación internacional. • Registrar meticulosamente las actividades de análisis; incluye capturas de pantalla, registros de herramientas forenses y cualquier dato relevante. • Se pone en consideración herramientas que cumplen con los objetivos (existe variedad en el mercado con características similares): **Análisis de datos:** Belkasoft Evidence Center, Autopsy,Paraben E3 (Device Seizure), BlackLight, etc.	aceptadas para interpretar los datos de manera precisa
Análisis de comunicaciones:	**Examinar registros** de llamadas, mensajes SMS, correos electrónicos y aplicaciones de mensajería instantánea.		
Análisis de archivos multimedia:	**Revisar** fotos, videos y grabaciones de audio.		
Análisis de aplicaciones:	**Investigar aplicaciones** instaladas, su uso y datos almacenados.		
Análisis de redes:	**Investigar la actividad de red**, identificar conexiones a servidores, direcciones IP sospechosas, y patrones de tráfico inusuales.		
Metadatos:	**Examinar metadatos** de archivos y aplicaciones; obtener datos de las acciones del usuario, fechas, horas, modificación y acceso.		
Análisis de seguridad:	**Revisar configuraciones de seguridad** del dispositivo, incluyendo contraseñas, cifrado y autenticación e identifica vulnerabilidades.		
Detección de malware:	**Escanear el dispositivo** en busca de malware.		
Documentación Detallada:	**Registrar cada paso del proceso** de análisis		

Etapa	Procedimiento	Recomendaciones	Correspondencia ISO 27037:2012
	Presentación de informes		
Redacción y presentación	**Elaborar un informe pericial** que presente de manera clara y concisa los hallazgos. **Cumplir con los requisitos legales** y judiciales de la jurisdicción correspondiente. **Incluir una reconstrucción de los hechos** basada en la evidencia digital analizada. **Presentar el informe** ante la autoridad judicial competente. Estructura básica del Informe Forense: • Título y Fecha • Resumen Ejecutivo • Descripción del Caso • Metodología • Resultados del Análisis • Conclusiones y Recomendaciones • Anexos	• Presentar la evidencia de una manera precisa, basado en una metodología rigurosa, para que sea aceptable en un tribunal, • Incluir detalles completos de la cadena de custodia. • Documentar las herramientas y técnicas utilizadas en todo el proceso. • Realizar verificaciones cruzadas con otras fuentes de evidencia (de ser posible). • Utilizar un lenguaje claro y evitar terminología técnica compleja sin explicación. • Organizar de manera lógica, con una progresión desde la descripción del caso hasta las conclusiones. • Incluir gráficos, tablas y diagramas para ilustrar los hallazgos y facilitar la comprensión. • Incluir una descripción detallada de los procedimientos realizados, permitiendo que se pueda replicar el proceso. • Documentar todas las observaciones y decisiones tomadas.	**Cláusula 8 - Documentación de la Evidencia:** Resalta la importancia de documentar adecuadamente todas las actividades realizadas durante el manejo de la evidencia digital. La presentación de informes debe reflejar esta documentación detallada para asegurar la transparencia y reproducibilidad del análisis.

d. Recomendaciones técnicas para el apoyo a casos comunes de ciberextorsión

A continuación, se presentan recomendaciones para la aplicación de técnicas forenses específicas y medidas de seguridad para casos de ciberextorsión en dispositivos móviles Android, para garantizar una investigación detallada y protección de la víctima (Tabla 5).

Tabla 5
Recomendaciones técnicas para el apoyo a casos comunes de ciberextorsión

Caso	Contexto	Recomendaciones
Caso 1: Extorsión mediante Secuestro de Datos en un Dispositivo Android	Un usuario recibió un mensaje en su dispositivo Android indicando que sus datos personales habían sido cifrados y que debía pagar un rescate para recuperarlos.	**Aislamiento del dispositivo** (Modo avión) para detener la comunicación con el servidor del atacante. **Adquisición de Datos:** Cree una imagen completa de la memoria del dispositivo. **Análisis de datos y aplicaciones:** Analice todas las aplicaciones instaladas y sus permisos para identificar aplicaciones que puedan tener datos cifrados, analizando archivos del sistema y datos del usuario. **Recuperación de Datos:** Utilice herramientas especializadas para recuperar datos cifrados y descifrar ransomware específico. **Detección y eliminación de malware:** Escanee el dispositivo para identificar y eliminar el malware existente utilizando herramientas avanzadas de detección de malware. **Restaurar sistema (opcional):** Si no es posible recuperar datos, restablezca su dispositivo a la configuración de fábrica para eliminar todos los rastros de malware.
Caso 2: Extorsión mediante Aplicaciones de Mensajería	Un usuario recibió mensajes amenazantes en aplicaciones de mensajería como WhatsApp, en los que los atacantes demandaban un	**Adquisición de Datos:** realice la adquisición lógica y física de datos del dispositivo, incluidos los mensajes de WhatsApp y otras aplicaciones de mensajería. **Análisis de mensajes:** revise los mensajes enviados y recibidos por las aplicaciones de mensajería para identificar patrones, remitentes y contenido asociado. Extraiga

