UIDE
Powered by
Arizona State University

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Tesis previa a la obtención de título de
Ingeniero en Tecnologías de la
Información.

AUTOR: Jefferson Fernando Ramírez Lozada.

TUTOR: Mgtr. Milton Ricardo.

"Elaborar una guía con las mejores prácticas entre estándares, herramientas y procedimientos para investigación forense orientada a incidentes."

Loja – Ecuador
Septiembre – 2025

CERTIFICACIÓN DE AUTORÍA

Yo, Jefferson Fernando Ramírez Lozada, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedo mis derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, Reglamento y Leyes**.**

FIRMA AUTOR

APROBACIÓN DEL TUTOR

Yo, Milton Ricardo Palacios Morocho, certifico que conozco al autor del presente trabajo de titulación “Elaborar una guía con las mejores prácticas entre estándares, herramientas y procedimientos para investigación forense orientado a incidentes informáticos”, Jefferson Fernando Ramírez Lozada, siendo el responsable exclusivo tanto de su originalidad y autenticidad, como de su contenido.

……

Mgtr. Milton Ricardo Palacios Morocho

DIRECTOR DEL TRABAJO DE TITULACIÓN

DEDICATORIA

Este trabajo lo dedico, en primer lugar, a mis padres. A mi padre Matías, quien fue el pilar de mi formación personal y profesional. De él aprendí la disciplina, la responsabilidad y el deseo constante de superación. Aunque ya no me acompaña físicamente, su ejemplo y enseñanzas permanecen vivos y me inspiran a seguir adelante. A mi madre Beatriz, por su apoyo incondicional, su cariño y por ser la fuerza que me sostuvo en cada etapa de este proceso. Su paciencia y comprensión han sido fundamentales para alcanzar esta meta.

A mis hermanas (Mónica, Lorena y Maritza), quienes de una u otra manera han contribuido en mi vida, compartiendo experiencias, confianza y motivación. Su compañía y respaldo me han dado impulso para seguir persiguiendo mis objetivos.

A mi sobrina Melina, porque con su ternura y alegría ha sido un motor invaluable que me motivó a continuar incluso en los momentos más difíciles.

A mi novia, por acompañarme en este camino, por su apoyo constante, su comprensión y por alentarme a crecer tanto en lo personal como en lo profesional.

Finalmente, a mis maestros, les dedico este trabajo como muestra de gratitud y respeto. Su orientación, paciencia y dedicación en la enseñanza marcaron de manera significativa mi formación académica y profesional.

AGRADECIMIENTOS

Quiero manifestar mi sincero agradecimiento a la Universidad Internacional del Ecuador, pues esta casa de estudios me dio la gran ocasión de instruirme y crecer en el ámbito profesional. Su contribución resultó esencial en la edificación de mi saber y para llevar a buen término este proyecto de titulación.

A mis estimados profesores, que con entrega, paciencia y gran empeño compartieron su sabiduría y vivencias, siendo una guía esencial durante todo mi trayecto universitario. Cada uno de ellos ha dejado una marca imborrable en mi vida, tanto en lo profesional como en lo personal.

De manera particular, agradezco profundamente al Mgtr. Milton Palacios, mi director de tesis, por su guía, su apoyo incondicional y sus valiosas sugerencias, que fueron de gran ayuda para el desarrollo y la finalización de este trabajo de investigación.

Su dedicación y acompañamiento fueron cruciales en todo el proceso. También, hago extensivo mi agradecimiento a la Mgtr. Lorena Conde Zhingre, directora de la carrera, por su liderazgo, su respaldo y la confianza que depositó en mí a lo largo de mi trayectoria académica. Su gestión y motivación fueron fundamentales para poder alcanzar esta importante meta.

Por último, doy las gracias a todos aquellos que, de algún modo u otro, fueron parte de esta etapa tan trascendente, brindando su apoyo y confianza para que hoy este gran esfuerzo pueda verse concretado.

ÍNDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

El acelerado crecimiento de la computación en la nube ha transformado la forma en que las organizaciones almacenan y procesan información. Se estima que para 2025 más de la mitad del gasto empresarial en La presente investigación tiene como objetivo desarrollar una guía metodológica para la investigación forense de incidentes informáticos en entornos de computación en la nube, integrando estándares internacionales, herramientas especializadas y procedimientos aplicables al contexto ecuatoriano. La guía se fundamenta en normas como ISO/IEC 27037:2012, ISO/IEC 27042:2015, NIST SP 800-86 y RFC 3227, y se articula con el marco legal nacional vigente, especialmente el Código Orgánico Integral Penal (COIP) y la Ley Orgánica de Protección de Datos Personales (LOPDP).

El trabajo se desarrolló mediante una metodología de investigación aplicada, combinando revisión bibliográfica y validación práctica a través de casos simulados en Amazon Web Services (IaaS) y Microsoft 365 (SaaS). En ambos escenarios se documentó la adquisición de evidencias digitales, el cálculo de hashes para garantizar integridad, el uso de herramientas forenses (Magnet AXIOM, FTK Imager, Autopsy, entre otras) y la aplicación de plantillas de cadena de custodia e informes periciales.

Los resultados demuestran que la guía propuesta facilita la estandarización de procesos forenses en la nube, asegura la trazabilidad de la evidencia y fortalece la validez jurídica de los hallazgos. Se concluye que su aplicación permite mejorar la respuesta ante incidentes informáticos, aportando una herramienta práctica para peritos forenses, fiscales y profesionales de seguridad digital en Ecuador.

Palabras clave: Informática forense, nube, ISO/IEC 27037, NIST SP 800-86, incidentes informáticos, cadena de custodia, Amazon Web Services, Microsoft 365.

ABSTRACT

This research aims to develop a methodological guide for forensic investigation of cloud-based cybersecurity incidents, integrating international standards, specialized tools, and procedures tailored to the Ecuadorian legal context. The guide is based on ISO/IEC 27037:2012, ISO/IEC 27042:2015, NIST SP 800-86, and RFC 3227, and aligned with national regulations, including the Organic Comprehensive Criminal Code (COIP) and the Organic Law on Personal Data Protection (LOPDP).

The study followed an applied research methodology, combining literature review with practical validation through simulated case studies in Amazon Web Services (IaaS) and Microsoft 365 (SaaS). Both scenarios documented evidence acquisition, hash calculation to ensure data integrity, the use of forensic tools (Magnet AXIOM, FTK Imager, Autopsy, among others), and the application of standardized templates for chain of custody and expert reports.

The results demonstrate that the proposed guide standardizes cloud forensic processes, ensures evidence traceability, and strengthens the legal admissibility of findings. It is concluded that its application enhances the response to cloud-related cybersecurity incidents, providing a practical tool for forensic experts, prosecutors, and cybersecurity professionals in Ecuador.

Keywords: Digital forensics, cloud, ISO/IEC 27037, NIST SP 800-86, cybersecurity incidents, chain of custody, Amazon Web Services, Microsoft 365.

INTRODUCCIÓN

El acelerado crecimiento de la computación en la nube ha transformado la forma en que las organizaciones almacenan y procesan información. Se estima que para 2025 más de la mitad del gasto empresarial en software e infraestructura se habrá trasladado a servicios cloud. Este auge de plataformas como AWS, Microsoft Azure o Google Cloud ofrece grandes ventajas en escalabilidad y flexibilidad; sin embargo, también implica nuevos retos en materia de seguridad informática. En particular, cuando ocurren incidentes informáticos en la nube (como accesos no autorizados, filtraciones de datos o ataques cibernéticos), surge la necesidad de llevar a cabo investigaciones forenses digitales adaptadas a este entorno. Garantizar la integridad y disponibilidad de los datos en la nube requiere la aplicación rigurosa de análisis forense, tanto para comprender lo sucedido como para preservar evidencia con fines legales (Patau, 2023).

La informática forense en la nube se puede entender como la aplicación de los principios y técnicas de la investigación digital forense en entornos de computación distribuida. Si bien comparte los objetivos del forense tradicional (identificar, recolectar, analizar y preservar evidencia digital), su enfoque y métodos deben adaptarse a las características únicas del entorno cloud. A diferencia del análisis forense clásico, donde los especialistas suelen tener acceso físico directo a los dispositivos comprometidos, en la nube los datos residen en infraestructuras de terceros (proveedores de servicios cloud) a las que el investigador no puede acceder físicamente. Esto introduce desafíos adicionales: por ejemplo, la información puede estar replicada en múltiples ubicaciones geográficas, compartida entre varios clientes (multitenencia) y sujeta a políticas de retención propias de cada proveedor. Además, muchos datos en la nube son altamente volátiles (logs en memoria, máquinas virtuales efímeras), lo que demanda acciones rápidas y específicas

para su adquisición antes de que se pierdan. En suma, el análisis forense en entornos cloud requiere técnicas especializadas y buenas prácticas para enfrentar la naturaleza dinámica, distribuida y virtualizada de estos sistemas. La presente guía se propone precisamente abordar esta necesidad, compilando las mejores prácticas basadas en estándares internacionales, herramientas especializadas y procedimientos comprobados para llevar a cabo investigaciones forenses de incidentes informáticos en la nube de forma eficaz y confiable (Báez, 2025).

CONTEXTO Y JUSTIFICACIÓN

En la última década, las organizaciones han migrado masivamente sus activos digitales a la nube, atraídas por ventajas operativas y económicas. Junto con esta migración, también han aumentado los incidentes de ciberseguridad en entornos cloud, desde brechas de datos hasta ataques a infraestructuras críticas. La informática forense juega un rol crucial en este contexto: permite investigar incidentes, identificar a los responsables y extraer aprendizajes para mejorar la seguridad. En entornos corporativos, una respuesta forense eficaz no solo ayuda a esclarecer lo ocurrido, sino que fortalece la confianza en la nube al garantizar que, incluso ante un ataque, es posible preservar la integridad del entorno y de la evidencia digital. Sin embargo, llevar a cabo análisis forenses en la nube presenta complejidades particulares que justifican la elaboración de una guía especializada (Patau, 2023).

En segundo lugar, los entornos cloud son altamente dinámicos y volátiles: recursos que existían al momento de un incidente (como instancias en ejecución, registros en memoria, sesiones activas) pueden desaparecer o alterarse poco después. Esto demanda procedimientos rápidos y ordenados de recolección de datos, siguiendo principios como el orden de volatilidad (priorizar la captura de evidencias volátiles antes de que se desvanezcan).

En tercer lugar, cada proveedor de servicios en la nube maneja políticas y tecnologías distintas – por ejemplo, formatos de registros, mecanismos de auditoría, herramientas de exportación de datos – lo que dificulta la estandarización. De hecho, cada proveedor define sus propias políticas de retención de logs, accesibilidad a datos de clientes y niveles de soporte para investigaciones, generando un escenario heterogéneo (Globatika Lab, 2025).

Diversos organismos internacionales han reconocido estos desafíos emergentes. Por ejemplo, NIST ha categorizado obstáculos técnicos, legales y organizativos para la forensia en la nube, instando a desarrollar estándares y tecnologías que los aborden (Linthicum, 2024).

En la actualidad no existe un estándar único ampliamente adoptado que cubra todas las fases de la forensia en la nube, aunque sí marcos generales de forensia digital. Esta brecha refuerza la justificación del trabajo de titulación: es necesario compilar y adaptar las mejores prácticas de distintos estándares y fuentes, para ofrecer una guía integral orientada a los incidentes en la nube. La guía servirá para que profesionales de seguridad, peritos forenses y administradores de TI cuenten con un referente unificado al enfrentar un incidente cloud, asegurando que la identificación, recolección, análisis y preservación de la evidencia digital se realice de forma válida y confiable (Ehigiator , Idahosa, Asante , & Okungbowa , 2024).

En última instancia, un manejo estandarizado de la evidencia en la nube no solo facilita las investigaciones internas, sino que aumenta las probabilidades de que dicha evidencia sea aceptada en procesos legales y sirva para atribuir responsabilidades o mejorar la seguridad a futuro.

PLANTEAMIENTO DEL PROBLEMA

A pesar del crecimiento de la informática en la nube y de la frecuencia con que ocurren incidentes de seguridad en este entorno, las organizaciones enfrentan hoy un vacío en cuanto a directrices específicas para la realización de investigaciones forenses en la nube. Muchos equipos de respuesta a incidentes aplican metodologías tradicionales de informática forense, diseñadas para entornos locales, que no contemplan plenamente las particularidades del entorno cloud (Ehigiator , Idahosa, Asante , & Okungbowa , 2024).

Esto puede derivar en varios problemas: evidencias digitales cruciales podrían pasar inadvertidas o no ser preservadas a tiempo (por ejemplo, no capturar a tiempo una instancia virtual comprometida que luego es eliminada); los procedimientos de recolección podrían no garantizar la integridad de los datos (por ejemplo, si no se aplican hashes o cadenas de custodia apropiadas en datos extraídos de la nube); o bien podría incurrirse en violaciones legales al no respetar las condiciones de los proveedores cloud o regulaciones de protección de datos internacionales. En resumen, la ausencia de una guía unificada y adaptada a la nube conlleva riesgos de ineficacia investigativa y de invalidez de la evidencia obtenida (Linthicum, 2024).

El problema específico que aborda este trabajo es la falta de un conjunto consolidado de estándares, herramientas y procedimientos adaptados a la forensia en la nube que pueda ser utilizado de forma consistente en la investigación de incidentes informáticos. Si bien existen normas internacionales relevantes (ISO/IEC, NIST, RFC, entre otras) y herramientas especializadas, estas a menudo se aplican de forma aislada o parcial en el contexto cloud. No hay un manual práctico integrado que oriente, paso a paso, desde cómo identificar las fuentes de evidencia en distintos modelos de servicio (IaaS, PaaS, SaaS), pasando por la correcta adquisición de datos volátiles y persistentes, hasta el análisis e interpretación de los hallazgos en un entorno

virtualizado. La carencia de tal guía dificulta que los investigadores menos experimentados en entornos de nube logren resultados consistentes, reproducibles y acordes con las mejores prácticas. Por ejemplo, cada proveedor cloud ofrece diferentes herramientas de auditoría (CloudTrail de AWS, Azure Monitor, etc.); sin lineamientos claros, elegir y usar estas herramientas efectivamente para fines forenses puede ser confuso.

En consecuencia, se plantea la necesidad de desarrollar una guía de buenas prácticas que compile y adapte las recomendaciones de los principales estándares internacionales, a la vez que evalúe las herramientas forenses disponibles y establezca procedimientos operativos claros para entornos cloud. La resolución de este problema permitirá mejorar la eficiencia de la respuesta a incidentes en la nube, minimizar la pérdida de datos críticos durante las investigaciones y asegurar que los resultados obtenidos sean válidos técnicamente y defendibles legalmente (Yepez, 2025).

De esta manera, la guía propuesta contribuirá a cerrar la brecha entre la teoría (normativas y principios) y la práctica (uso de herramientas y técnicas) en el ámbito de la forensia digital en la nube.

OBJETIVOS

OBJETIVO GENERAL

- Desarrollar una guía con las mejores estándares, herramientas y procedimientos para la investigación forense de incidentes informáticos en la nube.

OBJETIVOS ESPECÍFICOS

- Analizar los estándares, herramientas y procedimientos de análisis forense para incidentes informáticos en la nube.
- Comparar las fortalezas y debilidades de los estándares, herramientas y procedimientos para análisis forense.
- Establecer la guía con normas y procedimientos para que garantice su validez y aplicabilidad en casos prácticos.
- Validar la guía documentada a través de máximo tres casos prácticos.

METODOLOGÍA

Para alcanzar los objetivos planteados, se seguirá una metodología de trabajo dividida en dos fases principales: una fase de investigación teórico-práctica, y una fase de desarrollo de la guía como tal.

Fase de Investigación: En esta etapa se realizará una exhaustiva revisión bibliográfica y documental, complementada con pruebas prácticas, con el fin de sentar las bases conceptuales y técnicas de la guía. Las actividades incluyen:

- Recolección de información proveniente de fuentes confiables (artículos científicos, libros, estándares internacionales, normativas legales vigentes y manuales de herramientas tecnológicas) relacionadas con la informática forense en la nube. Esto permitirá construir un marco teórico actualizado sobre mejores prácticas y principios aceptados.
- Identificación de problemas técnicos, legales y éticos asociados a la recolección, análisis y preservación de evidencia digital en entornos de nube. Se prestará especial atención a desafíos como la volatilidad de los datos, la privacidad, la jurisdicción internacional y la cadena de custodia en servicios cloud.
- Uso práctico de herramientas forenses especializadas en entornos cloud, con el objetivo de evaluar su desempeño en la identificación, adquisición y análisis de evidencias. Por ejemplo, se probarán herramientas de captura de máquinas virtuales, análisis de logs de proveedores (AWS, Azure, etc.) y utilidades de preservación de datos volátiles, documentando sus capacidades y limitaciones.
- Simulación de escenarios reales de incidentes informáticos en la nube para validar

la aplicabilidad de las herramientas y procedimientos estudiados. Se recrearán, en un ambiente controlado, incidentes típicos (como una intrusión en una instancia cloud o una filtración de información desde almacenamiento en la nube) y se pondrán en práctica las técnicas forenses para recopilar y analizar la evidencia en cada caso. Estos ejercicios permitirán refinar las recomendaciones de la guía basándose en observaciones empíricas (Linthicum, 2024).

Fase de Desarrollo: Con la información recopilada y analizada en la fase anterior, se procederá al diseño y elaboración de la guía forense. Este diseño estará fuertemente basado en estándares internacionales reconocidos, seleccionados por su relevancia y aplicabilidad a la computación en la nube. En particular, se tomarán como referencias principales las siguientes normas y lineamientos:

- ISO/IEC 27037 – que establece directrices para la identificación, recolección, adquisición y preservación de evidencia digital. Este estándar provee principios para asegurar la autenticidad e integridad de la evidencia desde el momento de su obtención, aspectos fundamentales para que los hallazgos sean admisibles en procesos legales. La guía adaptará las recomendaciones de ISO 27037 al contexto cloud (por ejemplo, cómo identificar y aislar evidencias en entornos virtualizados, uso de *snapshots* para preservar estados de sistemas en nube, etc.).

- ISO/IEC 27042 – que se enfoca en las metodologías para el análisis e interpretación de la evidencia digital. Complementando al anterior, este estándar orienta sobre cómo realizar un análisis forense riguroso y reproducible. La guía incorporará estas metodologías para asegurar que los procedimientos analíticos (como el examen de registros de auditoría cloud, análisis de metadatos en archivos almacenados en la

nube, correlación de eventos, etc.) produzcan resultados fiables y objetivos (Yepez, 2025).

- NIST SP 800-86 – publicación del Instituto Nacional de Estándares y Tecnología (NIST) que provee una “Guía para la Integración de Técnicas Forenses en la Respuesta a Incidentes”. De este documento se extraerán lineamientos pertinentes a entornos distribuidos, asegurando que la guía integre la forensia dentro del ciclo de respuesta a incidentes en la nube. Por ejemplo, se contemplará cómo coordinar con proveedores cloud durante una investigación, cómo documentar y comunicar hallazgos forenses en el contexto de la gestión de incidentes, y cómo las técnicas forenses pueden apoyar la mitigación temprana de amenazas en entornos cloud.
- RFC 3227 – que establece pautas para la recolección y resguardo de evidencia volátil, introduciendo el concepto de "orden de volatilidad". La guía incorporará este principio para priorizar la captura de datos en la nube según su volatilidad (p.ej., primero memoria y procesos en ejecución de una máquina virtual comprometida, luego discos virtuales y, finalmente logs persistentes), minimizando la pérdida de información crítica. Asimismo, se adoptarán las recomendaciones del RFC en cuanto a documentación de cada paso de adquisición y preservación de evidencias, reforzando la cadena de custodia (Linthicum, 2024).

Estos estándares y referencias serán la estructura de la guía. En base a ellos, se organizará el contenido en secciones específicas que aborden las etapas clave de una investigación forense en la nube, tales como:

- **Identificación de evidencias en entornos cloud:** Cómo reconocer qué datos y recursos pueden contener evidencia relevante tras un incidente. Incluirá la identificación de fuentes como registros de servicios cloud (eventos de acceso, logs de aplicaciones SaaS, métricas de máquinas virtuales), snapshots de sistemas virtualizados, copias de seguridad en la nube, contenido de almacenamientos compartidos, entre otros. Se proporcionarán criterios para determinar la relevancia de cada tipo de evidencia según el caso (p. ej., en IaaS examinar primero registros del hipervisor o tráfico de red virtual, en SaaS enfocarse en logs de aplicación o historiales de administración).

- **Adquisición y preservación de la evidencia digital:** Procedimientos para recolectar datos de la nube sin alterarlos y asegurar su integridad. Se detallará el uso de herramientas y servicios para volcado forense de máquinas virtuales, exportación de registros auditados, clonación de discos virtuales y captura de información volátil (memoria RAM, estados de contenedores, etc.). Se enfatizará el cumplimiento del *orden de volatilidad* recomendado por RFC 3227 – es decir, capturar primero los datos más volátiles – y la aplicación de técnicas de preservación como el cálculo de hashes criptográficos y el uso de medios de solo lectura para almacenar las evidencias. Además, se incluirán lineamientos para mantener una adecuada cadena de custodia en entornos cloud, documentando en todo momento quién, cómo y cuándo se accedió a cada evidencia, incluso cuando esta debe ser obtenida mediante solicitudes al proveedor de servicios (Báez, 2025).

- **Análisis e interpretación de la evidencia:** Métodos para examinar las evidencias recopiladas y extraer conclusiones válidas. Esta sección, guiada por ISO/IEC

27042, abarcará técnicas de análisis forense aplicadas a datos de la nube: revisión de logs de seguridad en busca de patrones de ataque, análisis de imágenes forenses de discos en la nube con software especializado, correlación temporal de eventos entre múltiples fuentes (por ejemplo, relacionar una alerta de seguridad con cambios de configuración en la nube y con conexiones de red sospechosas). Se propondrán herramientas para automatizar parte de este análisis y se describirán buenas prácticas para interpretar los hallazgos evitando sesgos. También se abordará cómo documentar los resultados del análisis de forma clara (informe forense), de modo que puedan ser entendidos por terceros y utilizados como evidencia experta.

- **Consideraciones legales y de cumplimiento:** Dado que las investigaciones en la nube a menudo implican datos que atraviesan fronteras y servicios de terceros, la guía dedicará una sección a resumir las implicaciones legales más relevantes. Se orientará sobre cómo manejar datos personales cumpliendo regulaciones (p. ej., GDPR), cómo coordinar con proveedores cloud respetando sus términos de servicio y procesos formales (por ejemplo, Amazon o Microsoft tienen procedimientos para solicitudes legales de datos), y cómo preparar la evidencia para posibles procedimientos judiciales. Se destacará la importancia de la cooperación internacional cuando la evidencia reside fuera de la jurisdicción local, así como la necesidad de preservar la privacidad de otros clientes en entornos multiarrendatarios durante la recolección de datos.