Caso	Contexto	Recomendaciones
	pago para no divulgar información privada.	metadatos de mensajes para identificar la hora, la ubicación y otros datos contextuales. **Identificación de remitentes**: analice los contactos y las listas de amigos en las aplicaciones de mensajería para identificar posibles extorsionadores. Use herramientas de análisis de redes sociales y contactos para establecer conexiones entre las partes. **Análisis de archivos adjuntos:** extraiga y analice los archivos adjuntos enviados y recibidos en busca de información adicional o indicios de malware.
Caso 3: Extorsión mediante Acceso No Autorizado a la Cámara y Micrófono	Un usuario fue extorsionado con videos e imágenes comprometedoras capturadas sin su conocimiento utilizando la cámara y el micrófono del dispositivo Android.	**Adquisición de Datos:** Realice recolección lógica y física de datos del dispositivo, incluidos mensajes de WhatsApp y otras aplicaciones de mensajería. **Análisis de mensajes:** Revise mensajes enviados y recibidos para identificar patrones, remitentes y contenido relevante. Extraiga sus metadatos y determinar hora, ubicación y otros datos contextuales. **Identificación del remitente:** Analice los contactos y listas de amigos de la aplicación de mensajería para identificar posibles extorsionadores. Use herramientas de análisis de redes sociales y contactos y establecer conexiones entre el extorsionador y la víctima. **Análisis de archivos adjuntos:** Extraiga y analice todos los archivos adjuntos enviados y recibidos para obtener información adicional y signos de malware.
Caso 4: Extorsión mediante Interceptación	Un usuario reportó que su dispositivo Android estaba interceptando mensajes de texto	**Análisis de mensajes:** Extraiga los mensajes de texto del dispositivo y analice patrones de interceptación. **Análisis de aplicaciones de SMS:** Revise las aplicaciones de SMS instaladas y sus

Caso	Contexto	Recomendaciones
de Mensajes de texto	y que los atacantes estaban utilizando esta información para extorsionarlo.	permisos para identificar aplicaciones sospechosas que puedan estar interceptando y reenviando mensajes. **Monitoreo de red:** Analice el tráfico de red del dispositivo para identificar comunicaciones no autorizadas que podrían enviar mensajes interceptados a un atacante. **Verifique su configuración de seguridad:** Asegúrese de que su dispositivo tenga la configuración de seguridad adecuada, como la autenticación de dos factores y cifrado de datos.

Tomando como referente estas recomendaciones, se puede tener una visión más clara de las posibles acciones a seguir para realizar un análisis forense de dispositivos móviles Android de manera adecuada, asegurando la integridad de la evidencia y proporcionando apoyo crucial en casos de ciberextorsión; cabe destacar que cada caso pudiese tener sus particularidades propias en cada una de las etapas del análisis forense.

Discusión

Los datos presentados indican un aumento de casos de ciberextorsión en América Latina y el Ecuador, lo que destaca la necesidad de desarrollar un procedimiento adecuado de análisis forense para dispositivos móviles. Demostrando la importancia de implementar la norma ISO/IEC 27037:2012 para garantizar la integridad de la evidencia digital y admisibilidad en procedimientos legales. Este resultado es consistente con estudios previos que destacan la importancia de los estándares internacionales en informática forense, como se muestra en Menahil et al., (2021) y Tamma et al., (2018).

Los resultados obtenidos disponen de una clara correspondencia con los estudios de Menahil et al., (2021) y Barbosa et al., (2021), en los cuales se indica que existe la necesidad de disponer de normas estandarizadas para la preservación de la evidencia digital; así como también se observa una coherencia significativa con el trabajo de Murudumbay (2022), quien enfatizó en la importancia de contar con metodologías y herramientas específicas para la recolección de evidencia. En adición, en investigaciones como las de Angel et al., (2023) y Neth et al., (2023) resaltan la importancia de contar con herramientas especializadas para el análisis forense de dispositivos móviles; de manera similar Manrique (2019) enfatiza en la necesidad de un enfoque sistemático y la actualización continua de dichas herramientas, debido a la rápida evolución de las tecnologías y las tácticas de ciberataque.