- **Herramientas y buenas prácticas recomendadas:** A lo largo de la guía se incorporarán las herramientas identificadas en la fase de investigación (tanto de

código abierto como comerciales) que hayan demostrado ser eficaces en entornos cloud. En esta sección final se presentará un resumen de dichas herramientas categorizadas por función (por ejemplo, herramientas de adquisición de imágenes forenses en la nube, utilidades para análisis de registros de AWS/Azure, plataformas SIEM integradas con entornos cloud, etc.), junto con consejos de uso y limitaciones. Asimismo, se listarán mejores prácticas operativas generales para prepararse ante incidentes en la nube, como habilitar logs avanzados, conservar backups periódicos, definir procedimientos de respuesta en contratos con los proveedores, y entrenar al personal en escenarios simulados (Globatika Lab, 2025).

Finalmente, tras la elaboración del borrador de la guía, se llevará a cabo su validación práctica. Esto implica aplicar la guía en uno o más casos de estudio simulados (hasta tres escenarios diferentes, según lo previsto en los objetivos). Cada caso práctico consistirá en recrear un incidente en la nube (por ejemplo, una intrusión en una máquina virtual, un abuso de privilegios en una aplicación SaaS o una exfiltración de datos desde almacenamiento cloud) y seguir paso a paso las recomendaciones de la guía para gestionarlo forensemente. Durante esta validación se evaluará la efectividad y la exhaustividad de la guía: si todas las evidencias relevantes fueron identificadas, si los procedimientos propuestos resultan viables en un entorno realista, si las herramientas sugeridas funcionan adecuadamente y si los resultados obtenidos son consistentes. Cualquier hallazgo o dificultad durante estos ejercicios servirá para refinar y ajustar la guía antes de su versión final. De este modo, nos aseguraremos de que la guía propuesta no solo esté alineada con los estándares teóricos, sino que también sea prácticamente aplicable y útil para responder a incidentes informáticos en la nube en entornos empresariales reales.

En síntesis, mediante esta metodología combinada de investigación documental, experimentación práctica y desarrollo iterativo, se espera construir una guía sólida y confiable. La guía resultante proporcionará un marco de actuación forense claro para entornos cloud, aumentando la capacidad de respuesta ante incidentes de seguridad y contribuyendo a que la evidencia digital en la nube sea manejada con el máximo rigor técnico y legal. Esto representará una valiosa aportación tanto para la comunidad de seguridad informática como para las organizaciones que operan en la nube, fortaleciendo la confianza en la resolución de incidentes y en la administración de justicia digital en la era de la computación en la nube (Báez, 2025).

CAPÍTULO I: ESTADO DEL ARTE

INTRODUCCIÓN

(Sanchez, 2025) concuerda en que, en sus orígenes, la informática forense se limitaba a la extracción de evidencia en discos duros y memorias de sistemas locales. Sin embargo, con la popularización de la computación en la nube a partir de la década de 2000, los data centers trasladaron datos y operaciones a infraestructuras virtualizadas administradas por terceros, lo cual implicó que la evidencia quedara fuera del control físico del investigador. Varios estudios recientes están de acuerdo en que este último evento dificulta varios métodos tradicionales de adquisición, debido a que muchos artefactos tienen una existencia corta y se replican entre centros de datos. La respuesta a esta problemática fue la forense en la nube, que reinterpreta las fases clásicas de identificación, recolección, preservación y análisis bajo los modelos IaaS, PaaS y SaaS.

La complejidad de estos entornos radica en la multitenencia, la dispersión geográfica de los datos y la volatilidad de los recursos dinámicos, factores que comprometen la cadena de custodia. Así, (Burgos, Cruzado, & Seclen), sobre la base de dos estudios publicados entre 2016 y 2022, ya afirma que “más del 60 % de los artículos analizados ponen de manifiesto disparidades metodológicas a la hora de incluir la evidencia alojada en la nube al diccionario de infraestructuras”. Mientras tanto, desde el punto de vista normativo, Chiun y Enrique confirman que “a partir de la adopción estricta de la ISO/IEC 27037:2012, los tiempos de análisis han caído significativamente, y la tasa de casos resueltos aumentó en las unidades de hardware”. Sin embargo, (Chiun & Enrique, 2024) presenta una objeción al señalar que “no existen protocolos unificados que garanticen la admisibilidad de la evidencia en la nube, ya que, desde la adquisición, la dependencia de las API de los proveedores sigue creciendo”.

Las propuestas más recientes avanzan hacia la “forensic readiness”, es decir, la preparación previa de infraestructuras multicloud para facilitar la respuesta a incidentes (Burgos, Cruzado, & Seclen). (Vaca & Dulce-Villarreal, 2024) apuntan que, si la blockchain se añade a la propia cadena de custodia, se puede registrar cada operación a través de hashes inmutables y reforzar la mencionada trazabilidad probatoria. Con estos mecanismos y varias plantillas operativas, además de herramientas como Magnet AXIOM Cloud o Timesketch, se pretende obtener informes que sean a la vez técnicamente precisos y abogables. En consecuencia, la literatura que ha convergido en la lengua española permite que se redacte una guía de buenas prácticas que defina un conjunto de estándares, herramientas y procedimientos (Vera & Adrián, 2024).

FUNDAMENTOS TEORICOS

1.1 Análisis forense en la nube

(Pita Vera, 2024) define el análisis forense en la nube como una especialización dentro de la informática forense centrada en la identificación, recolección, preservación y análisis de la evidencia digital que reside en los entornos de computación en la nube. Dado que el estándar enfoque de la informática forense se centra en dispositivos físicos, las peculiaridades de los servicios en la nube, como la virtualización y la distribución, requieren otro enfoque. (Echeverría Espinoza, 2024) afirma que, a saber, el análisis forense en la nube se trata sobre la "nube" y los desafíos únicos que representan. En el contexto del Ecuador, esta disciplina emergente aborda la serie de los siguientes desafíos clave.

La falta de acceso físico directo a los servidores donde se almacenan los datos es uno de los desafíos más significativos. En la nube, la información puede estar en servidores en diferentes partes del mundo, y desde la perspectiva de los investigadores forenses ecuatorianos, debe volverse inaccesible en términos de acceso físico directo (Orna Lora, 2024). Esto es opuesto a las oportunidades que tenían los expertos forenses y los gestores de bases de datos en el pasado. Además, un aspecto crucial a tener en cuenta es la naturaleza elástica y volátil de los propios datos. Significa que un recurso puede crearse o destruirse, que los recursos son dinámicos y, por lo tanto, la evidencia existe o no existe. Por lo tanto, la migración constante y el movimiento de datos entre servidores también juega un papel importante en dificultar el acceso a la evidencia (Vera & Adrián, 2024).

El entorno de multitenencia, en el que varios usuarios comparten la misma infraestructura física producida sobre la nube, está diseñado para aumentar los casos de un incidente en particular en el que el valor de evidencia debe ser aislado sin comprometer la privacidad de otros usuarios que comparten el mismo espacio (Echeverría Espinoza, 2024). Para abordar este problema, se hace necesario aplicar funcionalidades especializadas de una técnica forense que se asegure de que los mismos datos mantengan su integridad y confidencialidad durante todo el proceso de investigación. Un componente que no puede pasarse por alto es la colaboración de los proveedores en la nube. La capacidad de recopilar evidencia compromete al proveedor, quien controla la infraestructura subyacente, y los registros de auditoría deben coordinarse y programarse en un contrato específico y necesitar instrumentos de comunicación eficientes para permitir el acceso a la evidencia necesaria de un caso de estudio en particular (Orna Lora, 2024).

Además, en el caso de Ecuador, los problemas adicionales se refieren a la privacidad y la seguridad de los datos almacenados en la nube. Dado que los servicios de nube no incluyen el cifrado de extremo a extremo, al igual que la nube iCloud, existe una mayor posibilidad de que los desconocidos puedan acceder a la información del usuario (Pita Vera, 2024). Además, según Pita Vera, cumplir con un requisito adicional, la necesidad de contar con una conexión a Internet para acceder a los servicios y analizar los datos, también plantea problemas adicionales en términos de vulnerabilidades de seguridad. Finalmente, (Orna Lora, 2024) sugiere que el marco legal, en general, puede resultar insuficiente, lo que subraya aún más la necesidad de abordar los problemas existentes.

1.2 Evidencia digital y tipos de evidencia en la nube

1.2.1 Evidencia digital

La definición de evidencia digital establece que es cualquier información de valor probatorio existente almacenada o transmitida en formato electrónico (Gallegos Yánez & Andrade Ulloa, 2025). Si bien, en el marco legal del país, Ecuador reconoce a la evidencia digital como prueba en un procedimiento de juicio. Ahora bien, en el panorama de la nube, la evidencia digital posee ciertas particularidades. Por un lado, su ubicuidad inherente significa que puede existir en varias ubicaciones físicas y virtuales. Naturalmente, esto hace que la evidencia sea significativamente más difícil de identificar y recopilar en el futuro. Por otro lado, la idea de que la evidencia puede modificarse o eliminarse, en un período de tiempo relativamente corto es inherente a la nube. Los investigadores de ciberseguridad y digitales deben actuar de manera rápida y efectiva en colaboración cercana (Orna Lora, 2024).

1.2.2 Tipos de evidencia digital en la nube

En las configuraciones de la nube, se presentan varios tipos de evidencia digital relevantes para el entorno forense. Los registros de auditoría son útiles, ya que muestran todas las tareas ejecutadas en los sistemas, lo que ayuda a los investigadores a elaborar las secuencias de los eventos ocurridos con el sistema. Asimismo, las imágenes de las máquinas virtuales son adecuadas, ya que capturan todo lo que estaba en el sistema durante el período de tiempo seleccionado (Orna Lora, 2024).

Otro tipo de evidencia crucial son las configuraciones y políticas de seguridad. Pueden presentarse como un elemento crucial que ayudará a comprender las vulnerabilidades de un sistema que los atacantes explotaron. Está claro que Pita Vera se refería a información sobre cómo sucedió la violación de seguridad cuando expuso el siguiente punto (Vera & Adrián, 2024).

Asimismo, los datos de aplicaciones y servicios en la nube, que abarcan información producida por las aplicaciones ejecutadas en la nube, como bases de datos, archivos de configuración y registros de interacciones de días, también pueden resultar de gran utilidad para la comprensión de la ciberdelincuencia (Orna Lora, 2024). Otros tipos de evidencia digital en la nube pueden consistir en correos, archivos almacenados, registros de acceso y actividad del usuario, así como información sobre la infraestructura y configuración de los servicios de nube utilizados (Vera & Adrián, 2024).

1.3 Delito informático en el contexto ecuatoriano

En Ecuador, amplias gamas de delitos informáticos entran en jurisdicción del Código Orgánico Integral Penal. Los delitos van desde el acceso no autorizado a los sistemas y la interceptación de datos hasta el sabotaje (Suárez Liriano & Rocafuerte Del Pezo, 2024). A los efectos del Código, se entiende por delito informático cualquier hecho punible en el que, como medio o como objeto, se utilice una computadora, se obtenga o defienda un beneficio para el responsable y se cause un daño a las personas. La creciente dependencia y adhesión a los sistemas de tecnología de la información y comunicación (TIC), ha generado un espectacular aumento de este tipo de delitos en el país.

Ante dicho escenario, las autoridades de Ecuador han implementado diversas medidas para incrementar su capacidad de investigación y castigo de los delitos cibernéticos. Estas incluyen la instauración de divisiones especiales dentro de la policía federal y fiscalía, así como la adquisición de herramientas tecnológicas avanzadas para la detección y extracción de pruebas digitales. Entre los delitos cibernéticos más comunes en el país, se hallan el hurto de identidad, el fraude electrónico y el acceso no autorizado a sistemas.

El marco legal ecuatoriano, basado principalmente en el COIP, describe las sanciones y los procedimientos de juzgamiento de tales delitos. Entre los demás, se encuentra la violación de derechos de privacidad e intimidad (Art. 178); la ilegal divulgación de bases de datos (Art. 229), la interceptación de comunicaciones y datos informáticos (Art. 230), los actos de perjuicio a la integridad de sistemas informáticos (Art. 232) y el costo de reparación para restaurar su funcionalidad (Art. 234); el acceso sin autorización a sistemas; y los tipos incluidos de defraudación, entre otros delitos (Art. 186, Art. 234.1). (Suárez Liriano & Rocafuerte Del Pezo, 2024).

Las estadísticas recientes muestran que la amenaza de delitos informáticos en el país está aumentando. En 2023, “los ciberataques también superaron el 30 por ciento en la República de Ecuador” (Universo, 2024). Desde 2020, la policía ha recibido varias denuncias sobre delincuentes informáticos, y los dos más comunes eran “robo de identidad criminal y fraude”. Por lo tanto, se trata de modificaciones de leyes y capacidades de investigación adecuadas para combatir la inseguridad cibernética en rápido cambio, que son necesarias en el caso ecuatoriano (Comercio, 2025).

1.4 Perito forense

Hay un número de roles especializados en el ámbito del análisis forense digital, cada uno con tareas específicas para hacer en el proceso investigativo. El principal rol, sin embargo, es el perito forense informático. Un profesional activamente implicado en la investigación de los incidentes de seguridad en los cuales los sistemas de TI están involucrados y la evidencia digital está disponible. Sus tareas principales implican identificar, recolectar, preservar, analizar y presentar evidencia digital de tal forma que su evidencia sea admitida en el sistema judicial. En

Ecuador, la criminalidad activa ha llevado a un auge en la necesidad de peritos informáticos, quienes son necesarios en el análisis técnico basándose en la evidencia para presentar un caso (Orna Lora, 2024).

Los peritos forenses en Ecuador realizan sus actividades tomando en cuenta las metodologías y estándares internacionales. Por ejemplo, podría ser la norma ISO 27037, que es un conjunto de líneas directrices para identificar, recoger, adquirir y preservar la prueba digital. Orna Lora explica que la capacitación, certificación y acreditación de los peritos forenses son críticos, puesto que el reconocimiento de la informática forense se basa en el profesionalismo de los expertos. La acreditación de los peritos forenses en Ecuador la lleva a cabo el Consejo de la Judicatura, la máxima autoridad judicial en la nación iberoamericana y comprobación de que los peritos forenses poseen los conocimientos y experiencia necesarios (Orna Lora, 2024).

1.5 Privacidad y jurisdicción

La privacidad y la jurisdicción son elementos críticos en el terreno de la ciencia forense de la nube, sobre todo en un caso de la realidad ecuatoriana dada la naturaleza transnacional de los servicios de computación en línea. La legislación ecuatoriana de mayor importancia en el tema del uso indebido de datos es la Ley Orgánica de Protección de Datos Personales. (Barahona Robayo & Mayorga Mayorga, 2024) indican que esta ley define los marcos jurídicos en el país para proteger los datos personales de los ciudadanos. Según la Ley Orgánica de Protección de Datos, cada persona tiene el control total de sus datos personales. No puede ser obviado este hecho sin el consentimiento de su propietario. Además, los piratas informáticos responsables de los delitos de violación de datos son apreciados y condenados de diversas maneras. En mi opinión, en el contexto ecuatoriano, la privatización de la infracción en datos se condena de manera efectiva debido a la pantalla del derecho (Orna Lora, 2024).

No obstante, el ámbito global de los servicios en la nube crea desafíos significativos en términos de jurisdicción y aplicación de las leyes de privacidad. Por ejemplo, los datos de un usuario ecuatoriano pueden almacenarse en servidores en un país diferente, y puede resultar en incertidumbre sobre las leyes aplicables y las agencias con jurisdicción relevante en caso de investigación forense. La transferencia internacional de datos y la necesidad de cooperación entre jurisdicciones son elementos cruciales que deben abordarse en investigaciones de delitos informáticos en la nube (Orna Lora, 2024).

1.6 Cadena de custodia y autenticidad de la evidencia

(Gallegos Yánez & Andrade Ulloa, 2025) define la cadena de custodia como el proceso documentado que garantiza la integridad y la autenticidad de la evidencia digital desde el momento de su recolección hasta que se presenta en un proceso legal. La cadena de custodia es el proceso que se practica para garantizar que la evidencia no se ha alterado y se considerará admisible en el tribunal Gallegos Yánez & Andrade Ulloa, 2025. Dado lo fácil que es manipular y falsificar evidencia digital, es especialmente importante mantener una cadena de custodia sólida en este caso. Cualquier error en la cadena de custodia puede socavar la validez de la evidencia y potencialmente afectar el juicio.

En Ecuador, el Código Orgánico Integral Penal, COIP, exige específicamente la cadena de custodia de la evidencia física y la evidencia digital relevante para un caso (Suárez Liriano & Rocafuerte Del Pezo, 2024). Por lo tanto, se presume que se debe documentar con detalle cada uno de los pasos en el manejo de la evidencia, desde su recolección, embalaje, etiquetado, transporte, almacenamiento y análisis (Orna Lora, 2024). Además, hay maneras tecnológicas de verificar que los datos no han sido manipulados desde su recolección, a saber, funciones hash y firmas digitales.

Dentro del ámbito de la nube, la cadena de custodia tiene problemas especiales a causa del carácter disperso de los datos y la posibilidad de modificaciones que no dejan rastros evidentes. A pesar de estos desafíos, hay mundiales como la norma ISO 27037, que proporcionan orientaciones para establecer y mantener la cadena de custodia de la evidencia digital en diferentes contextos, incluso en la nube (Orna Lora, 2024) Al mismo tiempo, en Ecuador se ha detectado falta de coherencia en la preservación de la evidencia digital y la necesidad de actualizar los manuales operativos y mejorar la formación del personal encargado de su tratamiento, a fin de garantizar la aplicación correcta de los protocolos de la cadena de custodia en todo el país (Gallegos Yánez & Andrade Ulloa, 2025).

1.7 Normas y estándares para el análisis forense digital en la nube

1.7.1 ISO/IEC 27037:2012

Título: Directrices para la identificación, recolección, adquisición y preservación de evidencia digital.

Organismos: Organización Internacional de Normalización (ISO) y Comisión Electrotécnica Internacional (IEC).

1.7.1.1 Alcance y objetivo

El ISO/IEC 27037:2012 es un estándar que establece pautas sobre la búsqueda, identificación y adquisición de evidencia digital y todo sin comprometer su autenticidad e integridad (ISO, 2012).

Objetivo principal: Garantizar la validez legal de la evidencia obtenida en cualquier entorno digital.

Aplicabilidad en la nube: Es importante ya que este tipo de procedimientos será adaptativo para los sistemas distribuidos donde los archivos se almacenan en centros de datos dispersos o en un entorno controlado por parte de organizaciones externa.

1.7.1.2 Elementos destacados

A. **Identificación de Evidencia**

- Consiste en decidir qué informaciones son importantes para la investigación. En el ámbito cloud, eso significa trabajar con el proveedor para alcanzar registros y archivos dispersos por numerosos lugares.

B. **Adquisición Forense**

- Utiliza herramientas autorizadas, y genera hashes criptográficos verdaderos (p. ej., SHA-256), para garantizar que la información no sea cambiada una vez que está en su poder.

C. **Preservación**

- Las copias deben ser almacenadas en lugares seguros para evitar el acceso no autorizado o cambio.

D. **Cadena de Custodia**

- Requiere documentar cuidadosamente cada paso del proceso, desde la identificación de las pruebas hasta su presentación en juicio.

1.7.1.3 Relevancia en Ecuador

Falta de acceso físico: Dado que no es posible el acceso físico a esta información, evidencias digitales permiten el descubrimiento electrónico en lugares fuera del control directo del investigador (Asamblea Nacional del Ecuador, 2024).

Regulación local: El marco legal ecuatoriano, que incluye el Código Orgánico Integral Penal y la Ley Orgánica de Protección de Datos Personales, demanda que prueba tiene que apegarse a procedimientos formales en forma tal que pueda ser presentada ante tribunales judiciales.

1.7.2 ISO/IEC 27042:2015

Título: Directrices para el análisis e interpretación de la evidencia digital.

Organismos: ISO/IEC.

1.7.2.1 Objetivo y alcance

La ISO/IEC 27042:2015 describe metodologías para examinar y correlacionar evidencias electrónicas (ISO, 2015).

- **Enfoque**: Facilitar la reproducibilidad de los análisis y la solidez de los resultados.
- **Ámbito en la nube**: Permite gestionar incidentes donde los datos están dispersos o sujetos a variaciones constantes, propias de los servicios cloud.

1.7.2.2 Componentes clave

A. **Preparación del Análisis**

- Define las metas y delimita las fuentes de datos digitales (logs, registros de auditoría, máquinas virtuales).

B. **Técnicas de Interpretación**

- Comprende métodos para correlacionar incidentes, detectar comportamientos anómalos y reconstruir líneas temporales.

C. **Documentación de Procesos**

- Indica la necesidad de describir cada paso y cada herramienta empleada, requisito crucial para la validez forense (Asamblea Nacional del Ecuador, 2014, art. 476).

1.7.2.3 Relevancia en Ecuador

- **Elasticidad del Entorno Cloud**: La infraestructura compartida demanda análisis dinámicos y estricta colaboración con el proveedor para obtener datos fidedignos (Mintel, 2019).
- **Normativas Locales**: El uso de técnicas analíticas reconocidas en ISO/IEC 27042 ayuda a cumplir la legislación ecuatoriana sobre delitos informáticos y protección de datos (Ley Orgánica de Protección de Datos Personales, 2021).

1.7.3 ISO/IEC 27043:2015

Título: Principios y procesos para la investigación de incidentes de seguridad de la información.

Organismos: ISO/IEC.

1.7.3.1 Alcance

Este estándar define un marco integral para la gestión de incidentes cibernéticos informáticos (ISO, 2015).

- **Fases**: Detección, contención, investigación, informes y lecciones aprendidas.
- **Visión global**: Al mismo tiempo, se ocupa de situaciones necesarias que involucran equipos técnicos y apoyo de proveedores externos.

1.7.3.2 Aspectos esenciales

A. **Planificación de la Investigación**

- Leyes de procedimiento indican protocolos para la coordinación de acciones con todos los proveedores de servicios cloud involucrados, así como con las autoridades judiciales.

B. **Procesamiento de la Evidencia**

- Determina el orden lógico para examinar los datos guardados, correlacionar eventos e intentar mantener la integridad de los registros.

C. **Retroalimentación y Aprendizaje**

- Al finalizar la investigación, recomienda documentar los hallazgos y reforzar medidas de seguridad a futuro.

1.7.3.3 Relevancia en Ecuador

- **SLA y Acuerdos:** En caso de incidentes en la nube, es necesario asegurarse de que el contrato con el proveedor incluya la posibilidad de recoger datos forenses cuando así sea necesario (Ley Orgánica Promoción de Datos Personales, 2021).

- **Cooperación con Instituciones**: Permite la colaboración entre organismos públicos y privados en la reconstrucción de incidentes y la persecución penal de los responsables (COIP, 2014, artículos 230-234).

1.7.4 RFC 3227: Guía para la recolección y el manejo de evidencia digital

Título: Guidelines for Evidence Collection and Archiving.

Organismo: Internet Engineering Task Force (IETF).

1.7.4.1 Propósito

El RFC 3227 propone directrices para la colección y el almacenamiento de datos según su volatilidad, un aspecto crítico en los entornos cloud donde los recursos pueden desaparecer en segundos (IETF, 2002).

1.7.4.2 Principios fundamentales

A. **Orden de Volatilidad**

- Prioriza la captura de memoria RAM, procesos activos y conexiones de red antes de que la máquina virtual se reinicie o se elimine.

B. **Documentación Minuciosa**

- Cada actuación (fecha, hora y mocito) será anotada a fin de poder justificar ante un tribunal ecuatoriano la integridad de la prueba (COIP, 2014, art. 474).

C. **Uso de Herramientas Certificadas**

- Evita que la información adquirida sufra alteraciones involuntarias tras adquirirla.

1.7.4.3 Aplicación en la nube

- **Captura Remota**: Los datos en la nube se recopilan básicamente a través de APIs (interfaces de programación) o portales de gestión.
- **Dependencia de Proveedores**: Es necesario normalmente cooperar con los proveedores, y se necesita asesoría técnica para obtener copias internas o snapshots de registros de máquinas virtuales.

1.7.5 NIST SP 800-86

Título: Guide to Integrating Forensic Techniques into Incident Response.

Organismo: National Institute of Standards and Technology (NIST).

1.7.5.1 Alcance

El NIST SP 800-86 trata sobre cómo hacer peritajes forenses en respuesta a incidentes de seguridad, cubriendo ya sea el mundo de TI convencional o los sistemas virtualizados (NIST, 2006).

1.7.5.2 Componentes principales

A. **Preparación**

- Se instruye a las organizaciones para que tengan planes y equipos forenses listos antes de que ocurra un incidente.

B. **Recolección de Datos**

- Se especifica cómo recoger y conservar la evidencia sin contaminarla.

C. **Examen y Análisis**

- Plantea estrategias de correlación y evaluación de logs, metadatos y configuraciones que son fundamentales en ambientes cloud.

D. **Reporte**

- Sugiere elaborar un informe final que registre las evidencias, conclusiones y recomendaciones, ajustándose a la normativa nacional (COIP, 2014, art. 476).

1.7.5.3 Relevancia en Ecuador

- **Escalabilidad de la Nube**: Provee lineamientos que facilitan la respuesta coordinada ante incidentes masivos o simultáneos (Mintel, 2019).
- **Cadena de Custodia Ecuatoriana**: El COIP y la Ley Orgánica de Protección de Datos Personales exigen estrictos controles para asegurar que la evidencia digital se conserve y manipule de forma legítima.

Tabla 1

Fortalezas y Debilidades de los Estándares internacionales de informática forense en la nube

Estándares internacionales de informática forense en la nube: fortalezas y debilidades, aplicabilidad y relevancia en Ecuador						
Estándar	**Alcance / Propósito**	**Aplicabilidad en la nube**	**Fortalezas**	**Limitaciones**	**Relevancia en Ecuador**	**Casos de uso típicos**
ISO/IEC 27037:2012	Directrices para identificación, recolección, adquisición y preservación de evidencia digital.	Adaptable a entornos distribuidos (CSP, regiones, centros de datos remotos).	Estructura clara de adquisición y preservación (hash, control de acceso); facilita validez legal.	Requiere coordinar con CSP; acceso indirecto a infraestructura del proveedor; dependencia de formatos/retención.	Soporta exigencias del COIP y LOPDP para admisibilidad; útil cuando no hay acceso físico al hardware.	Congelar snapshots/volúmenes, exportar logs; apertura de cadena de custodia.
ISO/IEC 27042:2015	Directrices para análisis e interpretación de evidencia; enfoque en reproducibilidad.	Correlación de logs cloud (CloudTrail/Azure/GCP), VMs y artefactos distribuidos.	Metodología para correlación temporal y consistencia; facilita auditoría del análisis.	Curva de madurez: exige trazabilidad detallada y herramientas compatibles; grandes volúmenes de datos.	Alinea documentación exigida (ej. Art. 476 COIP: describir procesos/herramientas).	Reconstrucción de líneas de tiempo multiservicio; validación de hipótesis.

ISO/IEC 27043:2015	Marco de gestión de incidentes (detección, contención, investigación, reporte, lecciones).	Incidentes con proveedores externos, SLA y equipos mixtos (CSP–organización).	Proceso extremo a extremo; integra coordinación con CSP y mejora continua.	Implementación depende de SLA y capacidades del proveedor; requiere gobernanza.	Refuerza que contratos incluyan cláusulas de cooperación forense (SLA) acorde a LOPDP.	Plan de respuesta Cloud + OnPrem; post-mortem y endurecimiento.
RFC 3227 (IETF)	Guía para recolección y archivado según orden de volatilidad.	Priorización de RAM/procesos/red en VMs; captura remota donde sea factible.	Regla práctica clara (qué capturar primero); minimiza pérdida de evidencia volátil.	En nube, obtener RAM puede ser complejo; depende de permisos y ventanas de tiempo.	Útil para justificar prioridad de capturas ante fiscalía/tribunal; respalda la prontitud.	Live response en IaaS; captura temprana de memoria/conexiones y luego disco/log.

Nota. Elaboración propia con base en *a*ISO/IEC 27037:2012, *b*ISO/IEC 27042:2015, *c*ISO/IEC 27043:2015, y *d*Brezinski y Killalea (2002). COIP = Código Orgánico Integral Penal; LOPDP = Ley Orgánica de Protección de Datos Personales.

1.8 Fundamento constitucional

La Constitución de la República del Ecuador (2008) sienta la base jurídica fundamental que sostiene la validez y la gestión de las pruebas electrónicas en el país:

- **Art. 66**: Garantiza el derecho a la intimidad personal y familiar, sin el cual no se podrían recolectar ni analizar datos de carácter sensible.
- **Art. 76**: Respeto al debido proceso y a la validez de las pruebas presentadas en juicio. Por tanto, cualquier metodología forense que se emplee deberá hacerlo según la legalidad y la conservación de la prueba en toda su integridad.
- **Art. 92**: R Regulación del Hábeas Data y Protección de Datos Personales. Esta norma establece que cualquier persona puede exigir acceso, rectificación o cancelación de su información.
- **Art. 425**: Determina la jerarquía normativa revestida en un ordenamiento constitucional. Igualmente, si las normas aplicables a la evidencia digital contradicen algo que establece la propia Constitución o de una ley, la norma será observar sólo el sentido claro contenido en ella (Asamblea Nacional del Ecuador, 2008).

Estas disposiciones constitucionales exigen que el análisis forense digital sea llevado a cabo respetando los principios de proporcionalidad, legalidad y protección de la intimidad, a fin de garantizar la legitimidad de las pruebas durante los procesos judiciales.

1.8.1 Código Orgánico Integral Penal (COIP)

El Código Orgánico Integral Penal (COIP), publicado en el Registro Oficial Suplemento 180 de 10 de febrero de 2014, tipifica los delitos informáticos y establece lineamientos esenciales

para la cadena de custodia y la validez de la evidencia digital (Asamblea Nacional del Ecuador, 2024).

1.8.1.1 Delitos informáticos

El COIP recoge varios tipos penales que requieren una investigación forense sólida para su comprobación:

- **Acceso no autorizado a sistemas informáticos** (Art. 234): Castiga con 3 a 5 años de prisión a quienes ingresen ilícitamente a sistemas computacionales.
- **Interceptación de datos** (Art. 230): Sanciona con 3 a 5 años de prisión la captura ilegal de información en tránsito o almacenada.
- **Revelación ilegal de bases de datos** (Art. 229): Prevé de 3 a 5 años de prisión para quienes difundan sin autorización información contenida en sistemas o bases de datos.
- **Ataque a la integridad de sistemas informáticos** (Art. 232): Castiga con 3 a 5 años de prisión a quienes alteren, dañen o destruyan información o recursos informáticos.
- **Art. 178**: Violación a la intimidad, aplicable cuando se accede indebidamente a comunicaciones o registros personales.
- **Art. 190**: Apropiación fraudulenta por medios electrónicos, relativo a la obtención ilegítima de bienes ajenos mediante sistemas informáticos.

La investigación forense digital permite demostrar si estos actos delictivos se han cometido, aportando evidencias que confirmen actividades ilícitas (Asamblea Nacional del Ecuador, 2008).

Tabla 2

Delitos Informáticos

Delito	Artículo	Sanción	Descripción Breve
Acceso no autorizado a sistemas informáticos	Art. 234	3 a 5	Ingresar ilícitamente a un sistema o base de datos sin consentimiento del titular.
Interceptación de datos	Art. 230	3 a 5	Capturar, observar o registrar ilegalmente datos en tránsito o almacenados en sistemas informáticos.
Revelación ilegal de bases de datos	Art. 229	3 a 5	Difundir o compartir información protegida contenida en bases de datos sin autorización.
Ataque a la integridad de sistemas informáticos	Art. 232	3 a 5	Alterar, dañar o destruir sistemas, datos o programas, afectando la disponibilidad y el normal funcionamiento.
Violación a la intimidad	Art. 178	1 a 3	Acceder y divulgar indebidamente comunicaciones o registros personales, vulnerando la intimidad ajena.
Apropiación fraudulenta por medios electrónicos	Art. 190	3 a 5	Obtener ilegalmente bienes ajenos mediante el uso o manipulación de sistemas electrónicos.

Nota. Elaboración propia con base en el Código Orgánico Integral Penal (COIP) de la República del Ecuador (Asamblea Nacional, 2014)

1.8.1.2 Validez de la evidencia digital

Art. 456: Regula la cadena de custodia requiriendo que toda evidencia digital, incluida la digital, sea registrada y custodiada con detalle a fin de no perder su integridad.

Art. 476: Habla de la interceptación de comunicaciones, requiere orden judicial y asegura la admisión de pruebas legalmente obtenidas.

Art. 500: Establece que el contenido digital puede ser presentado como prueba, siempre que cumpla los requisitos de autenticidad y legalidad.

También subraya la necesidad de procesos forenses transparentes, mediante lo cual COIP pretende garantizar ambas cosas: la legitimidad de evidencias tecnológicas y su fiabilidad judicial.

1.8.2 Ley de comercio electrónico, firmas electrónicas y mensajes de datos

Publicada en el Registro Oficial Suplemento 557 de 17 de abril de 2002, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Asamblea Nacional del Ecuador, 2008) reconoce la validez legal de las transacciones electrónicas y de los documentos digitales.

1.8.2.1 Aspectos relevantes para el análisis forense

Art. 7: La información digitalizada tiene los mismos valores que la original, siempre que se cumplan las medidas de integridad pertinente.

Art. 11: Los mensajes de datos perdurarán para el caso de que sean necesarios para prueba en materia de derecho.

Art. 14: La información sensible quedará protegida y existirán medidas de control para prevenir una divulgación no autorizada.

Art. 52: Las pruebas electrónicas serán admisibles de manera que electrónicos mediante registros de auditoría, correos electrónicos, logs de sistemas, entre otros.

1.8.2.2 Firma electrónica

Art. 17.- Incluye los requisitos de una firma electrónica al exigir que sea fiable, única y necesariamente vinculada con el firmante.

Art. 19.- Regula la validación de certificados digitales, algo fundamental en comprobación de identidades documento gráficas y autenticación de documentos.

Art. 20.- Establece la fiabilidad de los dispositivos de creación y verificación de firmas electrónicas, cuyo adecuado uso es esencial para la recolección y preservación de la evidencia digital.

Ley de Comercio Electrónico fortalece el marco del marco ecuatoriano al admitir que la firma electrónica y el documento o mensaje de datos tienen valor probatorio, dos pilares básicos para pruebas digitales en el campo del peritaje (Asamblea Nacional del Ecuador, 2008).

1.9 Concepto, aplicabilidad, ventajas y limitaciones de las herramientas en la nube

En esta sección, se presenta una tabla comparativa detallada de las herramientas y los conceptos fundamentales de la forensia digital, con énfasis en su aplicabilidad, ventajas y limitaciones en los entornos de computación en la nube. La tabla presenta una síntesis de cómo funcionan, para qué se utilizan, cuáles son sus ventajas específicas que pueden ser implementadas en la nube, cuáles son sus limitaciones inherentes a estos entornos y cuáles podrían ser los casos de uso más relevantes. Esta presentación estructural de la información se hace para comprender mejor dónde se posiciona tal o cual herramienta/concepto dentro del ecosistema complejo de la forensia en la nube.

La inclusión de esta hoja de cálculo permite una comparación rápida y directa de las características, ventajas y desventajas de cada herramienta o concepto, resaltando sus fortalezas y debilidades únicas en el contexto específico de la forensia en la nube. Además, sirve como una herramienta invaluable en la escritura o identificación de qué herramientas son más relevantes para preguntas de investigación específicas y puede ayudar a justificar la selección de los autores.

El análisis forense en la nube, también conocido como cloud forensics, es un término que describe la colección y el análisis de pruebas digitales específicamente relacionadas con incidentes y delitos informáticos que involucran sistemas informáticos en la nube. El análisis forense de la nube es simplemente una extensión del análisis forense tradicional. Este campo emergente ha evolucionado para abordar los legados de la informática forense convencional en infraestructura en la nube, así como los desafíos distintivos creados por la infraestructura en la nube. La coherencia y la adaptabilidad del análisis forense de la nube se desarrollan a través de su propio acercamiento a los desafíos sustantivos y procesuales presentes en la nube. El análisis forense de la nube se esfuerza por superar muchos desafíos presentes en la nube, incluyendo los distintos servicios, sistemas y procesos utilizados. El análisis forense de la nube intenta abordar un amplio rango de ciberdelincuencia que incluye varios malos usos de la nube, como la divulgación de información, el robo de identidad y el phishing (Arsys, 2024).

Un aspecto fundamental del análisis forense en la nube es la consideración de la normativa legal aplicable a la obtención y el tratamiento de los datos en la nube, especialmente cuando estos se almacenan en jurisdicciones cruzadas o están sujetos a la jurisdicción de un proveedor de servicios externo, CSPs. La dificultad de determinar la propiedad de las pruebas y su admisibilidad en diferentes foros introduce una complejidad adicional para la informática forense en comparación con las áreas mejor establecidas de informática forense, donde la jurisdicción es más

clara. A medida que más organizaciones y particulares adoptan la nube, los crímenes digitales dirigidos al entorno de la nube se han multiplicado exponencialmente, destacando aún más la importancia crítica del cloud forensics para proteger y confiar en la nube. La naturaleza distribuida y virtualizada de los datos en la nube exige un enfoque forense específico, capaz de superar los retos tecnológicos y legales asociados con este modelo (Arsys, 2024).

1.9.1 The Sleuth Kit (TSK) / Autopsy

1.9.1.1 Aplicabilidad en la nube

Sleuth Kit es una recopilación de software libre, principalmente herramientas de línea de comandos, así como una biblioteca en lenguaje C. Ambos se diseñan para facilitar el análisis de imágenes de disco y la recuperación de archivos. Por otro lado, “Autopsy es una GUI de TSK de código abierto que aprovecha las capacidades del TSK y las combina con otras herramientas de investigación forense digital en un entorno de análisis”. Los investigadores pueden utilizar Autopsy para revisar las imágenes de disco duro, así como unidades de almacenamiento USB o tarjetas de memoria. En consecuencia, “existe evidencia de que Autopsy puede analizar datos digitales si se presentan como un formato de almacenamiento, y así tener derecho a considerarse” (Arsys, 2024).

1.9.1.2 Ventajas

La plataforma Autopsy se destaca por su facilidad de uso, ya que se creó para ser intuitiva desde su configuración inicial. La plataforma cuenta con asistentes que guían al usuario en todas las etapas de la investigación, lo que permite que cualquier persona, inclusive los menos experimentados, la maneje, gracias a su enfoque en “investigar primero” (Alemán Ariza, 2024). Además, le plataforma es altamente extensible, ya que permite a los usuarios agregar sus propios

módulos y complementos dirigidos a ampliar la funcionalidad disponible para satisfacer sus necesidades periciales específicas (Alemán Ariza, 2024). Autopsy suministra varias características críticas para los investigadores forenses digitales, incluido el análisis de la línea de tiempo de los eventos, el filtrado de archivos conocidos mediante hash, la búsqueda de palabras clave importantes, el análisis de artefactos de bases de datos web, como historial de navegación y cookies, la recuperación de archivos eliminados, el análisis de archivos multimedia y el descubrimiento de malware (Alemán Ariza, 2024).

La herramienta también se destaca por su eficiencia, ya que Autopsy puede realizar las tareas en segundo plano de forma paralela, aprovechando la capacidad de los procesadores multicore, lo que permite analizar más rápido. Una de las ventajas más fuertes de Autopsy es que es de código abierto y gratuito, por lo que es atractiva para una gran cantidad de profesionales e investigadores con un presupuesto ajustado. También se puede señalar que The Sleuth Kit, la base de Autopsy, permite el examen no intrusivo de las imágenes del disco y los sistemas de archivos para preservar la evidencia original. Autopsy puede recuperar actividad reciente del sistema, historial de navegación web, cookies, archivos eliminados y palabras clave, proporcionando una visión clara de la actividad digital (Autopsy, 2024).

1.9.1.3 Limitaciones

Todo esto significa que la aplicabilidad directa de TSK y Autopsy en entornos de nube tiene limitaciones significativas si los datos almacenados en la nube no se adquieren y formatean previamente en un formato que puedan manejar (Arsys, 2024). Además, si bien TSK está diseñado para funcionar principalmente a nivel de sistema y discos, las estructuras de almacenamiento de datos en la nube son diferentes, lo que dificulta aún más el análisis directo (Sleuth Kit, 2024). Si bien Autopsy es una herramienta poderosa, su eficiencia puede verse reducida cuando se trata de

volúmenes de datos muy grandes, en comparación con algunas de las soluciones comerciales que se han apoyado especialmente en este propósito. Finalmente, Autopsy puede tener limitaciones en términos de soporte para diferentes sistemas de archivos, como XFS, lo que podría ser relevante en ciertas configuraciones de nube (Sleuth Kit, 2024).

Además de la naturaleza volátil de los datos en la nube, las necesidades de una colaboración activa con los CSP para obtener la evidencia forense plantean desafíos adicionales para el uso de TSK y Autopsy en la nube. A diferencia de los análisis forenses en sistemas locales, en los que la adquisición de datos se resuelve generalmente de manera más directa, las investigaciones en la nube dependen en última instancia de la disposición del CSP o de la oportunidad de brindar al investigador los datos necesarios en un formato que sea accesible para las herramientas como TSK y Autopsy. Por lo tanto, aunque las herramientas discutidas son útiles en un contexto forense digital más amplio, su aplicabilidad en escenarios de investigación en la nube en particular se puede limitar debido a las dificultades relacionadas con la adquisición de datos y la compatibilidad de formatos (Arsys, 2024).

1.9.2 Volatility y Rekall

1.9.2.1 Aplicabilidad en la nube

La primera, la Volatilidad, se define como un marco de código abierto ampliamente utilizado para llevar a cabo análisis forense de la memoria volátil, es decir, la memoria de acceso aleatorio de un sistema informático. El segundo el Rekall, por otro lado, se convirtió en una bifurcación descendente del proyecto Volatility en 2011 y ofrece funcionalidades muy similares para el análisis de la memoria de la máquina Walters, F. R. Ambas herramientas están diseñadas para extraer y analizar los datos residentes en la memoria de un ordenador, los cuales son

eliminados completamente cuando se apaga mientras se instala el ordenador, según (Walters, 2007).

En el ámbito específico del cómputo en la nube, la relevancia de Volatility y Rekall radica enteramente en la posibilidad de obtener volcados de memoria de las instancias en ejecución en la nube, aunque es menos común, ya que las instancias en la nube pueden referirse a máquinas virtuales que corren en un modelo popular de servicio en la infraestructura conocido como Infraestructura como Servicio (IaaS). Recientemente, algunos proveedores de nube han comenzado a proporcionar la funcionalidad de la creación de volcado de memoria de su instancia para facilitar el trabajo forense en la nube. A pesar de que la mayoría de los volcados de memoria pueden ser creados en instancias que ejecutan una variedad de sistemas operativos, como Windows, Linux y macOS, estas herramientas tienen la capacidad de analizarlos (KeepCoding, 2024). En este caso, es relevante en el análisis forense en la nube cuando el volcado de memoria de la instancia en ejecución es posible, a menudo, en el modelo de servicio IaaS, donde los usuarios tienen la libertad de acceder a máquinas virtuales.

1.9.2.2 Ventajas

Sin embargo, Volatility y Rekall ofrecen una serie de ventajas significativas para el análisis forense digital al trabajar con volcados de memoria, especialmente en el contexto de la nube donde dichos volcados a menudo están disponibles. Estos incluyen la capacidad de ver la lista de procesos en ejecución en el momento en que se observó el volcado de memoria, la lista y los parámetros de las conexiones de red activas, las credenciales bajo las cuales se lanzan los procesos representados en el volcado de memoria y otras credenciales de usuario que el sistema podría haber almacenado en la memoria; las claves secretas de los sistemas o aplicaciones utilizadas; y muchos otros, algunos de los cuales son críticamente valiosos para la evidencia. Uno de los más valiosos es el

hecho de que Volatility y Rekall pueden detectar software malicioso que no es visible en el disco duro debido a su naturaleza volátil o porque no se lanza intencionalmente de una manera que deja indicadores en el disco duro (Walters, 2007).

Asimismo, Volatility contiene una gama amplia de modos y comandos que permiten a los investigadores examinar el contenido de un archivo de volcado de memoria en un nivel más detallado y, por lo tanto, identificar fácilmente artefactos y patrones sospechosos. Volatility 3, a su vez, introduce varias mejoras notables de rendimiento en comparación con sus predecesoras, Volatility 2 y Rekall, que hacen que sea mucho más rápido y, por lo tanto, sea más fácil de usar para analizar grandes dumps de memoria. Cabe destacar que Volatility se basa en arquitectura extensible; tiene mucho de complementos desarrollados y mantenidos por una comunidad activa de investigadores y profesionales de la seguridad, lo que guarda un enorme potencial para expandir las capacidades de la herramienta para analizar diferentes tipos de artefactos de memoria (Walters, 2007).

1.9.2.3 Limitaciones

No obstante, existen algunas limitaciones significativas que se asocian al uso de Volatility y Rekall en el análisis forense en la nube. La primera es que obtener volcados de memoria en entornos de nube puede ser un proceso complicado y depende en gran medida de la funcionalidad y las directrices proporcionadas por el proveedor de servicios en nube. La volatilidad inherente de los recursos de la nube generalmente implica que la evidencia en la memoria se pierda rápidamente a menos que se tome la iniciativa de adquirir volcados de memoria inmediatamente después de encontrar un incidente (Arsys, 2024).