Por otro lado, se menciona que durante el desarrollo de la presente investigación se presentaron limitaciones como, por ejemplo: la dependencia de herramientas forenses que pueden no estar actualizadas con las versiones más recientes del sistema operativo Android y que el enfoque en la norma ISO/IEC 27037:2012 podría no abarcar todas las técnicas de ciberextorsión existentes, en especial aquellas nuevas y no contempladas en la norma.

A continuación, se señala los resultados más importantes por orden de prioridad:

- Contar con un procedimiento de análisis forense de dispositivos móviles Android, basado en la norma ISO 27037:2012, enriquecido con técnicas y recomendaciones aplicables.
- Brindar un acercamiento a las herramientas forenses específicas para Android, que han demostrado ser adecuadas para extraer y analizar los datos críticos.
- Disponer de recomendaciones procedimentales, dirigidas al apoyo positivo en los procesos investigativos de casos de ciberextorsión, y que estén alineadas a las normas legales vigentes en el Ecuador.

Cabe destacar que los resultados obtenidos corroboran la hipótesis planteada, y que sería un aporte vital para las investigaciones de casos de ciberextorsión en dispositivos Android. Este hallazgo está alineado con las conclusiones de investigaciones anteriores como las de Murudumbay (2022), Menahil et al., (2021) y Tamma et al., (2018), que enfatizan en la necesidad de enfoques sistemáticos en la informática forense. La implementación de la norma ISO/IEC 27037:2012 asegura que la evidencia digital sea manejada correctamente, lo cual es crucial para su uso en procedimientos legales (Barbosa et al., 2021).

Es importante continuar investigando y desarrollando nuevas técnicas y herramientas forenses que se adapten a las tácticas de ciberextorsión en constante evolución. También se recomienda la formación continua de los profesionales de la informática forense para garantizar la correcta implementación le procedimiento planteado.

Además, se propone tener en cuenta, para futuras investigaciones, lo siguiente:

- Evaluar la aplicabilidad del procedimiento de análisis forense definido en dispositivos con diferentes sistemas operativos.
- Continuar actualizando los procedimientos de análisis forense para incluir nuevas técnicas y herramientas que aborden amenazas emergentes.
- Fomentar la capacitación continua de los profesionales en informática forense y en la gestión de recursos necesarios.
- Realizar estudios comparativos entre diferentes normas y procedimientos para identificar las mejores prácticas y mejorar continuamente los procesos forenses.

Conclusiones

Con base a los datos recopilados, se muestran un aumento de los casos de ciberextorsión en América Latina, especialmente en Ecuador. Este fenómeno pone de relieve la necesidad de contar con métodos modernos y adecuados para contribuir a la investigación de estos delitos. Además, este estudio confirma la importancia del establecimiento de un procedimiento de análisis forense basado en el estándar ISO/IEC 27037:2012; este estándar proporciona una base sólida para identificar, recopilar, recuperar y preservar evidencia digital, asegurando su integridad y admisibilidad en procedimientos legales; y que éste esté alineado a las regulaciones legales del Ecuador con respecto a la ciberextorsión.

Se destaca el uso de herramientas específicas para análisis forense en dispositivos Android, que facilitan la investigación de casos, al permitir la extracción y el análisis detallado de datos críticos como mensajes de texto, registros de llamadas y aplicaciones.

Se identifica los desafíos relacionados con el análisis forense de dispositivos móviles Android, incluyendo la diversidad de dispositivos y versiones de sistemas operativos, una sólida protección de datos y la inestabilidad de la información.

En conclusión, la investigación realizada no solo destaca la necesidad de desarrollar un procedimiento de análisis forense en dispositivos Android, sino que también refuerza la relevancia de las normas internacionales y su aplicabilidad para la mejora continua de los procedimientos forenses y la formación continua de profesionales; direccionados al apoyo significativo en las investigaciones de casos de ciberextorsión.

Referencias bibliográficas

Angel, M., Tutor, J., Barrena, T., & Martín, A. (2023). Análisis forense de la huella digital de un usuario en sistemas informáticos. https://riunet.upv.es/handle/10251/198592

Barbosa, E. L., Posso, J. H., & Cruz, N. A. (2021). CONDICIONES DE ADMISIBILIDAD DE LA PRUEBA TECNOLÓGICA EN LOS PROCESOS DE CIBERDELITOS. https://repository.ucc.edu.co/server/api/core/bitstreams/44c86841-1b7a-4556-9c8e-e9ff62958057/content

Código Orgánico Integral Penal (COIP) (2014). https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Corredera, P. A. (2023, octubre 28). Qué es el análisis forense digital: Historia, Proceso, Tipos, Desafíos - CIBERNINJAS. https://ciberninjas.com/hacking-analisis-forense/

El Universo. (2024, mayo 3). Ecuador es el tercer país con las mayores amenazas cibernéticas en América Latina, según Check Point | Ecuador | Noticias | El Universo.

https://www.eluniverso.com/noticias/ecuador/ecuador-enfrenta-un-creciente-riesgo-de-ciberataques-en-el-2024-nota/

IFSA, I. F. S. A. (2023). MINIMUM REQUIREMENTS FOR DIGITAL AND MULTIMEDIA EVIDENCE (1a ed.).