Otra limitación significativa es que Rekall, aunque fue una valiosa herramienta en su tiempo, ya no es mantenida por sus desarrolladores, lo que puede limitar su utilidad para futuras investigaciones y análisis, en constante evolución en la medida en que cambian los sistemas operativos y los mecanismos de ataque. Por otro lado, el análisis de la memoria en general requiere un conocimiento técnico significativo para interpretar correctamente los datos extraídos de los volcados de memoria y descartar la información no relevante para la investigación. Finalmente, las técnicas anti-forenses utilizadas por los atacantes pueden dificultar en última instancia la adquisición de volcados de memoria completos y confiables, lo que perjudica la efectividad de los análisis de Volatility y Rekall (Arsys, 2024).

1.9.3 Log2timeline / Plaso / Timesketch

1.9.3.1 Aplicabilidad en la nube

Log2timeline es una herramienta forense digital que se creó de tal forma que cualquier información puntual, llamada marca de tiempo, pudiera ser extraída de una gran cantidad de fuentes de datos con el fin de crear una superlínea de tiempo. Plaso es una reescritura del mismo en Python que hace funcionar un motor, el cual toma el lugar de múltiples procesos forenses útiles para construir líneas de tiempo más consolidadas. Por otro lado, Timesketch es una herramienta web de código abierto que permite a los investigadores colaborar en la creación y visualización de líneas de tiempo forenses. Por último, en Timesketch, los investigadores importaron el archivo de salida generado por Plaso para hacer que los mismos sean visibles e interactivos o analizables (Universidad de New Haven, 2018).

En cuanto a cómo pueden aplicarse estas herramientas al marco de la computación en la nube, el primer paso esencial es adquirir los registros relevantes que hayan sido elaborados por los

distintos servicios en la nube involucrados en el incidente. Esto puede incluir registros de acceso a la plataforma, registros de actividad del usuario, registros de auditoría de tiendas y cualquier otro tipo de log que pueda contener la marca de tiempo relevante para el incidente de seguridad en cuestión. Plaso está diseñado para ser extensible y admite la recopilación y análisis de registros desde diversas fuentes, incluyendo de manera específica los registros de AWS CloudTrail, el registro de actividad de Azure y Google Cloud utilizado por GCP. Una vez que los datos se han procesado utilizando Plaso para construir una línea de tiempo, estos datos se cargan en Timesketch (ya sea un archivo CSV o un archivo Plaso DFT bundle) para facilitar el análisis y la visualización a través de su interfaz web (The Digital Forensics, 2019).

1.9.3.2 Ventajas

Una de las ventajas clave de log2timeline y Plaso es su capacidad para generar líneas de tiempo superiores que consolidan eventos marcados en el tiempo de múltiples fuentes dispares en un solo lugar coherente para su análisis forense. Esta característica es de particular valor en la nube, donde la actividad puede estar dispersa a través de numerosos servicios y registros. Es especialmente para el caso de Plaso debido a que es un marco altamente extensible. Pueden añadirse nuevos analizadores y complementos con asiduidad para dar soporte a una creciente gama de formatos de registro y fuentes de datos.

Las herramientas de replanteo como Timesketch facilitan la colaboración entre los investigadores, el intercambio de líneas de tiempo enviadas para la revisión y la capacidad de realizar una búsqueda eficiente dentro de los datos, lo que permite la identificación rápida de patrones y correlaciones de eventos aparentemente no relacionados: también desempeña un papel vital en la visualización de datos. Análogo. Ofrece a los usuarios un filtrado avanzado, en el cual los usuarios pueden enfocarse en eventos específicos. Hace el filtrado mediante la generación de

gráficos tales como mapas de calor, histogramas. Finalmente, la habilidad de añadir un evento específico a eventos enriquece el análisis y facilita la documentación de hallazgos. Además, Plaso es especialmente versátil, ya que es posible crear líneas de tiempo muy específicas, que se centran únicamente en ciertos tipos de eventos o artefactos, pero también líneas de tiempo superiores, que cubren la totalidad de la actividad registrada en un sistema o conjunto de sistemas (The Digital Forensics, 2019).

1.9.3.3 Limitaciones

Sin embargo, a pesar de las muchas ventajas de su uso, no se libra de limitaciones. Además, existe un desafío fundamental al preparar registros de la nube para ser "plaseados", ya que, con raras excepciones, los registros deben recolectarse y ocasionalmente convertirse previamente a un formato compatible con Plaso. Con la amplia gama de formatos de registro que se pueden utilizar de nube a nube, la creación de analizadores de registros personalizados para Plaso puede consumir mucho tiempo; esto también puede ser una nueva carga en el centro de análisis de un CSIRT de universidad. Además de la cuestión de la compatibilidad, el volumen excesivo de información que fluye en y a través de entornos de nubes hiperescalas plantea problemas nuevos, pero no únicos de "big data".

El procesamiento y análisis de las líneas de tiempo exigen recursos, así como la administración de los datos de resultados. Si bien Timesketch proporciona al usuario final una interfaz web intuitiva para el análisis y la visualización, la eficacia en la creación de muchas líneas de tiempo a menudo requiere la capacidad de usar log2timeline y Plaso. Esta capacidad, a su vez, implica una cierta habilidad técnica en la línea de comandos (Universidad de New Haven, 2018).

1.9.4 EnCase (Guidance Software / OpenText)

1.9.4.1 Aplicabilidad en la nube

EnCase es una plataforma forense comercial de Guidance Software, que es parte de OpenText, que disfruta de una amplia adopción en varias áreas de la investigación digital, que van desde la informática forense tradicional hasta la seguridad digital, la investigación de seguridad y la revisión de apelación electrónica. Entre las características principales de EnCase se encuentra la capacidad de recuperar datos de una variedad de fuentes, que van desde los tradicionales segmentos de informática forense que incluyen Windows, Mac y Linux hasta dispositivos móviles y, en el contexto de este trabajo, aplicaciones que operan en plataformas en la nube. OpenText ofrece varias opciones para la implementación de EnCase en plataformas en la nube, que incluyen implementaciones en la plataforma nativa de OpenText, la nube OpenText, y las otras plataformas en la nube pública basadas en proveedores de servicios de nube comunes, incluidos AWS, GCP o Azure. EnCase está diseñado para recopilar evidencia específica de la nube, incluida la que se genera localmente en los dispositivos y en plataformas en la nube populares, como las redes sociales Facebook, Twitter, Instagram, los servicios seleccionados de Google, iCloud, WhatsApp, la base de LinkedIn y más.

Además, puede recopilar información de navegadores web, videos, archivos y servicios de localización para asegurarse de que toda la evidencia relacionada con la nube sea sintetizada y resaltada para su uso en casos de ciberdelitos. A través de esta capacidad de integrar fuentes de datos en la nube y fuera de ella en un solo caso de investigación, EnCase demuestra su utilidad en escenarios que involucran jurisdicciones de nube complejas (OpenText, 2024).

1.9.4.2 Ventajas

Todas las ventajas proporcionadas anteriormente hacen de EnCase una herramienta poderosa para un análisis forense, y para nuestro propósito específico, específicamente con respecto a la nube. Existe la posibilidad de previsualizar los resultados, la adquisición de datos procesales en múltiples unidades de almacenamiento o fuentes de datos, incluida la nube. La adquisición de datos ha sido facilitada por EnCase; permite adquirir rápida pero exhaustivamente datos de varias fuentes. Se ha hecho mucho más fácil y más compatible con diferentes dispositivos, que es uno de los aspectos más importantes de la investigación en caso de que la evidencia provenga de ambos sistemas basados en la nube y sistemas internos. Se permite la adquisición rápida de datos de un amplio rango de fuentes y cuenta con una variedad de dispositivos y está habilitada por diversas ediciones (OpenText, 2024).

Maximiza el uso de recursos costosos y excesivos procesando todas las pruebas en un caso, administrando múltiples evidencias en un solo caso y generando informes simples usables, reduciendo así la presión sobre las partes debido a la escasez de recursos. Findings pueden comunicarse a escucha utilizando informes claros y fáciles de describir. Con respecto a la nube, esto se ha logrado a través de EnCase Full se aplica soporte de artefactos que incluye todos los componentes de la actividad, tanto en el hardware como en la nube. Se utiliza la inteligencia artificial y el aprendizaje automático para especificar automáticamente imágenes, ya sean patológicas o imágenes de la indicación de un interés extremo. Un motor de indexación directa y flujos de trabajo basados en artefactos llenos de la eficiencia en la conducción del análisis. Se proporciona la programación con el soporte de EnScript, que es un lenguaje informático para scripter que puede especifique comandos basándolos de su investigación costosamente temporal, como haría la investigación basada en varios documentos diferentes o cualquier paso de

especificación de procesos personalizados, y luego ejecutar los procesos automáticamente; Se brinda soporte para tareas mucho más avanzadas (OpenText, 2024).

1.9.4.3 Limitaciones

Sin embargo, incluso con todas sus ventajas, EnCase tiene limitaciones, algunas de las cuales son aún más relevantes en el contexto del análisis forense en la nube. Uno de los aspectos es el hecho de que EnCase es un software comercial que implica un costo de licencia asociado. En algunos casos, para ciertos tipos de usos, las instituciones y los profesionales pueden encontrar este software prohibitivamente caro. Al igual que con muchas otras herramientas forenses, la complejidad y el tamaño de los datos en la nube pueden desafiar el procesamiento con EnCase. Otra limitación común para todas las investigaciones en la nube es la preocupación legal y de privacidad sobre si los investigadores tienen derecho a acceder a ciertos datos.

Otra limitación longitudinal de usar EnCase es que la falta de estandarización en la ciencia forense digital puede hacer que los resultados de un análisis en la nube sean inconsistentes de una plataforma CPARA a otra, lo que requiere que los investigadores sean expertos con los entornos en cuestión. Del mismo modo, dado el ritmo al que cambia la tecnología y el hecho de que la mayoría de las empresas de tecnología ahora usan técnicas de cifrado, es posible que el acceso y la desencriptación especializada para datos en la nube sean problemáticos incluso en entornos de nube confiables (Arsys, 2024).

1.9.5 FTK (Forensic Toolkit)

1.9.5.1 Aplicabilidad en la nube

FTK es otra herramienta comercial que es ampliamente reconocida y usada en las investigaciones forenses digitales. En este caso, FTK destaca por su capacidad de procesar

enormes cantidades de datos, y por consiguiente es una herramienta investigativa sumamente útil en lo relativo a discos duros y otros medios de almacenamiento digital. Si bien FTK fue diseñado para investigaciones tradicionales, en la actualidad cuenta con capacidades para hacer análisis forenses en la nube (Exterro, 2024).

Por otra parte, Exterro FTK Lab es una plataforma mediante de procesamiento distribuido de alta velocidad con capacidades de revisión colaborativa multi-usuario (Exterro, 2024), lo que resulta ideal para las grandes cantidades de datos que se suelen manejar mediante la nube. FTK ofrece funcionalidades como la indexación rápida de data, procesamiento de correos y registros del sistema y recuperación de ficheros eliminados, que hacen que sea una herramienta ideal para análisis de la data una vez extraída de la nube. Posee un motor de data carving que permite recuperar data conseguida o eliminada de muchas fuentes de data, que incluye al almacenamiento en la nube (Exterro, 2024).

1.9.5.2 Ventajas

La eficiencia en el procesamiento de grandes volúmenes de datos es una de las principales ventajas de FTK y es esencial en el análisis forense en la nube, ya que las cantidades pueden ser enormes. FTK ayuda a los investigadores al indexar rápidamente los datos, lo que les permite realizar búsquedas de forma rápida y precisa. Aparte del análisis de correos electrónicos, la recuperación de archivos eliminados y la revisión de registros del sistema, FTK también cuenta con un potente motor para data carving que permite la recuperación de datos.

También ofrece varias capacidades de visualización de datos, como líneas de tiempo, gráficos de clúster y funciones de geolocalización, para ayudar a los investigadores a visualizar las relaciones entre los diferentes elementos de evidencia en la nube. FTK incluye una herramienta de detección de malware automatizada conocida como Cerberus, que realiza este análisis utilizando

inteligencia artificial. Esto es relevante hoy, ya que muchos datos se originan y almacenan en la nube. Por último, es vital destacar que FTK Imager, una herramienta relacionada utilizada para la creación de imágenes forenses de discos, está disponible de forma gratuita. Para los investigadores que intentan optimizar el uso de los recursos económicos, esta es claramente una ventaja (Exterro, 2024).

1.9.5.3 Limitaciones

Al igual que EnCase, FTK es un software comercial. Requiere la compra de una licencia para su uso, lo que puede ser una limitación para algunos investigadores o instituciones. Tanto la complejidad como la naturaleza distribuida de los datos en la nube pueden presentar un desafío mayor con FTK que en una computadora personal. Necesitar acceder a los datos almacenados en la nube a través de los proveedores de servicios en la nube implicaría las mismas limitaciones legales y de cooperación que con otras herramientas forenses en la nube.

En cuanto a la producción, FTK. Aunque FTK es capaz de analizar los datos que provienen de la nube, no puede tener las mismas capacidades especializadas para ciertos servicios en la nube en comparación con herramientas que han sido diseñadas nativamente para estos ambientes o que se especializan en el análisis forense de servicios de nube. En general, si bien FTK sigue siendo una sólida herramienta para el análisis forense digital, es posible que su adaptación a la nube requiera realizar extracciones y preparar datos en formatos compatibles y no funcione óptimamente en ciertas plataformas de nube (Arsys, 2024).

1.9.6 AXIOM (Magnet Forensics)

1.9.6.1 Aplicabilidad en la nube

AXIOM, desarrollado por Magnet Forensics, es una suite integral de software forense digital diseñada para abarcar las etapas de adquisición, análisis y presentación de evidencia digital en una amplia variedad de casos (Alemán Ariza, 2024; Magnet Forensics, 2024). Una de las fortalezas de AXIOM radica en su capacidad para realizar análisis forense de manera integral, cubriendo dispositivos móviles, ordenadores y, de manera significativa para este contexto, datos almacenados en la nube, todo dentro de una única interfaz unificada (Alemán Ariza, 2024; Magnet Forensics, 2024). AXIOM Cloud, una funcionalidad específica dentro de la suite, permite a los investigadores adquirir datos de múltiples fuentes de la nube, incluyendo plataformas populares como Apple iCloud, Google Drive y cuentas de Google, Facebook, Microsoft OneDrive y cuentas de correo de Outlook y Office 365, Dropbox, Twitter y WhatsApp (Magnet Forensics, 2024).

La herramienta ofrece flexibilidad en los métodos de adquisición y autenticación para acceder a las cuentas en la nube, soportando tanto el uso de nombres de usuario y contraseñas como la autenticación a través de navegadores externos y la utilización de tokens de cuenta obtenidos de extracciones móviles (Magnet Forensics, 2024). Además, Magnet Forensics ha desarrollado AXIOM Cyber, una versión de la plataforma específicamente diseñada para las necesidades de las investigaciones corporativas, permitiendo a las organizaciones realizar la recopilación remota de datos tanto de ordenadores como de la infraestructura en la nube, facilitando así la respuesta a incidentes y la investigación de actividades maliciosas en entornos empresariales (Magnet Forensics, 2024).

1.9.6.2 Ventajas

En cuanto a las ventajas distintivas de AXIOM para el análisis forense en la nube, la plataforma destaca por su capacidad para recuperar y analizar evidencia digital de diversas fuentes, como dispositivos móviles, la nube, ordenadores y vehículos, todo dentro de un mismo caso, lo que facilita enormemente el trabajo de los investigadores. AXIOM ofrece herramientas analíticas potentes y fáciles de usar que permiten a los investigadores identificar rápidamente los datos más relevantes para el caso, lo cual es crucial para los grandes volúmenes de datos en la nube. La plataforma está diseñada también para procesar los resultados de las órdenes judiciales a los proveedores de servicios en la nube, lo que permite a los agentes acceder y analizar la información obtenida a través de procesos legales.

La herramienta puede ser utilizada para analizar los datos de código abierto y las cuentas de usuario en plataformas en la nube como Google y WhatsApp, lo que ofrece una vista más completa de la actividad en línea y las comunicaciones. AXIOM también ofrece el panel de Cloud Insights, que utiliza poderosas herramientas analíticas para identificar automáticamente más evidencia relevante en datos en la nube. La herramienta también es compatible con Magnet One, una plataforma utilizada para combinar varias soluciones de forense digital, lo que mejora la eficiencia y la colaboración entre los equipos de investigación en la nube. Magneten Forensics agrega que una de las ventajas de andar con AXIOM Cyber es que los agentes pueden almacenar la evidencia sin procesamiento automático, lo que puede resultar ventajoso en algunos escenarios (Magnet Forensics, 2024).

1.9.6.3 Limitaciones

A pesar de los muchos beneficios antes mencionados, AXIOM, siendo una herramienta comercial, requiere una licencia para ser comprada, lo que impacta en el costo para los usuarios u organizaciones. En vista de la complejidad de los entornos de nube y la necesidad de adaptarse a los cambios en la interfaz de programación de aplicaciones de los proveedores de servicios en la nube, a menudo los usuarios deben actualizar el software con regularidad para que funcione correctamente y sea compatible. Además, ya se ha mencionado que AXIOM, como otras herramientas similares de análisis forense en la nube, debe obtener permiso de los proveedores de servicios en la nube y no tiene acceso irrestricto a todos los tipos de datos en vista de las políticas de privacidad, las disposiciones legales y restricciones y limitaciones técnicas de los proveedores (Arsys, 2024).

1.9.7 AWS Forensic Toolkit / AWS CLI

1.9.7.1 Aplicabilidad en la nube

Es necesario mencionar que no existe una herramienta oficial conocida como “AWS Forensic Toolkit” como un solo producto ofrecido por Amazon Web Services. Sin embargo, AWS ofrece una amplia gama de servicios y herramientas nativas que pueden ser efectivamente utilizadas para la conducción de análisis forense en su plataforma de nube. Uno de estos instrumentos incluye la AWS Command Line Interface, que es una interfaz de línea de comandos unificada desarrollada específicamente para ayudar en la administración de todos los distintos servicios subyacentes a la infraestructura ofrecida por AWS. Estos servicios nativos, así como la versatilidad presentada por la CLI de AWS, pueden ser combinados de forma estratégica para la recopilación y análisis de evidencia que resida en la nube de AWS.

Algunos ejemplos de servicios de AWS altamente relevantes para el análisis forense incluyen AWS CloudTrail, que registra la actividad de la llamada a la API dentro de una cuenta AWS; Amazon CloudWatch Logs, que provee un registro centralizado para toda la infraestructura; Amazon GuardDuty, que monitoriza la actividad de amenazas; Amazon Inspector para análisis de recursos con fallas; Amazon Macie para el análisis de privacidad y detección de datos sensibles, y Amazon Detective para la creación y desarrollo de una investigación de incidentes de seguridad en profundidad. La CLI de AWS puede también ser usada para extraer registros de CloudTrail que sean guardados en Amazon S3 (Amazon Web Services, 2024).

1.9.7.2 Ventajas

La clara ventaja del uso de las herramientas proporcionadas por AWS para el análisis forense en la nube es la integración nativa con la infraestructura subyacente. Eso permite la interacción perfecta y sin complicaciones con los servicios y los datos de AWS. Además, (Amazon Web Services, 2016) la plataforma proporciona una amplia capacidad de automatización de datos para la recopilación y el análisis forense a través de Amazon GuardDuty, AWS Security Hub, Amazon EventBridge, AWS Step Functions y AWS Lambda Cado Security, 2024). La escalabilidad y flexibilidad de la propia nube de AWS también ofrecen ventajas para el análisis forense, donde los investigadores pueden modificar la cantidad de recursos disponibles según sea necesario. AWS CLI ofrece una herramienta poderosa para la automatización de tareas a través de scripts y permite un acceso detallado a toda la gama de servicios de AWS y sus respectivas APIs. Amazon Web Services, 2024) Los servicios como AWS CloudTrail son fundamentales debido a su función como un registro de la actividad publicada dentro del entorno de AW (Amazon Web Services, 2016).

1.9.7.3 Limitaciones

El uso de las herramientas de AWS para el análisis forense en la nube depende del conocimiento específico y profundo de los servicios de AWS y de la AWS CLI. La recopilación de datos volátiles, como la memoria de las instancias EC2, solo es posible directamente en la instancia, lo que presenta desafíos logísticos y de preservación. El modelo de responsabilidad compartida en la nube significa que la capacidad de recopilar ciertos tipos de evidencia puede variar significativamente dependiendo del servicio de AWS específico que se esté investigando. La automatización de procesos es una ventaja; sin embargo, una implementación excesiva o mal configurada de procesos forenses automatizados podría llevar a la ejecución innecesaria de tareas, consumiendo recursos y tiempo sin un beneficio directo para la investigación. La falta de una única herramienta consolidada para el análisis forense en AWS significa que los investigadores probablemente necesitarán coordinar el uso de varios servicios y la AWS CLI para ensamblar un flujo de trabajo forense completo, lo que aumenta la complejidad (Amazon Web Services, 2016).

1.9.8 Azure CLI y Scripts de Auditoría

1.9.8.1 Aplicabilidad en la nube

La herramienta de línea de comandos Azure Command Line Interface (CLI) es una interfaz de línea de comandos que otorga a los usuarios la capacidad de administrar los recursos y servicios de la plataforma Microsoft Azure. En la nube, los administradores y desarrolladores pueden automatizar tareas, realizar cambios en la configuración de recursos y administrar la infraestructura Azure utilizando el símbolo del sistema en lugar de la interfaz de usuario basada en navegador. En el campo del análisis forense en la nube de Azure, la CLI es esencial para automatizar varias tareas relacionadas con la seguridad y la auditoría, que son fundamentales para recopilar y analizar evidencia digital. Azure también ofrece varios scripts de auditoría que se pueden utilizar a través

de la CLI para generar informes y analizar la actividad dentro de la plataforma. Estos scripts pueden estar destinados a permitir el registro de auditoría en un servicio específico, configurar reglas de firewall para identificar cualquier patrón de tráfico sospechoso y llevar a cabo otras operaciones relativas al análisis forense en la nube. Además, Azure también desarrolla varios servicios de seguridad como Azure Security Center y Azure Policy, que incluyen funciones específicas para la administración de la seguridad y el cumplimiento normativo. Incluso estos servicios pueden ser operados utilizando la CLI, permitiendo a los profesionales ajustar su postura de seguridad y recopilar información en función de la programación (Microsoft, 2024).

1.9.8.2 Ventajas

Una de las ventajas más importantes de usar Azure CLI y los scripts de auditoría para el análisis digital en la nube es que los investigadores pueden automatizar tareas repetitivas y administrar la infraestructura de Azure a través de scripts personalizados. Por lo tanto, los scripts ahorrarán una cantidad significativa de tiempo al recopilar datos relacionados con los incidentes en cuestión (Azure, 2024).

Como resultado, es más probable que los scripts ayuden a los investigadores a recopilar registros de actividad y encontrar comportamientos o eventos sospechosos que ayudarían a los investigadores a saber si hay un desglose de la seguridad o no. La integración de Azure CLI con la suite de seguridad de Azure, Security Center y Azure Policy, también les permitirá a los investigadores detectar y responder a las amenazas, según Microsoft. Además, mediante Azure CLI, los investigadores pueden configurar políticas de seguridad, analizar alertas e incluso consultar la postura de la seguridad de un entorno de nube (Microsoft, 2024). Además, esencialmente, la Azure CLI es de fuente abierta y, por lo tanto, se puede ejecutar en distintos

sistemas operativos, lo que brinda flexibilidad que necesitan los equipos de investigación, ya que sus miembros pueden estar en distintos sistemas operativos.

1.9.8.3 Limitaciones

Azure CLI para forenses en la nube se beneficia del uso efectivo de CLI, que a su vez requiere un entendimiento efectivo de la propia CLI y los servicios de Azure a nivel de plataforma, algunos de los cuales ofrecen estos servicios. Esto significa igualmente que, para la aplicación efectiva de scripts de auditoría, los registros relevantes deben estar disponibles y adecuadamente configurados dentro de los servicios de Azure. Donde los registros necesarios no son habilitados o ya no están disponibles y/o mantenidos en la longitud requerida, los scripts de auditoría como base para la forense no serán necesaria. Además, la estructura de Azure en sí, que incluye conceptos como cuentas raíz, suscripciones y grupos de recursos, a menudo puede ser complicada y requiere la familiaridad efectiva del usuario para aplicar la CLI de una manera que puede guiar una investigación forense. A diferencia de la mayoría de las herramientas comerciales anteriores, que eran todas dedicadas (Azure, 2024).

1.9.9 Google Cloud CLI y Stackdriver

1.9.9.1 Aplicabilidad en la nube

En resumen, el gcloud CLI es un conjunto de herramientas de línea de comandos que permiten a los usuarios administrar los recursos y las aplicaciones alojados en la plataforma de Google Cloud Platform. Esta interfaz es un medio eficiente de interactuar con los servicios de GCP y permite a los administradores y desarrolladores realizar configuraciones, implementaciones y tareas de administración de recursos directamente desde la terminal.

Por otro lado, Stackdriver, ahora conocido como parte de Google Cloud Observability, es un servicio de monitoreo, registro y diagnóstico completo que se ofrece para la plataforma GCP. Una vez más, en el contexto de la nube GCP, la gcloud CLI se puede usar para interactuar con Stackdriver Logging y Stackdriver Monitoring, llamados ahora Cloud Logging y Cloud Monitoring, para recopilar información necesaria para una investigación de seguridad. Por ejemplo, esta interfaz se usa para consultar y extraer registros de Stackdriver Logging. Estos registros contienen el log de aplicaciones y servicios que se ejecutan en GCP y luego se analizan en busca de actividades sospechosas. Además, la gcloud CLI también se usa para administrar otros servicios GCP aplicables a la ciberseguridad, por ejemplo, Cloud Identity and Access Management y Security Command Center, también conocido como plataforma de gestión de seguridad y riesgo GCP (Google Cloud, 2024).

1.9.9.2 Ventajas

Por otro lado, una de las ventajas de la gcloud CLI es que "proporciona una interfaz de línea de comandos consistente para los mismos servicios de Google Cloud y se administran a través de la consola web de Cloud". Así, los investigadores pueden elegir la herramienta que mejor se adapte a sus necesidades en diferentes situaciones: la GUI o la CLI para la automatización y el scripting. Además, otra ventaja de Stackdriver Logging radica en "un log centralizado para toda la infraestructura de GCP". Dado que los eventos pueden estar dispersos entre diferentes servicios y registros, esta característica puede facilitar la correlación entre los eventos. En cuanto a otra nube CLI, gcloud "también le permite automatizar la ejecución de tareas de Cloud Storage a través de scripts que puede incorporar en Archivos por lotes o Planificadores de tareas de Windows". Es esencial para operar y administrar recursos en la nube a gran escala, incluso para implementar flujos de trabajo forenses personalizados.

Stackdriver Monitoring, por su parte, permite a los usuarios “crear métricas personalizadas basadas en registros recopilados”. Por lo tanto, es posible monitorear eventos específicos y crear alertas para ciertos comportamientos que podrían indicar actividad no deseada. Aparte de eso, “Google Cloud’s Security Command Center colecciona servicios relacionados con la seguridad a través de Stackdriver”. Se ha mencionado anteriormente que gcloud se integra con Stackdriver, y Security Command Center proporciona una vista unificada y centralizada de los riesgos en la plataforma de GCP. Puede ser beneficioso recopilar información de seguridad y eventos durante la encuesta para obtener un panorama de posibles incidentes y la postura de aseguramiento (Google Cloud, 2024).

1.9.9.3 Limitaciones

Un punto crucial sobre la efectividad de gcloud CLI en el análisis forense en la nube es que se requiere conocimiento especializado y detallado sobre la CLI y los servicios de Google Cloud para utilizar esta plataforma eficientemente. La gcloud CLI contiene una amplia variedad de comandos y opciones, cuyo aprendizaje pueden ser críticos para los usuarios que no están familiarizados con ella. Aunque el Security Command Center de GCP proporciona una visión centralizada de la seguridad, su cobertura de monitoreo puede no ser completa en todos los servicios de GCP o sus integraciones. En estos casos, otras herramientas pueden necesitarse para obtener visibilidad.

Por último, es fundamental configurar correctamente los registros en Stackdriver para asegurarse de que la información forense relevante esté disponible y sea accesible para el análisis. Si los registros no están configurados correctamente, o si las políticas de retención no permiten

mantener los registros determinados para el diagnóstico forense, no se podrá realizar un análisis forense completo (Google Cloud, 2024).

Tabla 3

Fortalezas y Debilidades de Herramientas Forenses Aplicadas en la Nube

Herramientas forenses en entornos de computación en la nube: fortalezas y debilidades, aplicabilidad y casos de uso					
Herramienta / Concepto	**Aplicabilidad en la nube**	**Fortalezas (en nube)**	**Limitaciones (en nube)**	**Casos de uso típicos**	**Requisitos / Notas**
Cloud Forensics (concepto marco)	IaaS/PaaS/SaaS; evidencia distribuida (CSPs, regiones, cuentas)	Enfoque integral: identificación, recolección, preservación, análisis, presentación	Retos legales/jurisdicción, propiedad de datos, retención y formato de logs	Investigaciones de violaciones de datos, fraude, intrusiones	Alineación legal; coordinación con CSP; cadena de custodia estricta
TSK / Autopsy	Indirecta en nube (vía imagen de VM/volumen: EBS, discos virtuales)	Código abierto, extensible; análisis filesystem; timeline, carving, artefactos web	Requiere imagen previa; rendimiento con grandes volúmenes; compatibilidad FS limitada en algunos casos	Análisis de snapshots/volúmenes (EBS) convertidos a imagen; recuperación de archivos, timeline	Necesita snapshot/imagen + hashes; trabajo offline sin tocar producción
Volatility / Rekall	IaaS con volcado de RAM (si el CSP/instancia lo permite)	Visibilidad de procesos, conexiones, credenciales en memoria; detección de malware in-memory	Difícil adquirir RAM en nube; Rekall sin mantenimiento; alta pericia	Respuesta a incidentes en vivo; detección de fileless/credenciales en RAM	Acceso root/agent; ventana de tiempo corta; preservar integridad del dump

log2timeline / Plaso / Timesketch	Procesa logs cloud (CloudTrail/Azure/GCP) y fuentes mixtas	Super timelines; colaboración y búsqueda (Timesketch); extensible por parsers	Preprocesar/convertir formatos; alto volumen de logs puede exigir recursos	Correlación de eventos entre servicios cloud y SO; reconstruir incidentes	Exportar logs (S3/Cloud Logging, etc.); gobernanza de retención
EnCase (OpenText)	Amplio: endpoints, móviles y artefactos cloud; despliegue en nubes públicas	Motor potente, reporting; EnScript (automatización); IA/ML para priorizar evidencias	Licenciamiento; complejidad; dependencias legales/privacidad; cifrado	Casos corporativos grandes; eDiscovery + evidencia híbrida (local/cloud)	Cooperación CSP; credenciales /órdenes; infraestructura para procesado
FTK (Exterro)	Análisis de datos extraídos de cloud; FTK Lab para carga distribuida	Muy eficiente en grandes volúmenes; indexación, data carving; detección de malware (Cerberus)	Licenciamiento; capacidades cloud específicas pueden requerir preparación previa	Procesar masivamente evidencia (discos, correos, dumps) proveniente de cloud	Preparar datos en formatos compatibles; FTK Imager (adquisición)
Magnet AXIOM / AXIOM Cloud	Adquisición directa de fuentes cloud (iCloud, Google, O365, OneDrive, WhatsApp, etc.)	Cobertura amplia de cuentas/nubes; panel Cloud Insights; flujo unificado móvil/PC/cloud	Licenciamiento; cambios de APIs requieren actualización; dependencia de permisos/órdenes	Casos con cuentas en la nube y mensajería; correlación multi-fuente	Credenciales /tokens u orden judicial; buenas prácticas de preservación

AWS nativas + AWS CLI	CloudTrail, CloudWatch, GuardDuty, Detective, S3, EBS, IAM	Integración nativa; automatización (CLI/Lambda/ Step Functions); escalable; responsabilidad compartida	Curva de aprendizaje; memoria de EC2 no nativa; responsabilidad compartida	Exportar CloudTrail, preservar snapshots EBS, automatizar colecta	IAM mínimo necesario; versionado/retención en S3; etiquetado forense
Azure CLI + scripts de auditoría	Azure Logging, Security Center/Defender, Policy; recursos por suscripción	Automatización de auditoría y postura; integración con servicios de seguridad	Complejidad de estructura Azure (tenant/suscripción/RG); logs mal configurados	Habilitar/extraer auditoría, revisar alertas y conformidad	Asegurar diagnostic settings y retención; permisos RBAC adecuados
gcloud CLI + Cloud Logging/Monitoring (Stackdriver)	Cloud Logging/Monitoring, IAM, SCC (Security Command Center)	Logging centralizado; scripting/automatización; alertas y métricas	Requiere buena configuración/ retención; cobertura SCC no siempre total	Consultar y correlacionar logs GCP; telemetría de incidentes	Políticas de retención correctas; cuentas de servicio/roles mínimos
Procedimientos: Preservación & Cadena de Custodia	Transversales a todo modelo (IaaS/PaaS/SaaS)	Garantizan admisibilidad: integridad (hash), trazabilidad, control de acceso	Exigentes en disciplina/tiempo; errores invalidan evidencia	Todo caso: aislar, snapshot/dump, hash, documentar, encadenar	Actas firmadas, hashes SHA-256/512, bitácora, oficios/órdenes

Nota. Elaboración propia con base en documentación técnica y literatura de informática forense (Carrier, 2005; Brezinski & Killalea, 2002; Case et al., 2014; Google Cloud, 2023; Microsoft, 2023; Amazon Web Services, 2023; OpenText, 2023; Exterro, 2023; Magnet Forensics, 2023).

CAPÍTULO II: ANÁLISIS Y DISEÑO

INTRODUCCIÓN

La investigación forense en la nube se ha vuelto compleja debido a que la mayoría de las organizaciones que se dedicaban a almacenar información ya no lo hacen debido a la computación en la nube, la cual almacena sus datos en diferentes partes del mundo mediante terceros. Aparte, la computación en la nube, especialmente la privada, debe procesar una gran cantidad de operaciones por segundo, lo que hace que la digitalización sea insuficiente e inapropiada para las áreas específicas, las naciones y el acceso físico a los medios de almacenamiento que debe investigarse digitalmente. En el caso de mi país, no se cuenta con una estructura metodológica que oriente la investigación forense en entornos computacionales en la nube.

2.1 Análisis de requerimientos

Para iniciar la fase de requerimientos, se realizó una entrevista programada con dos profesionales de la Fiscalía General del Estado involucrados en el análisis forense en la nube. La entrevista identificó los estándares internacionales reconocidos, las herramientas especializadas y los mejores procedimientos para realizar investigaciones forenses en entornos de cómputo en la nube. Posteriormente, con base en esta información, fue posible definir los requerimientos funcionales para la planificación y el diseño, así como la construcción de la guía que se propone en la materia.

2.1.1 Requerimientos funcionales

Para cada requisito se establece el siguiente formato:

Tabla 4

*Requerimientos Funcionales (RF*01*)*

Número de requisito	RF01
Nombre de requisito	La guía debe contar con una estructura adecuada, entendible para seguir el procedimiento del análisis forense en la nube.
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la fiscalía general del Estado
Prioridad del requisito	☐ Alta/Esencial ☒ Media/Deseado ☐ Baja/ Opcional

*Requerimientos Funcionales (RF*02*)*

Número de requisito	RF02
Nombre de requisito	La guía debe detallar un protocolo apropiado para el manejo eficiente de la evidencia digital.
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la fiscalía general del Estado
Prioridad del requisito	☒Alta/Esencial ☐Media/Deseado ☐ Baja/ Opcional

*Requerimientos Funcionales (RF*03*)*

Número de requisito	RF03
Nombre de requisito	La guía debe incluir procedimientos bajo normas y estándares internacionales que permita la investigación forense en la nube.
Tipo	X Requisito ☐ Restricción

Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☒Alta/Esencial ☐Media/Deseado ☐ Baja/ Opcional

*Requerimientos Funcionales (RF*04*)*

Número de requisito	RF04
Nombre de requisito	La guía debe estar alineada con la normativa legal ecuatoriana vigente.
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☒Alta/Esencial ☐Media/Deseado ☐ Baja/ Opcional

*Requerimientos Funcionales (RF*05*)*

Número de requisito	RF05
Nombre de requisito	La guía debe listar los tipos de delitos informáticos más frecuentes en la web.
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☐Alta/Esencial ☒Media/Deseado ☐ Baja/ Opcional

*Requerimientos Funcionales (RF*06*)*

Número de requisito	RF06
Nombre de requisito	Se debe integrar en la guía las mejores herramientas para el análisis forense en la nube

Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☒Alta/Esencial ☐Media/Deseado ☐ Baja/ Opcional

*Requerimientos Funcionales (RF*07*)*

Número de requisito	RF07
Nombre de requisito	La guía debe establecer las plantillas y formatos adecuados para llevar el control en el proceso del análisis forense en la nube
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☐ Alta/Esencial ☒Media/Deseado ☐ Baja/ Opcional

*Requerimientos Funcionales (RF*08*)*

Número de requisito	RF08
Nombre de requisito	Validar la guía por un perito informático.
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☐ Alta/Esencial ☒Media/Deseado ☐ Baja/ Opcional

Se detallan los requerimientos funcionales esenciales que la guía debe satisfacer:

1. **RF01:**

Esto significa establecer con total claridad la organización del grupo de trabajo destinado a investigar con la asistencia forense. En otras palabras, es necesario establecer los límites de la responsabilidad de todas las personas involucradas en el equipo, incluidas las que conocen la ciencia y las que conocen la ley. La organización es, sin duda, necesaria para garantizar una organización adecuada, la capacidad de trazar cada operación realizada y, por supuesto, para asegurarse de que esta operación no se vea interrumpida.

Acciones:

No solo identificará quién es quién en el proceso, sino que también detallará qué hace cada persona en particular. Imagínese, por ejemplo, el Coordinador Forense, quien estará a cargo de administrar y supervisar todo el procedimiento, mientras que, en otra esquina, el Analista Forense Digital se dedicará a indexar y entender cada una de las coordenadas técnicas a su disposición. El Especialista en Infraestructura Cloud, a su vez, usará su conocimiento para asesorar sobre cómo y de dónde tomar los registros que sean de interés. Claro está que el responsable legal será el encargado de asegurarse de que no se salga la esfera de lo permitido. Su abogado también tendrá la tarea de ser mentor en cuestiones legales.

Por último, pero igual de importante, el Custodio de la Evidencia será quien reciba, marque, almacene y proteja a capa y espada el material. La guía también contará con algún tipo de diagrama o gráfico que ayudará a mostrar de forma clara las relaciones de reporte. De esta forma, será sencillo identificar cómo y quién se reporta a quién.

2. **RF02**

En este sentido, la meta es ineludible: debemos sentar procedimientos meticulosos que cubran cada una de las fases del manejo de evidencia digital en entornos de nube. Es decir, debemos ocuparnos desde el instante mismo en que se identifican y recogen las pruebas, hasta el momento en que se preservan, trasladan, almacenan y, finalmente, eliminan de ellos. Todo esto con la finalidad de garantizar la integridad de esta evidencia, y la congruencia y unicidad de la cadena de custodia que la acompaña a lo largo de todo el camino.

Acciones

- Cómo se realiza la cadena de custodia: la creación de un código único para cada elemento de prueba, el etiquetado, el embalaje cuidadoso y el registro documental detallado.
- Estándares para los principales documentos. Esto incluye actas de incautación, bitácoras de manipulaciones y registros fotográficos del estado de las pruebas.
- Apreciar claramente lo que se necesita hacer para preservar la evidencia como se describió necesario. Esto incluiría el uso de hashes de verificación, la seguridad de los contenedores relevantes y la constante supervisión de las condiciones ambientales, incluidas la temperatura de la sala y la humedad.
- Procedimientos bien definidos para un transporte seguro. Bajo este elemento, se contempla el uso de sellos inviolables, la necesidad de que la evidencia esté acompañada por personal autorizado, y las rutas definidas y seguras.
- Controles periódicos para asegurar la integridad de la evidencia. Por ejemplo, el rehashing y completa comparación de registros existentes.

Además de todo lo anterior, y esto ya es crucial, la guía añade una implantación de un procedimiento plenamente estandarizado conforme con la regulación en nubes internacionalistas.

3. **RF03**

La guía debe presentar una metodología estandarizada, basada en estándares internacionales y buenas prácticas.

Acciones

- Cada una de las fases del proceso forense, a saber, la preparación, adquisición, preservación, análisis y presentación, se mapeará cuidadosamente, es decir, se asociará directamente con los requisitos formulados en los estándares internacionales correspondientes.
- Se traerán instancias de diagramas de flujo, mostrando los puntos críticos de decisión, especialmente relevantes en escenarios donde se utilizan servicios tradicionales como Infraestructura como Servicio IaaS, Plataforma como Servicio PaaS y Software como Servicio SaaS.
- Se añadirían listas de verificación (checklists) que faciliten las auditorías internas, de tal forma que garantice su concordancia con los procedimientos registrados.

4. **RF04**

Todos los procedimientos sobre los que versa esta guía deben ser guardados con ajuste respecto al Código Orgánico Integral Penal, la Ley orgánica de datos personales y cualquier otra normativa nacional aplicable. Esto nos asegurara que la adquisición y el manejo de la evidencia digital se llevara a cabo bajo los estándares de la legalidad, la proporcionalidad y el debido proceso.

Acciones:

- En ese sentido, serán identificados y mencionados de manera específica aquellos artículos presentes en el COIP y en la normativa de protección de datos personales que se proyecten más relevantes en relación a las tareas de recolección y análisis de evidencias.

5. **RF05**

Además, la guía deberá presentar, compilar y describir los tipos de delitos informáticos más comunes en el ámbito ecuatoriano. Me refiero a casos como el phishing, ransomware, estafas en línea y diversos tipos de accesos no autorizados, por mencionar algunos. En resumen, este propósito se traduce en proporcionar una estructura, un contexto claro y cuatro glosarios suficientes de qué y cuáles son los tipos de ataques para acumular y recolectar la evidencia de manera más eficaz.

Acciones

- Para ello, además, se tomarán datos estadísticos de fuentes oficiales, como también de organismos especializados, con el propósito de estimar qué tipos de delitos cibernéticos seleccionaremos para confeccionar la guía, de acuerdo a la real sequedad con que se presente cada uno.

6. **RF06**

Por otra parte, un capítulo imprescindible de la guía se refiere a un catálogo de herramientas forenses comúnmente usadas: Magnet AXIOM, Autopsy, Volatility, AWS CloudTrail Insights y similares. Las herramientas serán clasificadas no solo por su eficacia presentada, sino también por disponibilidad en la nube y, lo que es más importante, la cantidad y dureza de uso en las cortes de justicia.

Acciones

- Por otro lado, se expondrá una matriz comparativa detallada de las prestaciones de las

herramientas. En ella, se podrá encontrar la plataforma, el licenciamiento, la clase de evidencia y la facilidad de uso que soportan.

- Además, en función de los mencionados documentos, serán preparadas guías de instalación y configuración, a saber, paso a paso para los sistemas operativos Windows, Linux y macOS.

7. **RF07**

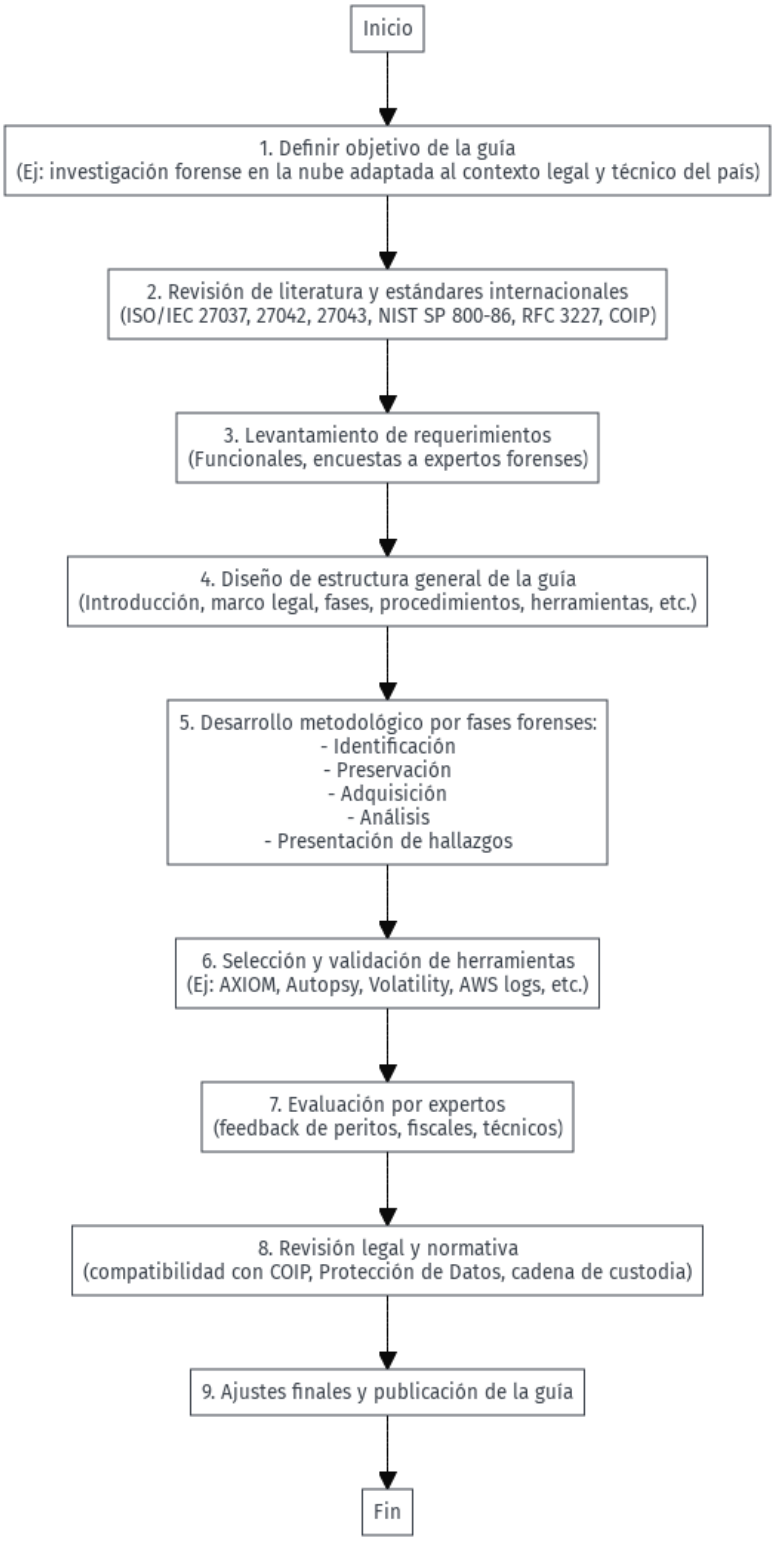
Otra característica vital de esta guía es el suministro de plantillas ya estandarizadas como formularios, checklists, y bitácoras. El único objetivo detrás de esto es simplificar drásticamente las abrumadoras tareas de documentación y de llevar un registro de toda actividad forense en la nube. De tal manera, intentaremos asegurarnos de que dichas tareas sean consistentes, completamente trazables y actúen como chequeos de casos accesibles de buenas prácticas.