Interpol. (2019). GLOBAL GUIDELINES FOR DIGITAL FORENSICS LABORATORIES. INTERPOL Global Complex for Innovation. https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

La Hora. (2023a, marzo 9). Extorsión sexual y las nuevas tecnologías en Ecuador – Diario La Hora. https://www.lahora.com.ec/esmeraldas/extorsion-sexual-y-las-nuevas-tecnologias-en-ecuador/

La Hora. (2023b, septiembre 25). Las extorsiones han crecido un 85% este 2023 en Ecuador – Diario La Hora. https://www.lahora.com.ec/pais/las-extorsiones-han-crecido-un-85-este-2023-en-ecuador/#google_vignette

Manrique, C. J. (2019). Análisis de la seguridad de smartphone con sistema android. https://repository.unad.edu.co/handle/10596/31570

Martínez, A. (2016, febrero 23). Herramientas para realizar análisis forenses a dispositivos móviles | INCIBE-CERT | INCIBE. https://www.incibe.es/incibe-cert/blog/herramientas-para-realizar-analisis-forenses-dispositivos-moviles

Menahil, A., Iqbal, W., Iftikhar, M., Shahid, W. Bin, Mansoor, K., & Rubab, S. (2021). Forensic Analysis of Social Networking Applications on an Android Smartphone. https://doi.org/10.1155/2021/5567592

Murudumbay, M. J. (2022). Marco de trabajo y herramientas para el análisis forense en la atención de los delitos informáticos de Cibergrooming bajo los dispositivos móviles Android. Pro Sciences: Revista de Producción, Ciencias e Investigación, 6(43), 280–296. https://doi.org/10.29018/issn.2588-1000vol6iss43.2022pp280-296

Neth, J., Schuba, M., Brodkorb, K., Neugebauer, G., Hoener, T., & Hack, S. (2023). Digital Forensics Triage App for Android. Proceedings of the 18th International Conference on Availability, Reliability and Security, 1–6. https://doi.org/10.1145/3600160.3605017

Niubox. (2021, julio 30). Ley de Protección de datos Personales en Ecuador: Una mirada desde los derechos humanos - Niubox. https://niubox.legal/ley-de-proteccion-de-datos-personales-en-ecuador-una-mirada-desde-los-derechos-humanos/

Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). PARLAMENTO EUROPEO Y DEL CONSEJO . https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:02016R0679-20160504

Pozo, C., Torres, H., Guamán, R., Alvarez, F., & Narvaez, C. (2020). Methodologies and Forensic Analysis Tools on Android Mobile Devices: A Systematic Literature Review. 2020 15th Iberian

Conference on Information Systems and Technologies (CISTI), 2020-June, 1–7. https://doi.org/10.23919/CISTI49556.2020.9140852

Primicias. (2023, junio 27). Ecuador: cada vez hay más víctimas de extorsiones “clásicas” y virtuales. https://www.primicias.ec/noticias/en-exclusiva/ecuador-extorsiones-denuncias-virtual-siciliana/

Rivera, C. (2023, agosto 24). Un estudio proyecta a 2023 como el año con más casos de ataques cibernéticos en Latinoamérica - El Diario. https://eldiario.com/2023/08/24/estudio-2023-ano-con-mas-casos-de-ataques-ciberneticos-latinoamerica/

Tamma, R., Skulkin, O., Mahalik, H., & Bommisetty, S. (2018). Practical Mobile Forensics Third Edition A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms. www.packtpub.com

Vera, G. (2022, abril 3). Ciberataques: América Latina, muy vulnerable por indiferencia de gobiernos - Novedades Tecnología - Tecnología - ELTIEMPO.COM. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataques-america-latina-muy-vulnerable-por-indiferencia-de-gobiernos-662478

Zambrano, M. A. (2022). El informe criminológico forense en los delitos informáticos [Bachelor’s thesis, Universidad Internacional del Ecuador]. https://repositorio.uide.edu.ec/handle/37000/5246

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento:

N/A

Nota:

El artículo no es producto de una publicación anterior.