Acciones

- Asignar formatos específicos a la cadena de custodia, el plan de recolección de evidencia, el registro de logs, los documentos resultantes del análisis e informe final del caso.
- Establecer los campos de llenado obligatorio. Se establecerán recomendaciones claras si son seleccionados a continuación para evitar cualquier omisión posible que condujera a un resultado crítico.
- Con la validación de las plantillas por peritos de la Fiscalía y el ajuste en su vocabulario técnico-jurídico para que se adecue al uso local.

Ilustración 1

Diagrama de flujo para el diseño de guía metodológica para el análisis forense en la nube



2.2 Diseño de la guía metodológica

Este proyecto tiene como objetivo clave facilitar la gestión eficiente de las investigaciones forenses en informática que ocurran cada vez con mayor frecuencia en los intrincados sistemas de nube. Aquí, la estrategia sistemática descrita se basa en pautas globales amparadas por el consenso en el ámbito de la informática forense. Permiten asegurar la exactitud técnica del proceso, la posibilidad de replicar cada acción realizada y, muy importante, la legitimidad procesal absoluta de la investigación.

A la vez, se prestó especial atención a hacerla pertinente para la situación tecnológica y el marco legal que existen en la República del Ecuador. Antes de seguir adelante con el desarrollo de la guía, fue necesario emprender un estudio comparativo detallado de las guías internacionales más destacadas para investigaciones digitales, con énfasis en las dirigidas a entornos de nube. Para esto, se realizaron encuestas y preguntas directas a los peritos de la fiscalía general. Por lo tanto, los datos aportados por estos profesionales fueron indispensables para comprender tanto sus preferencias como las deficiencias prácticas que presentan a diario en la práctica nacional.

2.2.1 Análisis comparativo de estándares

- ISO/IEC 27037:2012. Bueno, este en realidad es un estándar que proporciona ciertas directrices. Sí, directrices, pero, en realidad, son muy claras y, al mismo tiempo, notablemente detalladas. Específicamente, estamos hablando de directrices relacionadas con la identificación, recolección, adquisición y preservación preliminar de la evidencia digital. Su relevancia, la verdad, no se puede discutir, especialmente si nos referimos a la primera fase en cualquier investigación realizada. La razón es que asegura que la cadena de custodia está en su lugar y la integridad de la evidencia, en última instancia, se mantiene intacta desde el primer contacto. Esto, por cierto, debe mantenerse para que la evidencia

sea admisible en la corte.

- ISO/IEC 27042:2015: Este es un buen complemento para el estándar anterior. Aparte de la guía detallada sobre todo el proceso, esta norma proporciona orientación para otra etapa, un examen y análisis exhaustivo de la evidencia digital previamente recopilada. Para ser honesto con ustedes, este estándar no solo ayuda, sino que permite un proceso de reconstrucción completo y minucioso del evento digital asociado con el incidente bajo auditoría. Claramente, juega un papel crítico en los escenarios de la corte.
- NIST SP 800-86: Si hay algo que distinga a este estándar, es su enfoque completamente operativo. SP 800-86 es lijado con la mano de alguien que tiene la intención de reaccionar a cualquier incidente de seguridad por computadora que pueda surgir. Cubre todo, desde la recolección y el examen de la información; las siguientes etapas de análisis y hasta la formulación de informes finales. La joya de este estándar, sin embargo, radica en el gran detalle de los procedimientos que ofrece. Además, SP 800-86 es un campeón auténtico de la integración de equipos técnicos y legales en la mitigación de incidentes.

Tras todo el análisis comparativo, y con el muy especial peso que tuvieron los resultados de las encuestas a los expertos forenses de la Fiscalía, la conclusión fue clara: indiscutiblemente, el estándar ISO/IEC 27037:2012: Este se destacó como a enorme distancia la opción más recomendable para esa fase inicial de adquisición y preservación de la evidencia digital. ¿Por qué se puntuó tanto esta posibilidad? Fue muy valorado tanto por su gran especificidad técnica a este respecto, como por su claridad metodológica, y también, sí, su enorme aceptación dentro del ámbito judicial ecuatoriano. Del mismo modo, para cuando se aplique ese análisis técnico más completo, quedó completamente clara la conveniencia de combinar con puntos específicos la ISO/IEC 27042:2015. Y no solo eso, también quedó totalmente garantizado que utilizar NIST SP

800-86 era fundamental, y que, perfectamente aplicado, articulaba de forma notablemente eficaz tanto las acciones más operativas como las legalmente indicadas.

¿La herramienta especializada? Por mucho, y conforme a la encuesta, fue Magnet AXIOM el software más indicado y efectivo. Grandes posibilidades indicadas fueron su capacidad para mantener la integridad de la evidencia digital, su total posibilidad de conectarse con casi cualquier infraestructura cloud y el enorme y fácil reporte que genera: un reporte, por otro lado, así vale la pena recalcarlo, altamente especializado técnicamente y 100 % válido legalmente.

2.3 La estructura de la guía metodológica

La presente guía metodológica se estructura utilizando un formato muy claro y, a su vez, en mi opinión, bastante coherente. De hecho, esta forma está diseñada para abordar todos los elementos fundamentales de una investigación forense en la nube de manera sistemática. Más específicamente, nuestra guía se desglosa de la siguiente manera:

2.3.1 Introducción

En esta primera sección se presentan varios puntos clave que brindan al lector una visión contextual clara:

- Por último, otra sección relacionada con esta guía es la justificación, que debería explicar por qué se necesita desarrollar este proyecto, al mismo tiempo que resalta el vacío en la práctica forense digital en Ecuador.
- Los objetivos generales y específicos que fundamentan la creación de la metodología propuesta.
- Referencias a normas internacionales que son base para la metodología (ISO/IEC 27037:2012, ISO/IEC 27042:2015, NIST SP 800-86).

- Breve resumen del marco legal ecuatoriano aplicable, con énfasis en el Código Orgánico Integral Penal, la Ley Orgánica de Protección de Datos Personales y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

2.3.2 Alcance

Finalmente, se procederá a señalar de una vez por todas los límites y la aplicabilidad de nuestra guía metodológica. Por decirlo de alguna manera, hasta dónde llega y para qué sirve:

- Indicar la aplicación de la guía en los diferentes modelos de servicio en la nube: Infraestructura como Servicio, IaaS, Plataforma como Servicio, PaaS y Software como Servicio, SaaS.
- Identificar los principales proveedores cloud asegurados en relación (con referencia a Amazon Web Services – AWS; con menciones a Microsoft Azure).
- Esta página se aplica a la guía de diseño del Centro de Datos Definido basada en Microsoft. Confirme la totalidad de la guía también es compatible con arquitecturas híbridas y también con entornos de nube privada.

2.3.3 Roles y responsabilidades

Este es el escenario final donde se abordarán, con claridad intransigente, los roles específicos que se necesitan o se exigen en un escenario de investigación forense en la nube, o en una escena crítica, por decir lo que haga falta. Al mismo tiempo, ellos abordarán las responsabilidades específicas de todo lo recién mencionado. Habrá:

- **Coordinador Forense (Líder de Investigación):** Sera quien tendrá la gran tarea de llevar a cabo la revisión de todo el proceso y, evidentemente, la de autentificar los documentos que se generen al final.

- **Analista Forense Digital:** ejecutar técnica y recursos necesarios para realizar los análisis a través de la recolección y la preservación de la evidencia.
- **Especialista en Infraestructura Cloud:** Su área de acción abre todas las posibilidades, su rol es vital, brindar soporte técnico en el acceso y la extracción de datos directamente desde los entornos de nube.
- **Responsable Legal / Asesor Jurídico:** La persona que realiza la siguiente función debe: "tomar todas las medidas necesarias para garantizar el cumplimiento de todos los aspectos legales en cada una de las etapas del proceso de investigación".
- **Custodio de la Evidencia:** El titular del perfil es responsable de la administración y garantía del almacenamiento y transporte de la evidencia digital, así como de su manejo adecuado, manteniendo la cadena de custodia intacta y sin fallas.

2.3.4 Marco legal aplicable

El presente segmento de guía se ofrece para introducir de una manera muy directa, el marco normativo sin el cual, en ningún caso, se pueden violar todos los aspectos de todo el proceso forense. Es vital para el aspecto de la validez de la ciencia:

- La Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP).
- La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- La Ley Especial de Telecomunicaciones.
- El Código Orgánico Integral Penal (COIP).
- La Ley Orgánica de Protección de Datos Personales (LOPDP).

Se presentará un breve análisis de referencia para cada una de estas directrices antes mencionadas, con lo cual se quiere decir directamente sobre cómo y en qué medida afectan estos procedimientos en relación con cómo obtener y tratar con la evidencia digital en la nube.

2.3.5 Protocolo detallado de acceso y extracción de evidencia

Esta es una de las partes más importantes. Se describirán de manera estricta y detallada los pasos secuenciales que, sin falta, se seguirán para asegurar la adquisición y el mantenimiento adecuados de la evidencia digital en las investigaciones en la nube. Este es un aspecto crítico que no debe pasarse por alto.

- **Detección inicial del incidente:** Se identificarán claramente los mecanismos y los criterios establecidos para determinar qué eventos son sospechosos.
- **Identificación técnica de servicios y activos involucrados:** Se explicará la forma de cómo crear un inventario claro y altamente específico de los recursos de la nube que podrían ser vulnerables.
- **Obtención formal de autorización legal:** Un procedimiento legal que no se puede negociar es el necesario para asegurarse de que el acceso a los datos en la nube sea completamente legal.
- **Congelamiento (*Legal Hold*) y notificación al proveedor cloud:** En este apartado se describirán los pasos, con alta especificidad, para realizar el "congelamiento" de la evidencia en el ambiente del proveedor de la nube, como por ejemplo AWS, entre otros.
- **Extracción controlada y verificable de la evidencia:** A continuación, se mostrarán las técnicas detalladas de descarga segura, y es imprescindible agregar, verificables de los

datos. También incorporaremos el uso de hash como SHA-256, SHA-512 para asegurar su integridad.

- **Transferencia segura y custodia rigurosa:** Se explicará la cadena de custodia con la que se debe realizar el proceso completo de almacenaje y traslado de la evidencia anteriormente descrita, garantizando que no haya ningún desliz.
- **Análisis forense especializado en laboratorio controlado:** Se dibujarán las pautas específicas mediante las cuales realizar un análisis técnico exhaustivo, utilizando siempre herramientas forenses especializadas y, por supuesto, en un entorno seguro y debidamente controlado.
- **Cierre formal del caso y archivo definitivo de la documentación:** Una vez finalizada la investigación, se abordará el proceso de conclusión formal. Consta de la redacción del reporte final y de la documentación de todos los procesos cumplidos.

2.3.6 Acceso a dispositivos sincronizados

La evidencia especial es cuando la evidencia digital no solo se almacena en la nube, sino también en dispositivos personales que están sincronizados con ella. ¿Cómo manejamos eso?

- Se dibujará la descripción del procedimiento legal específico para la obtención de acceso y la autorización judicial explícita necesaria, ya que no podemos proceder sin ella.
- Se presentará la técnica forense destinada a la adquisición y mantenimiento de la integridad de las imágenes digitales provenientes de dispositivos sincronizados con servicios cloud.

2.3.7 Análisis técnico de herramientas forenses

En este punto, nos dedicaremos a describir las herramientas especializadas que hemos elegido para las investigaciones en entornos cloud. Pondremos un énfasis particular en sus capacidades y sus puntos más fuertes:

- **Magnet AXIOM Cloud:** En este sentido, daremos una descripción de las capacidades del producto, las fortalezas; estas últimas serán específicas para los entornos SaaS la compatibilidad con las diversas plataformas y cómo genera, de hecho, los informes forenses.
- **FTK Imager:** Presentaremos un análisis sobre sus habilidades técnicas para la obtención de imágenes forenses. Tal como para el manejo seguro de evidencias procedentes de entornos cloud.
- **Otras herramientas complementarias:** Además, mencionaremos algunas otras herramientas, que, a pesar de no ser las principales, es beneficioso tenerlas en consideración. Son las siguientes: AWS CloudTrail, que es útil para la auditoría de logs, X-Ways Forensics, Cellebrite UFED Cloud y Velociraptor.

2.3.8 Consideraciones técnicas y legales para el uso de herramientas

Este apartado se dedicará a detallar aspectos que son cruciales. Su fin es asegurar que el uso de las herramientas forenses digitales en la nube sea siempre el correcto, legalmente aceptable y técnicamente válido.

- Se requiere la plena libertad en las condiciones legales de licenciamiento y, no menos importante, la necesidad de mantener las actualizaciones requeridas.
- Detalladas directrices para documentar cada acción realizada con las herramientas. La

documentación es crucial aquí.

- Exigir requisitos muy específicos para la validación técnica de los resultados que se obtengan. Esto es para garantizar, sin lugar a dudas, la admisibilidad jurídica.
- Haber adoptado los procedimientos de obligado cumplimiento para preservar, de manera estricta y sin excepciones, la cadena de custodia.

2.3.9 Formatos y plantillas forenses

Por último, un conjunto de herramientas de documentación que ya están estandarizadas. No es nada más que garantizar la uniformidad, la claridad y una trazabilidad completa en todo el procedimiento forense.

- Una plantilla oficial para la cadena de custodia digital.
- Un modelo de bitácora forense para un registro continuo de todas las actividades.
- Después, una lista de verificación oficial, para garantizar que todos los procedimientos sean realizados con la disciplina necesaria.
- Un formato estandarizado de Informe Técnico Final para la entrega de los resultados a las instancias judiciales y administrativas correspondientes.

CAPITULO III: DESARROLLO E IMPLEMENTACIÓN

3.1 Desarrollo de la guía metodológica

En este capítulo se describe la construcción de una guía metodológica para el análisis forense sobre la nube de computación, tomando en cuenta los antecedentes identificados en los capítulos anteriores. Dado que, al establecer la problemática, se encuentran con la carencia de un protocolo único para la realización de peritajes cibernéticos, lo que podría traducirse en prácticas poco homogéneas, pérdida de evidencia o inutilización de la prueba durante el enjuiciamiento, el marco conceptual se hace necesario, ya que el uso de servicios en la nube es cada vez más generalizado y complicado por los desafíos ya mencionados para la investigación pericial. La guía propuesta cerrará la brecha existente, al consolidar un procedimiento técnico-científico que sea fundamentado con estándares internacionales y adaptado a la legislación nacional.

Fase de desarrollo: La preparación de la guía siguió una lógica por etapas. Primero, se realizó una revisión bibliográfica de los marcos normativos y las mejores prácticas en la informática forense. Estos literales se limitaron a detectar los principios básicos a incorporar, por ejemplo: preservación de imágenes forenses, documentación completa y las etapas forenses clásicas. Además, durante la etapa I se realizaron entrevistas a peritos forenses nacionales que hubiesen tenido experiencia en incidentes Cloud. Los expertos hicieron hincapié, entre otras cosas, en la necesidad de actuar siempre de acuerdo con los canales legales para la cooperación con los proveedores y no intentar en ningún caso acceder a los datos no disponibilizados en la nube. “Nosotros no podemos acceder a la base de datos de una gran empresa con la misma seguridad seguramente que uno de sus empleados. Se trabaja con la empresa dueña de la información con las debidas formalidades legales, me refiero”, contextualizó uno de los peritos. “Lo que se hace, principalmente, es coordinar con las compañías que tienen la posición jurídica frente a ese proveedor de servicios Cloud, y ellos nos autorizan judicialmente a realizar la investigación

forense", añadió. Este tipo de entrevistas permitió detectar los primeros requerimientos de la guía: clara necesidad de poseer procedimientos estándar por cada fase forense, un kit de herramientas individual para ambientes virtualizados, consideraciones jurisdiccionales y un nuevo protocolo de la cadena de custodia.

Con toda la información recolectada, se procedió con el diseño estructural y contenido de la guía. Para ello, se establecieron las fases forenses aplicables al entorno cloud: identificación, preservación, recolección/adquisición, análisis, presentación, respetando la lógica secuencial ya consagrada a nivel internacional. En este orden, para cada fase, se definió objetivos, actividades, responsables y productos esperados. Adicionalmente, se incluyeron roles y responsabilidades específicas del equipo de respuesta forense en la nube – por ejemplo, coordinador forense, analista cloud, asesor legal, custodio de evidencia –, garantizando que la distribución de tareas y los controles cruzados minimicen los errores y aseguren la imparcialidad del proceso. Por último, se incluyeron plantillas editables – por ejemplo, formularios de cadena de custodia y bitácora forense –, para otras actividades: documentar cada paso. Esto implica que la guía se pensó desde su inicio para ser completamente trazable: Cada movimiento en la evidencia, declaraciones y acciones, está registrado y puede ser auditado o validado judicialmente.

Otro aspecto crucial del desarrollo es la adaptación del documento al marco normativo nacional. Para ello, se revisaron las leyes ecuatorianas pertinentes, principalmente el Código Orgánico Integral Penal y normativa sobre la evidencia digital. Entre los más específicos se encuentran el Art. 502 – 505 del COIP que requieren preservar la cadena de custodia de la evidencia digital de la obtención a la presentación del caso. Además, se tuvo que considerar la Ley de Protección de Datos Personales y la Ley de Comercio Electrónico, en especial, la relativa al manejo de datos sensibles y los permisos requeridos para acceder a información en la nube. Por

ejemplo, se estableció que cualquier dato obtenido de un servicio cloud debe de presentar un permiso judicial o el consentimiento informado del dueño de la cuenta, asegurando que la evidencia obtenida sea legal. Todos estos y otros requerimientos normativos fueron integrados en el documento final, asegurando que los procedimientos propuestos por el usuario sean válidos en el contexto ecuatoriano.

En conclusión, la estructura de contenidos de la guía fue fijada. Los ejes temáticos de los capítulos van desde los fundamentos como la introducción, objetivos, alcance y definiciones, hasta las directrices prácticas como los procedimientos por fase, las herramientas recomendadas y consideraciones especiales. Se conformó un capítulo de estándares aplicados y otro de herramientas forenses en la nube, así como un conjunto de capítulos dedicados a cada una de las fases del proceso forense con un protocolo detallado. La intervención de los expertos no solamente permitió nutrir el contenido, sino que también facilitó la validación preliminar de la estructura, con especialistas en la materia revisando borradores de la guía para retroalimentar en explicaciones y aplicaciones más claras. El resultado final de este desarrollo iterativo es la consolidación de la guía metodológica como un documento coherente de teoría y práctica, cuyo cumplimiento tramitará las acciones investigativas, reducirá errores en la recolección de evidencias y ayudará a producir informes forenses sólidos para presentar en ambientes jurídicos.

3.2 Selección de estándares y herramientas

En consecuencia, debidamente basado en las normas desarrolladas, en este caso, los estándares internacionales de informática forense, que cubren el ciclo de vida de la evidencia digital. Por lo tanto, se eligieron tres marcos principales como los más relevantes y que se complementan mutuamente:

ISO/IEC 27037:2012 – Ofrece directrices sobre la identificación, recolección, adquisición y preservación de evidencia digital. Este tipo de estándar informa los primeros pasos del manejo de la evidencia, poniendo un gran énfasis en la integridad a partir del momento del descubrimiento. Por lo tanto, estándares como ISO 27037 establecen principios como el uso de hashes y copias forenses bit a bit para asegurar autenticidad y roles, como Responsable de la Evidencia Digital y un Especialista Forense Digital. Para nuestro proyecto de adquisición inicial de datos con permanencia en entornos cloud, ISO 27037 también era significativo – por ejemplo, el procedimiento para generar snapshots de máquinas virtuales o la extracción de registros de logs.

ISO/IEC 27042:2015 – Directivas de entrega relativas al análisis e interpretación de evidencia digital. Complementa al primero en su enfoque de las fases sucesivas: cómo estudiar los artefactos obtenidos con mayor detalle e intentar recuperar los eventos aplicables desde ellos. Contiene directrices sobre cómo correlacionar los datos, los análisis de los sistemas de archivos, logs y otros objetos, recomendaciones acerca de las metodologías de interpretación y los informes de resultados. Aquí, la ISO 27042 fue útil al proporcionar las técnicas de análisis forense. En la guía, fue beneficioso hacer referencia a ellos, asegurando así que actividades como la reconstrucción de la secuencia en el ataque, y la detección de modificaciones sin autorización se lleven a cabo sistemáticamente y de acuerdo con mejores prácticas.

NIST SP 800-86 - Publicación del National Institute and Technology Guide to Integrating Forensic Techniques into Incident Response, 2006. Guía operativa que describe un modelo de práctica de plantilla de cuatro fases: Recolección, examen, análisis y reporte. En SANER, se enfocaron en que, a diferencia de otros, NIST 800-86 fue una guía orientada por procedimientos e incidentes: incidencias modernas, Sistemas distribuidos, servicios en la nube. No es un estándar de certificación de ISO, pero se comunica con los equipos de respuesta a incidentes, es decir

CSIRTs * NIST 800-86 toma la guía y muestra cómo operarla * Cómo agregar las cuatro fases en la gestión asegurar una integración estructurada y dinámica.

Como resultado de la concordancia comparativa de los marcos en este análisis, un modelo híbrido es la mejor opción que capitaliza sobre las fortalezas de cada uno. La guía metodológica expresamente incluye ISO 27037 para el Aseguramiento de la recolección de datos inicial, ISO 27042 para el análisis de datos técnicos detallado y NIST SP 800-86 como base operacional para la orquestación fundamental de todo el proceso. A través de esta integración de centros de estándares, la cobertura de extremo a extremo de la metodología se mantiene: desde la referencia del incidente hasta el testimonio de evidencia digital, ningún paso crítico fue pasado por alto. Adicionalmente, la combinación de estándares mitigó las debilidades de cada uno: ISO 27037 no tiene profundidad de análisis y no hay adquisición; NIST 800-86 llena esos vacíos y más. Finalmente, debe destacarse que el centro de atención resultante continúa en total concordancia con las necesidades legales ecuatorianas, en particular como se expresa directamente en el COIP. Como tal, los procedimientos propuestos no solo están basados en estándares internacionales, sino que también son admisibles en el contexto judicial local.

Respecto a las herramientas, la guía realiza una selección técnica de software forense apto para entornos cloud, tomando como base la compatibilidad, funcionalidad y aceptación comunitaria. Considerando los desafíos introducidos por la nube (virtualización, datos distribuidos físicamente, multi-tenant, etc.), las herramientas debían ser aptas para estas características. Los criterios de selección fueron: a) compatibilidad con servicios cloud , b) capacidad de preservar a la evidencia de alteración, c) registro de auditoría y documentación de actividades, d) validación frente a la comunidad forense y e) licenciamiento adecuado. Adicionalmente, se realiza una comparativa con las herramientas en uso real en la praxis forense por los expertos entrevistados.

Entre las herramientas recomendadas por la guía se encuentran las siguientes: Magnet AXIOM Cloud: Plataforma de nueva generación de análisis forense centrada en la capacidad de admitir todas las fuentes de datos del ámbito de la nube. Magnet AXIOM ha permitido firmar con los proveedores de servicio un modelo de trabajo seguro en fuentes como Office 365, Google Workspace, fuentes de chat, redes sociales y más. Le permite examinar los mensajes de correo electrónico, mensajes, archivos de Drive, historial y metadatos relacionados mientras utiliza otras capacidades adicionales de la indexación, búsqueda de palabras clave, filtrado por /usuario/ fecha y demás. Está indicado cuando es necesario extraer gran cantidad de información, directamente de plataformas en línea, en caso de incidentes con entornos SaaS. Por ejemplo, una fuga de información derivada de la cuenta de correo corporativo o casos de investigación de delitos en el uso de cuentas de correos personales. En el siguiente práctico desarrollado, Magnet AXIOM Cloud fue fundamental para la creación de una imagen de un correo de Microsoft y la recuperación de ítems eliminados.

FTK Imager/FTK: Esta es la clásica herramienta de Forensic Toolkit para la adquisición forense de datos y análisis a nivel local. Se seleccionó porque puede operar en un entorno IaaS; por ejemplo, se describe el uso de FTK Imager para montar y obtener imágenes de volúmenes de disco virtual de forma bit a bit en la nube pública de AWS o Azure. FTK Imager puede usar copias forenses E01, raw de unidades de almacenamiento en la nube, como los volúmenes EBS en AWS, preservando metadatos y que calculan automáticamente un valor hash. Se recomienda FTK para incidentes en IaaS en los que sea necesario analizar máquinas virtuales comprometidas, como extraer registros del sistema, identificar malware oculto en el sistema de archivos o reconstruir la actividad del atacante en un servidor en la nube. En el primer caso de uso, utilizando AWS, usamos

FTK para indexar y buscar patrones en los archivos de registro extraídos de la imagen del disco para identificar indicadores de ataque y extraer evidencia significativa para un informe profesional.

X-Ways Forensics: Un kit de herramientas de análisis forense avanzado y de bajo nivel, especialmente útil en la evaluación de discos extraídos con gran cantidad de pormenores de control. Si bien no está tan estrechamente vinculada a las investigaciones basadas en la nube, hemos decidido incluir X-Ways en nuestra guía como una variante más de la plataforma para investigar imágenes del disco extraídas de los IaaS. Eso se debe a que en los equipos de inspección menos potentes puede ser una solución completa y al hecho de que a veces X-Ways se puede utilizar incluso aunque FTK sea el programa principal.

AWS CloudTrail/Azure Monitor: Se trata más de servicios que de herramientas que se pueden instalar, ya que son componentes nativos de las plataformas cloud que emiten registros de auditoría y seguridad. Como se hace referencia varias veces en la guía, se consideran fuentes de evidencia: AWS CloudTrail registra todas las acciones llevadas a cabo en la cuenta AWS vía API, vía consola, etc., mientras que Azure Monitor – y su componente Azure Activity Log – hace lo propio con el entorno de Azure. Deberían aprovecharse estas líneas de rastreo autónomas para enriquecer el análisis técnico. Por ejemplo, los registros de CloudTrail podrían dar tiempo de ejecución de accesos y direcciones IP, difusión de configuraciones y creación de recursos, etc., lo cual es indispensable para construir una secuencia de eventos en torno a incidentes en la nube. En el caso de estudio, la exportación de logs de CloudTrail resultó ser útil para confirmar algunas actividades sospechosas en AWS y rellenar la línea del tiempo forense con eventos del plano de control de nube.

Elcomsoft Cloud eXplorer y Cellebrite UFED Cloud: Herramientas especializadas para la extracción de datos de los servicios cloud y los dispositivos móviles en los que estén sincronizados. Me centré en Elcomsoft porque se especializa en el ecosistema de Google; se pueden obtener todos los datos desde las cuentas de Google: Drive, Gmail, fotos, respaldos de Android, incluso si han sido eliminados. A su vez, Cellebrite UFED Cloud puede usar todo, desde iCloud de Apple hasta las cuentas de las redes sociales y estaba relacionado más con las investigaciones, donde los móviles de los sospechosos sincronizan la información con las nubes. Aunque no los apliqué directamente en la práctica de la tesis, los menciono en la guía como valiosas señalizaciones para ciertos casos de uso: o sacar un respaldo de un iCloud en un caso criminal, o extraer chats de Facebook en un caso de ciberacoso.

Velociraptor. Open-source tool para monitorización y respuesta forense en endpoints donde su uso en contextos cloud/híbridos permite ser desplegado para recolectar evidencia en vivo de múltiples sistemas de forma simultánea. La guía la referencia para escenarios PaaS o entornos híbridos donde se requiere ejecutar análisis y colecciones de datos en varios servidores o contenedores en la nube en tiempo real, y Velociraptor permite aplicar queries predefinidas para extraer logs, configuraciones o indicadores de compromiso sin necesidad de intervenir cada máquina manualmente. Esto es útil en general en casos de incidentes extendidos en infraestructura cloud corporativa.

Por supuesto, la guía no se limita a enlistar herramientas, sino que propone su uso dependiendo del modelo de servicio cloud concernido. Por ejemplo, para incidentes en infraestructura se sugieren herramientas de imágenes forenses de disco, y análisis de memoria en algunos casos, plataformas, donde a veces el acceso al sistema operativo subyacente está significativamente limitado se sugiere apoyarse en logs nativos del proveedor, en combinaciones

con utilidades como Velociraptor o Magnet Axiom, en capacidades limitadas a ciertos entornos. Para el caso de software como servicio el enfoque se dirige a herramientas capaces de interactuar vía API con las aplicaciones en la nube, o incluso, en algunos casos con las APIs forenses ofrecidas por los propios proveedores. Todo lo anterior asegura que el investigador forense tenga la herramienta correcta para cada situación, lo que permite maximizar la cantidad de evidencia obtenida sin violar la integridad ni los términos de servicio de los proveedores cloud citados.

Finalmente, degustamos cada una de las herramientas seleccionadas desde el punto de vista de las implicaciones legales. Cabe destacar que, según los principios generales de la guía, cualquier actividad con las herramientas debe ir seguida de la autorización correspondiente; por ejemplo, para acceder al buzón de correo con Magnet AXIOM Cloud, hay una voz en la sentencia durante nuestro caso y el consentimiento implícito de la usuaria propietaria de las carpetas. Además, a cada elemento extraído, es necesario asociar su hash criptográfico en la cadena de custodia, de la que se influyó. Por lo tanto, la veracidad de los estándares y las herramientas robustas confirma la guía desde el punto de vista del esquema metodológico, lo que le otorga una base teórica y práctica sólida y turbulenta a prepararse para la aplicación práctica que anunciamos continuación.

3.3 Implementación de casos prácticos

3.3.1. Implementación del caso práctico AWS

A modo de validación de la guía, se implementó está en un caso práctico que representa un incidente ocurrido en la nube AWS. Este caso ficticio, que funciona como estudio de caso, se corresponde con un escenario de acceso no autorizado a una instancia en Amazon Web Services, para crear escenarios que pusieran a prueba todas las fases que se estructuraron para la metodología de implementación. A continuación, se da a conocer en detalle el contexto del incidente, las acciones realizadas en cada fase de la guía y los resultados logrados.

3.3.1.1 Contexto del incidente AWS

El Caso Práctico 1 se generó el 21 de julio de 2025, luego de que un ciudadano acudió a las oficinas de la Fiscalía Provincial de Loja a formalizar la denuncia por los accesos no autorizados a un servidor en la nube de AWS que su empresa sostenía. La instancia afectada, con denominación "CasoPráctico", era portadora de información sensible y un aplicativo web para la empresa. La denuncia concibió el carácter de un delito en materia de acceso no consentido a un sistema informático, según el Artículo 234 del COIP, pues se argumentaron intrusiones a un sistema ajeno sin la debida autorización. Con la necesaria técnica en juego, el Fiscal emitió un oficio para que el Perito Informático Forense elabore el análisis del servidor comprometido y funciona una cadena de evidencia digital que compruebe o descarte acceso indebido hacia el mismo.

La orden fiscal contenía detalles y alcance claros, entregando al perito las credenciales de acceso a la consola AWS del afectado (usuario y contraseña temporal) para solicitar al mismo que acceda a la instancia CasoPráctico, localice el volumen de almacenamiento principal (Volumen "A") y, a continuación, realice un análisis forense completo del servidor. Asimismo, debía garantizar la integridad de la evidencia digital en todo momento y documentar cada paso de acuerdo con las políticas de la cadena de custodia. Esta autorización formal permitió al perito actuante interactuar con la infraestructura cloud del denunciante sin violar ninguna legislación. Con la recepción del oficio, la parte investigativa siguió la guía metodológica propuesta para comenzar la investigación pericial.

3.3.1.2 Identificación y preservación inicial

Siguiente a la guía de identificación, el perito comenzó por establecer los hechos conocidos y fuentes de evidencia disponibles. La notificación primaria del incidente provino de la subsecuente denuncia del administrador del servidor, quien aportó logs de aplicación (Apache) en que se observaban actividades dudosas a partir del día 15 del mes de julio de 2025, tales como conexiones de origen IP desconocida y modificaciones no autorizadas a archivos críticos. En primer lugar, la observación el indicio fue confirmado; la combinación entre el aviso y la verificación primaria de registros de Apache permitió con certeza afirmar que al servidor se le hacían solicitudes anómalas, de las cuales unas incluso parecían mostrar patrones sospechosos que modifican intentos de explotación a vulnerabilidades. Para ser más claros, se indicó específicamente la detección de intentos de inyección a la SQL en parámetros de URL. Con tal evidencia, el perito pudo provisionalmente clasificar el incidente como una intrusión origen externo a la aplicación web alojada (un ambiente de pruebas de concepto conocido como DVWA – Damn Vulnerable Web App) que explotaba vulnerabilidades conocidas.

El "Tiempo Cero" de activación de la respuesta forense se estableció a las 10:30 del 21/07/2025, inmediatamente después de recibida la denuncia, asegurando desde ese momento las evidencias preliminares. Las medidas de preservación inicial se ejecutaron de forma crítica por evitar la pérdida o alteración de datos volátiles: la instancia comprometida se aisló de la red mediante reglas restrictivas en su Security Group, se generó un snapshot del volumen de almacenamiento asociado al servidor donde se encuentran los EBS, y adicionalmente se exportaron los registros de Apache y de auditoría cloud correspondientes al periodo. Adicionalmente, las credenciales de acceso de solo lectura fueron creadas para uso forense, garantizando que las

siguientes acciones de adquisición no modificarían el entorno original. Todas se orientan a la guía: preservar antes de recolectar; la evidencia debe quedarse congelada en el estado en que se encontró.

Cada uno de los pasos anteriores fue documentado cuidadosamente. En particular, la cadena de custodia se inició para esta fase: el forense registró la hora exacta de cada actividad en la bitácora forense. Los soportes creados (e.g., etiquetando el ID del snapshot EBS y reverting de registros) fueron etiquetados para la referencia adecuada. La importancia de la documentación temprana es resaltada por la norma ISO 27037 y se aplicó rigurosamente; e.g., un hash SHA-256 fue calculado para el archivo de log Apache exportado en bruto para que, lógicamente audio que cualquier análisis posterior se hubiera realizado en una copia exacta del soporte originalmente adquirido. Por lo tanto, al final de la etapa de identificación/preservación, se obtiene un conjunto de evidencia congelada: la instancia aislada AWS, una imagen instantánea del disco, y los principales registros de actividad, todos bajo control forense.

3.3.1.3 Adquisición forense de la evidencia en AWS

En la etapa de Recolección/Adquisición, el objetivo era obtener copias forenses de la información identificada, para poder analizarla en detalle fuera del laboratorio sin modificar el original. Según la guía, al tratarse de una infraestructura IaaS, la práctica recomendada sería crear una imagen bit a bit del volumen del disco virtual afectado. Por ende, se tomó como fuente el snapshot EBS previamente generado (volumen “A” del servidor): con las herramientas forenses seleccionadas, se creó una imagen forense completa del disco en formato RAW (o E01). En este caso, se utilizó FTK Imager en una instancia forense de AWS preparada para el caso. Se adjuntó el snapshot a la instancia forense en modo solo lectura y se ejecutó FTK Imager para clonar el volumen bloque por bloque. Durante la adquisición, se verificó la integridad ejecutando hashes SHA-256 y SHA-1 sobre la imagen adquirida y el snapshot, generados con herramientas de AWS,

para asegurarse de que la copia fuera fiel al original. El hash de la imagen, por ejemplo, SHA-256 final, estuvo registrado en el Formulario de Cadena de Custodia.

Además del disco, los logs de AWS CloudTrail relevantes también fueron formalmente recolectados. AWS permite exportar los eventos de CloudTrail a archivos; para las fechas del evento, es decir, los días cercanos al compromiso, el perito realizó esta exportación y extracción. Estos registros contienen registros de todas las acciones a nivel de cuenta de AWS, como creación de recursos, accesos y cualquier tipo de cambios de configuración dieran cuenta al revisar el comportamiento de los atacantes a través de la evidencia de la máquina. Finalmente, las capturas de pantalla y los logs de la consola AWS a la que se conectó el atacante, también fueron recolectados para resaltar alertas y eventos significativos. Estos se adjuntaron como evidencia ilustrativa.

Este proceso de adquisición se llevó a cabo con procedimientos estrictos a la cadena de custodia. Cada uno de los soportes que contenían, evidencia el disco y el paquete de logs fueron sellados con sus hashes correspondientes y etiquetados. La imagen y todo lo recolectado se transfirió desde la nube hasta el laboratorio físico a través de un medio de almacenamiento externo cifrado. Esto incluyó un SSD portátil cifrado. Durante la entrega, los registros de custodia se actualizaron y firmaron tanto el perito que realiza la adquisición como el custodio receptor en el laboratorio de destino, incluyendo la fecha/hora de la transferencia, la persona que entrega/recibe, el tipo de evidencia y el hash de verificación de integridad. Por lo tanto, desde que se tomó la evidencia en AWS, no se ha creado oportunidad de la manipulación de la evidencia adquirida por parte de terceros.

Por último, cabe mencionar que no se pudo realizar la adquisición de memoria RAM de la instancia, limitaciones comunes en entornos cloud, una vez la VM está detenida, ya que, de acuerdo con el proveedor, no es factible tener acceso directo a la memoria RAM volátil. Sin embargo, se pudo mitigar parcialmente, logrando acceder a la información del estado de los procesos a través de los logs del sistema y acceso a AWS. Con las fuentes de prueba más importantes, disco y logs, se generó el traslado a la fase 4 del proceso de examen y análisis forense.

3.3.1.4 Examen y análisis de la evidencia AWS

El primer paso realizado en la fase de Examen y Análisis fue el examen de la imagen de disco según la guía y la norma ISO 27042. El propósito de esta etapa es poner en contexto el entorno forense. En nuestro caso, el servidor AWS es una instancia Ubuntu Linux con un servidor web ejecutándose, un servidor web Apache conocido que tiene la aplicación DVWA instalada en él. Se montó la imagen en modo solo lectura y se extrajeron los siguientes artefactos forenses utilizando las herramientas forenses X-Ways y FTK: archivos de log del sistema – la fuente principal, que se encuentra en dos ubicaciones distintas: /var/log/auth.log, los logs de Apache ubicados en /var/log/apache2/; diferentes archivos de configuración de Apache y PHP, historial de comandos (\.bash_history del usuario administrador) y otros. En el último paso de la fase de Análisis se encontró que DVWA estaba en el directorio web /var/www/html/dvwa/.

Una estrategia crítica también fue la construcción de una línea de tiempo. Se fusionaron registros de fuentes de tiempo diferentes: timestamps de las solicitudes de HTTP a partir de logs de Apache, marca de tiempo de las acciones de AWS desde el registro CloudTrail y fecha de modificación/creación del sistema de archivos del servidor. Se usó una herramienta de línea de tiempo para correlacionar eventos. A modo de ilustración, la intersección de estos datos reveló que el día 15/07/2025, alrededor de las 23:00, justo después del avistamiento del acceso no identificado

por el denunciante, se crearon o modificaron ciertos archivos en el directorio DVWA; además, segundos después, los registros de CloudTrail hicieron abrigar a los investigadores, como desde la dirección IP requerida también ejecutaron la invocación del agente SSM en el host. Esta correlación temporal robusteció la reorganización del ataque.

El propio análisis forense estaba dirigido a las respuestas a las preguntas clave: ¿Qué sucedió en el servidor? ¿Cómo conseguir al atacante? ¿Qué hizo y que consecuencias tuvo? En resumen, los hallazgos técnicos estaban:

Un vector de ingreso. El atacante explotó una aplicación web DVWA, que sabíamos que era vulnerable: inyección SQL, RCE, etc. Los logs de Apache durante ese periodo de análisis mostraron múltiples solicitudes HTTP con patrones maliciosos. En particular, noté repetidas peticiones HTTP GET con parámetros sospechosos que parecen ser intentos de inyección SQL en todos los formularios DVWA. Estas peticiones fueron constantes con una misma IP externa que se reflejó en el registro decenas de veces. Durante la verificación del origen de esta IP en bases públicas, resultó estar asociada con compromisos maliciosos. Me parece que un actor automatizado o semiautomatizado descubrió la presencia de DVWA y lanzó ataques.

Explotación y acciones del atacante: Examinando el sistema de archivos del servidor, se encontró varios archivos con los que no se instala en DVWA y otras versiones comúnmente aprobadas. Se descubrió un script PHP furtivo en la carpeta de DVWA, implementado como un archivo PHP basado en una web shell y con nombres semejantes a una librería estándar de PHP. La fecha de creación correspondía a las visitas no autorizadas y se sospecha que el atacante logró subir el archivo furtivo al servidor aprovechando la vulnerabilidad descubierta. Además, en los logs de acceso del sistema, auth.log, encontramos registros de conexiones SSH establecidas en horarios no comerciales y también para la IP sospechosa, inmediatamente después de la intrusión

web. Con todo, podemos afirmar que después de explotar el servidor web, el atacante escaló los privilegios o reutilizó las credenciales para establecer una conexión SSH no autorizada. Para demostrarlo, revisamos el bash_history del usuario administrador y desciframos comandos que afirmaba no haber ejecutado, como instalar herramientas de red y registrar un nuevo usuario con privilegios sudo. Todos estos indicios nos hacen deducir que el intruso obtuvo control sobre el sistema operativo.

Evidencia de exfiltración o daño. Buscó rastros de robo o destrucción de información, se halló. Por un lado, no se encontraron archivos de datos corporativos extraídos ni archivos de datos borrados masivamente, lo cual indica que el objetivo del atacante era centrarse más en comprometer el sistema en sí, en lugar de en la extracción activa, tal vez debido a que es un entorno de pruebas, DVWA, sin datos reales atractivos. Sin embargo, se encontraron registros y artefactos de intentos contrarios intentos de instalar herramientas adicionales: utilidades de red están presentes, por ejemplo, las de exploración de red guardadas en /tmp. Adicionalmente, se deja constancia de que el invasor no desactivó webshell, haciendo así una puerta trasera del sistema inoperable para posibles accesos futuros. Postanálisis de la contención, el perito recomendó eliminar esos artefactos y asegurar el servidor antes de reactivarlo.

Todo el hallazgo fue interpretado mediante la norma ISO 27042, es decir, todos los eventos fueron reconstruidos y documentados. En el reporte técnico fue presentada una secuencia. El atacante primero explotó DVWA a través de un SQLi, obteniendo posiblemente credenciales de administrador de la base de datos o incluso obtuvo la ejecución de comandos, por lo menos. Luego subió una webshell, es decir, un archivo malicioso y desde allí llevó a cabo la ejecución de comandos que le dieron acceso al sistema, es decir, SSH. Por último, realizó actividades poscompromiso típicas como intentos de instalación de herramientas o la creación de usuarios.

Esta narrativa técnica se ajusta perfectamente a la figura delictual denunciada, ya que es un caso de acceso no consensuado con intención, es decir, el delito de acceso no consentido tal y como fue tipificado por COIP 234.

En cuanto al análisis, usamos las herramientas forenses recomendadas. No encontramos una aplicación práctica para Magnet AXIOM en este caso, pero FTK y X-Ways nos permitieron analizar rápidamente grandes cantidades de datos. Con FTK, realizamos búsquedas de cadenas clave en los logs, en el sistema de archivos se utilizaron términos como “password”, “error”, “php”, etc., y encontramos el nombre de la webshell, y se realizaron algunos otros reportes parciales. Además, exportamos todas las evidencias significativas mediante FTK y las cargamos en el caso, además con sus hashes correspondientes. Eso nos permitió garantizar que cualquier otro perito u autoridad pudiera verificar independientemente cada evidencia.

3.3.1.5 Resultados y conclusiones del caso AWS

La aplicación de la guía metodológica en el Caso Práctico AWS fue exitosa en haber logrado cumplir nuestros objetivos forenses planteados. Después de todo, se confirmó la intrusión no autorizada al servidor de AWS: el atacante explotó la vulnerabilidad de la aplicación web para obtener acceso, instaló el código malicioso y accedió ilegalmente al sistema. Todas estas circunstancias quedaron demostradas con bastante evidencia digital sólida como resultado de la investigación. Por lo tanto, se obtuvo un conjunto de pruebas forenses que respaldarían nuestra conclusión entre la variedad de pruebas presentadas anteriormente: registros de Apache: los ataques en sí mismos (solicitudes de inyección SQL), trazas de AWS CloudTrail que confirman las conexiones desde la dirección IP del atacante, archivos maliciosos que se recuperaron del sistema: por ejemplo, la webshell y registros del sistema: la creación de accesos indebidos.

Toda la evidencia de este caso fue debidamente registrada y documentada con cuidado. El informe cumplió con la estructura del estándar y contuvo secciones de descripción general del incidente, métodos usados, resultado técnico y relación con la legislación. Además, se adjuntó la cadena de custodia firmada y la lista de hash acordada al inicio del caso. Es importante destacar que, cumpliendo con estándares internacionales, toda esta evidencia se mantiene confiable y aceptable, ya que los hashes garantizan la integridad de todos los archivos y el procedimiento minimizó cualquier posible contaminación. Así mismo, debo mencionar que el estándar aplicado resultó ser extensible a un entorno real de AWS, ya que se siguió el protocolo sin uso indebido de AWS y la instancia afectada por la evidencia no fue perturbada para la pericia.

Desde un punto de vista práctico, el caso también permite comprobar la efectividad de las herramientas elegidas, ya que FTK Imager permitió adquirir la imagen del volumen AWS exitosamente, y las utilidades para el análisis permitieron que el procesamiento con grandes logs y datos grandes se completara a tiempo razonable, poniendo de relieve eventos importantes. Además, dada la evidencia obtenida usando CloudTrail como fuente, la recomendación de la guía para siempre incluir los registros del proveedor cloud en el análisis es válida.

3.3.2 Implementación del caso práctico II

El segundo caso de estudio se realizó en un escenario de servicios en la nube SaaS, específicamente correo electrónico en Microsoft 365/Outlook.com. A diferencia del caso de AWS, que involucra una intrusión externa, este caso investiga un posible fraude informático donde la evidencia digital recuperable consistía en un correo electrónico eliminado. La guía metodológica fue aplicada nuevamente para probar su versatilidad en un entorno de cloud computing distinto utilizando el enfoque aplicado, ya que se enfoca en la adquisición de SaaS a través de herramientas especializadas y la validación de integridad de los datos en la nube de Microsoft.

3.2.2.1 Contexto del incidente en Microsoft 365

El Caso Práctico 2 trata de una denuncia presentada el 1 de agosto de 2025 en la Fiscalía de Loja, en relación con la posible comisión de un delito de estafa por medios electrónicos. En concreto, un ciudadano, Luis Alfredo T. P., alega haber sido objeto de un fraude al adquirir su teléfono celular a través de la plataforma online. Según su versión, el ciudadano realizó el pago mediante una transferencia bancaria a favor de la firma vendedora, la empresa TecnoXpress; la transacción fue confirmada a receptor a través del envío de una factura electrónica vía correo, junto con un recibo de depósito del dinero cursado al vendedor por el comprador. No obstante, el dispositivo adquirido nunca fue entregado al morador. Posteriormente, cuando el ciudadano quiso presentar dicha factura y los correos en los que los recibió, se dio cuenta de que los había borrado, junto con el recibo de banco donde también se anotaba la transacción. El accidente acabó dejando a un ciudadano sin pruebas que podrían haber servido como evidencia de la alegación de fraude.

Para abordar esta situación, la víctima solicitó a la Fiscalía la asistencia para recuperar mensajes que habían sido previamente eliminados de su cuenta de correo Microsoft Hotmail (Outlook.com) para ser posteriormente presentados como evidencia digital del proceso penal. Previo a ello, la Fiscalía al evaluar la denuncia, concluyó que siendo el caso que conforme al COIP y en las figuras de posible estafa mediante engaño, artículo 186, y delitos informáticos por uso de medios electrónicos, artículo 454, correspondería la realización de un peritaje informático forense en la cuenta de correo de la víctima, para ello dictaminado en una autorización formal donde el denunciante firmó un consentimiento para acceso controlado de su correo y proporcionó sus credenciales de usuario: luisasofia-1220@hotmail.com, password al perito designado por él mismo. En el documento se estableció la naturaleza y extensión de la pericia con el objetivo preciso

de recuperar correos electrónicos eliminados del 28 de julio al 5 de agosto del 2025, relacionados con la transacción del teléfono. En conclusión, había un marco legal y logístico para la industria de la guía forense de los correos electrónicos en la nube: consentimiento del titular y orden fiscal, al garantizar a las autoridades el uso exclusivo de las herramientas para rastrillar la nube en cuestión sin vulnerar la privacidad ni incurrir en desacato a las leyes o jurisprudencia.

3.2.2.2 Preservación y adquisición de evidencia en Microsoft 365

En cumplimiento de la guía, una vez notificado el caso, se procedió con premura a la preservación de la información almacenada digitalmente de la cuenta de correo de la víctima. Dado que se trataba de un entorno SaaS, la evidencia residió en servidores de Microsoft. La guía aconsejó que en estos casos no se debía tocar alguna plataforma, en su lugar, se debían utilizar herramientas que pudiesen interactuar con la plataforma vía APIs oficiales para que no se alterara el contenido del buzón como ya se mencionó. En resumen, la cuenta de correo fue adquirida forensemente por la herramienta Magnet Axiom Cloud, que es una de las tres herramientas seleccionadas en la sección 3.2.

Como primera medida de preservación, la fiscalía le cambió la contraseña a la víctima por un usuario forense temporal para que no se entrara de forma fraudulenta, y en su lugar, le permitiera al perito visualizar el contenido de la cuenta en modo lectura. Posteriormente, con Magnet AXIOM, se procedió a la conexión segura a la cuenta de Hotmail con las credenciales proporcionadas y la autorización obtenida. La herramienta estableció una sesión HTTPS con los servidores de Microsoft, con lo cual se garantizó la confidencialidad de la creación de la adquisición.

La adquisición forense implicó la extracción completa del buzón de correo de la usuaria en formato forense. En Magnet AXIOM Cloud existe la opción de directamente descargar todos los mensajes y carpetas de la cuenta, pero en este caso decidimos generar un archivo PST (formato estándar de Outlook) con su buzón completo y además un archivo complementario con metadatos de la actividad en la cuenta. Durante esta adquisición, también habilitamos la recuperación de elementos borrados: configuramos herramienta para que incluyera correos eliminados que aún estuvieran en carpetas “Eliminados” o incluso en la retención de Outlook. De hecho, Magnet AXIOM pudo recuperar exactamente el mensaje de interés en cuestión que había sido borrado de la bandeja de entrada principal, porque aún estaba en retención del servidor de correo. Junto con el mensaje extrajimos sus archivos adjuntos, en este caso pdf de factura electrónica y probablemente una imagen o pdf de comprobante de transferencia, y los metadatos completos de cabecera de cada correo, incluyendo información de encabezados como From, To, CC, Subject, Message-ID, rutas de recibido, sellos de tiempo, etc., que serían importantes para confirmar la autenticidad y el origen del correo recuperado.

Como resultado de la adquisición, Magnet AXIOM generó automáticamente un registro exhaustivo de la operación, de modo que se puede saber en cualquier momento cuando se hizo la conexión, que fue extraído y cualquier otra eventualidad. Tras finalizada la operación, la herramienta calculó los hashes criptográficos – SHA-256 y SHA-512 – de todos los archivos adquiridos (PST con el buzón, los adjuntos exportados, los reportes en formato JSON), de manera que proporcionó las “huellas digitales” de cada evidencia. Por consiguiente, estos valores hash fueron inmediatamente incluidos en la cadena de custodia y al log de auditoria; con marca de fecha, hora y responsable del acto adquisitivo, y cualquier cambio futuro de estos archivos podrá ser detectado si los nuevos hashes no coinciden con los originales.

Por lo tanto, para resumir la adquisición al final de este caso, estamos en posesión de un archivo PST que contiene todo el correo de la víctima a la fecha, incluidos los mensajes eliminados; archivos adjuntos clave separados para una fácil referencia. Un conjunto completo de metadatos y reportes de actividad de la cuenta, por ejemplo, un registro de accesos a la cuenta, como se revela mediante los reportes de Magnet AXIOM Cloud. Este material se conserva de manera segura en un medio cifrado, etiquetado y custodiado por el perito. Vale la pena mencionar que la guía respectiva establece la importancia de dejar los datos originales en la nube sin acceder a ellos. En línea con esto, Magnet AXIOM operó en el modo de solo lectura sin sincronizar ni marcar los mensajes, y la cuenta de la usuaria se dejó sin cambios, habiendo cambiado solo la contraseña de la misma de manera preventiva. Microsoft, como proveedor no está directamente involucrado en el proceso, ya que la herramienta se basa en APIS oficiales con la autenticación del usuario; sin embargo, la posibilidad de presentar una solicitud formal a Microsoft para la conservación de la cuenta estaba completa en la guía en caso de necesidad.

3.2.2.3 Examen y análisis forense del correo electrónico

Reunida la evidencia en un formato especial (toda la mailbox en formato PST), se da inicio a la fase de examen y análisis forense en laboratorio. Como primer paso, se verifica la integridad de los archivos, esto se logra comparando los hashes calculados post-adquisición con las rutas generadas al momento de la extracción. Todos los hashes cotejaron, lo que indica que la transferencia se logró exitosamente y sin ser modificada. Luego, se importa el PST en Magnet AXIOM Examine, la herramienta de análisis complementaria de Magnet, la cual fue diseñada y optimizada para manejar datos de correo.

La primera etapa del examen fue simplemente la revisión de la estructura del buzón: se abrieron las carpetas, tales como la Bandeja de entrada, Elementos eliminados, Enviados, etc., así como se identificó un intervalo de fechas relevante para el caso. A continuación, utilizaron la capacidad de filtrado de AXIOM para restringir la vista a todos los mensajes de correo electrónico enviados dentro de un rango temporal específico; en el caso donde se realizó la transacción entre Tarek y la empresa, estos serían a fines de julio y principios de agosto de 2025. Luego, se realizó una búsqueda en el PST de cualquier correo que contuviera palabras clave "factura", "transferencia" o el nombre "TecnoXpress". La búsqueda dio como resultado el correo eliminado que contenía la factura de compra de un teléfono y el recibo del depósito bancario. El mensaje estaba claramente en la carpeta de eliminados del PST, lo que confirmaba que el usuario lo había eliminado, pero se podía recuperar.

Una vez identificado el correo en cuestión, se llevó a cabo un análisis forense detallado de sus metadatos de cabecera para garantizar su autenticidad y origen. Se examinaron campos como "From" (remitente), "To" (destinatario), la fecha de envío y especialmente, las líneas de "Received" que muestran las rutas y servidores de correo por los que pasó el mensaje. Esto permitió confirmar, por ejemplo, que el correo efectivamente fue enviado por la dirección oficial de la empresa vendedora (e.g., facturacion@tecnoXpress.com) hacia la cuenta de la víctima, en la fecha y hora coherente con la narrativa del denunciante. También se verificó la firma DKIM/SPF en los encabezados para descartar falsificación del remitente: los metadatos indicaban que el mensaje pasó las validaciones de dominio, reforzando que no se trataba de un correo forjado, sino legítimo.

Entre otros, fueron examinados los archivos adjuntos recuperados, una factura y un comprobante. El primero, un archivo PDF sentado de una factura electrónica, fue abierto en un entorno aislado y fue verificado para que los datos coincidan con la transacción: contenía el nombre del comprador, la fecha del pago y el monto y concepto de la compra del teléfono, además de los sellos digitales de la empresa emisora. El segundo archivo, una captura de recibo de depósito, presentaba el número de transacción bancaria, además de la fecha y hora del pago. Ambos documentos parecían ser genuinos a primera vista. El perito calculó los hashes de dichos PDFs para incluirlos en el informe para poder identificarlos en cualquier otro medio. También verificó si posiblemente dichos archivos adjuntos no residían en OneDrive y en otro servicio adjunto a la cuenta, Magnet AXIOM daba la capacidad de verificar OneDrive también, pero no había copias adicionales allí.

Es importante destacar también que, de manera paralela, se investigaron los logs de actividad de la cuenta Microsoft, tal como se proporcionaban en los reportes JSON. Esto fue útil para ver si no se accedió a la cuenta de correo de maneras inusuales y, en general, si no hubo inicios de sesión desde IPs desconocidas que puedan sugerir que un tercero eliminó el correo maliciosamente. Según el análisis de los logs, no se encontraba evidencia de intrusión en la cuenta: en todos los inicios de sesión registrados, la ubicación y el dispositivo eran de la misma usuaria. Por consiguiente, la eliminación del correo fue efectivamente accidental, y la víctima no fue manipulada por un hacker. Sin embargo, fue necesario investigar esta opción para descartar un escenario alternativo, a pesar de haber sido poco probable.

En conclusión, el forenseo de correo permitió el recuperar la fecha de la evidencia perdida (email y adjuntos) y su correcta de validación, generando confianza judicial.

3.2.2.4 Resultados y hallazgos del caso Microsoft 365

Como se puede ver en el Caso Práctico 2, al aplicar la guía, fue posible recuperar evidencia digital crítica para investigar un fraude. A través del proceso forense, se logró recuperar el correo electrónico donde se encontraba la factura y el comprobante del pago generado, el cual es la prueba central de la transacción alegada, desde la cuenta de Outlook.com de la víctima. Este logro permitió que la Fiscalía pueda contar con dicha evidencia, la cual de otra forma se habría mantenido inaccesible por medios convencionales.

Los resultados específicos incluyen:

- Correo recuperado: El tercer correo es de TecnoXpress a la víctima, con fecha de enviado 28/07/2015 y respecto a la compra del teléfono más reciente y encontrado en la carpeta de eliminados. El cuerpo del correo expresaba agradecimiento por la compra y se refería a la factura y comprobante adjuntos.
- Adjuntos clave: La factura N.° XXX del PDF de TecnoXpress con el monto del teléfono, y un comprobante de transferencia bancaria, archivo o pantalla capturada o PDF obtenido por la institución financiera indicando el monto y la fecha. Ambos están adjuntos y se mantienen intactos.
- Confirmación de integridad y origen: El propio análisis atestigua que el correo y la documentación no habían sido cambiados: los hashes de los archivos coinciden y metadatos indican el origen legítimo. Por ejemplo, se confirma que el servidor de correo TecnoXpress fue enviado desde un dominio autenticado. Como se vio arriba, SPF/DKIM “pass” significa que la factura realmente fue enviada por la empresa, lo que indica un hecho adicional para la autenticidad de la evidencia.

- Ausencia de accesos indebidos: No hay pruebas de que un tercero haya accedido a la cuenta de la víctima para borrar el correo, lo cual habría sido un segundo delito. En este camino, en lugar de un asalto cibernético a la cuenta acreditada, el incidente oscureció un caso de pérdida accidental de prueba por la cuenta acreditada que se recuperó mediante técnicas forenses.

Toda la evidencia recuperada fue debidamente documentada. En la cadena de custodia, se incluyó el acceso al lugar de trabajo del medio conteniendo el PST con el hash correspondiente, así como de los adjuntos recuperados, bajo custodia del perito. Del mismo modo, en el informe pericial, se incluyó como anexo el correo recuperado junto con los adjuntos, en formato impreso y en medio digital, señalando en la conclusión que dichas piezas corresponden a la transacción del delito que evalúa. Se realizó además el detalle técnico del procedimiento utilizado para la recuperación, señalando que se utilizaron herramientas especializadas como Magnet AXIOM Cloud, acorde con las mejores prácticas, y la integridad de los datos está asegurada.

En definitiva, la guía probó su aplicabilidad en este caso a través de varias razones. En primer lugar, validó que las fases forenses tradicionales aún se aplican en una investigación forense de correo en la nube: se identificó un incidente y, en particular, además de la denuncia de fraude, “el correo faltante estuvo alrededor del 4 de julio”; se preservó la evidencia; se adquirió con rigor y se analizó a fondo, lo que conducía a la presentación de la evidencia en un “informe”. En segundo lugar, la guía reveló la importancia de cómo diferentes herramientas: sin la utilización de Magnet AXIOM, habría sido casi imposible recuperar ese correo eliminado. Por lo general, los proveedores OLTP como Microsoft solo mantienen los mensajes eliminados por un tiempo limitado y, a menudo, requieren un proceso legal prolongado para recuperarlos. Es decir, aquí no solo el perito era fundamental, sino también sus herramientas. Tercero, se reveló con respecto al marco legal.

Todo se llevó a cabo con el consentimiento y por los canales adecuados, por lo tanto, aquí, la defensa probablemente no puede objetar la legalidad de adquirir esta evidencia.

CAPITULO IV: RESULTADOS

4.1 Resultados del caso AWS

Como resultado, el caso de AWS Analysis siguió los procedimientos propuestos para la adquisición, preservación y análisis de evidencia digital y resultó en un conjunto de evidencia sobre la instancia EC2, sus volúmenes EBS asociados y los registros adicionales de actividad almacenados, como CloudTrail. Con el fin de mantener la cadena de custodia, las copias hash y las instantáneas de los volúmenes EBS creados se utilizaron para el análisis forense de los datos en un entorno aislado; sin embargo, se obtuvieron en un archivo de almacenamiento para demostrar la integridad. En el examen usando Magnet AXIOM y FTK, se identificaron varios artefactos relevantes para el caso.

Los registros correspondientes mostraron inicios de sesión no autorizados, incluidas direcciones IP externas, y operaciones de creación de instancias anteriores al incidente formateadas. El volumen en sí contenía archivos y metadatos recuperados que confirmaban el comportamiento inusual, como claves SSH agregadas y registros de sistema modificados. Mientras tanto, Magnet AXIOM permitió extraer información específica para la nube, como la configuración de AWS y los logs de usuario, y FTK permitió una interacción de nivel inferior con el volumen de la instancia.

En conclusión, el uso de FTK y Magnet AXIOM demostró ser suficiente en un entorno IaaS y pareció complementario de esta manera. FTK demostró ser exitoso en la recuperación de artefactos del sistema operativo, mientras que AXIOM fue capaz de identificar eventos, ya que se alojaba en servicios históricos.

4.2 Resultados del caso Microsoft 365

La prueba en el caso de Microsoft 365 significó el uso de posibilidades de AXIOM para adquirir y analizar datos de correo electrónico y de colaboración (OneDrive y SharePoint). Se

configuraron credenciales de administrador y se seleccionaron los buzones y recursos pertinentes. Como resultado, se recibió un archivo de caso con contenido exportado, incluyendo correos electrónicos, documentos compartidos, metadatos de archivos y registros de auditoría.

El análisis arrojó algunos resultados prometedores. En particular, se recuperó un correo sospechoso con un adjunto malicioso que el usuario había ocultado en una carpeta privada; los metadatos mostraban accesos repetidos en horarios inusuales. AXIOM vinculó un archivo a múltiples dispositivos y ubicaciones, lo que permitió investigar quién accedió al archivo y desde dónde. Esta información contextual fue crucial para interpretar la intención del incidente. Incluso los registros de auditoría de Microsoft 365 proporcionaron direcciones IP y marcas temporales precisas, incluyendo accesos desde ubicaciones extranjeras que indican actividad maliciosa. Estos resultados sugieren que recuperar e interpretar la evidencia en un entorno SaaS es factible si se utilizan las herramientas adecuadas.

La ventaja de Magnet AXIOM fue la capacidad de extraer datos de los correos y los servicios de nube en un único flujo de trabajo, lo que permitió recuperar la cronología completa de eventos con metadatos detallados.

4.3 Resultados de la encuesta

La encuesta se aplicó a tres profesionales forenses ecuatorianos (dos de la Fiscalía y uno de la Policía Nacional). Los principales hallazgos fueron los siguientes:

- **Experiencia y conocimiento:** El 100%, con más de 10 casos. En nivel de conocimiento, el 67% tenía un nivel avanzado, mientras que el nivel medio tenía un nivel promedio del 33%.

- **Proveedores conocidos:** Todos estaban familiarizados con AWS (100%) y la mayoría con Microsoft Azure (66%). Un tercio mencionó además Google Cloud Platform y Oracle Cloud (33% cada uno).
- **Desafíos percibidos:** El 100% coincidió en que los principales retos son la volatilidad de la evidencia y la falta de herramientas especializadas.
- **Recursos necesarios:** En este sentido, todas las respuestas subrayaron la necesidad de capacitaciones técnicas continuas y de herramientas forenses en la nube, el 33% mencionó también la necesidad de mejora inmediata del marco legal.
- **Procedimientos institucionales:** Solo el 33% indicó que su institución cuenta con protocolos estandarizados para investigaciones en la nube, mientras que el 67% reconoció que no los tiene.
- **Marco legal y cooperación:** Todos señalaron que conocían sobre el marco legal actual y que habían solicitado información sobre los servicios ofrecidos por proveedores en la nube. El 66% afirmó que la cooperación entre países era aceptable, mientras que un 33% opinó que era buena. No obstante, un 67% dijo que los acuerdos internacionales son parciales o insuficientes.
- **Prioridades para la guía:** Un 66% señaló la importancia de incluir detalles técnicos y metodológicos, mientras que un 33% enfatizó la necesidad de fortalecer la cooperación internacional.

Estos resultados evidencian consenso en varios puntos: la necesidad de capacitación, la carencia de protocolos estandarizados y la relevancia de la cooperación internacional.

4.4 Discusión general

La evaluación de los casos prácticos y de la encuesta valida la utilidad de la guía metodológica propuesta. Desde el punto de vista técnico, los procedimientos resultaron aplicables: la minería de evidencia en snapshots de AWS y la inspección forense arrojaron resultados claros y, en el caso de Microsoft 365, se pudo recolectar correos y documentos pertinentes.

Los resultados con respecto a estándares internacionales indicaron que los métodos utilizados, el hashing, los procedimientos no invasivos y la sistemática de la documentación, son adecuados para mantener la integridad y la fuerza probatoria. Desde el punto de las herramientas, se comprobó que FTK y Magnet AXIOM se complementan muy bien en cobertura de evidencia local y en la nube.

En cuanto al nivel institucional, la encuesta demostró la falta de procedimientos estandarizados en la mayoría de las entidades ecuatorianas, lo que fundamenta la necesidad de una guía como la presentada. Al mismo tiempo, se señaló la conveniencia de la capacitación constante y de la cooperación internacional, como herramientas para llevar la metodología a la práctica, superando las limitantes legales y las barreras técnicas.

En definitiva, se concluye que la guía es un recurso válido para la aplicación en investigaciones reales y un valioso aporte tanto al ámbito académico como judicial ecuatoriano, siempre y cuando vaya acompañada de esfuerzos de formación y de esfuerzos en conjunto y colaboración.

CAPITULO V:
RECOMENDACIONES Y CONCLUSIONES

5.1. Conclusiones

El proceso de elaboración de esta tesis, sustentado en el estudio de estándares, herramientas y procedimientos forenses en la nube, así como en la validación mediante casos de prueba, dio lugar a una serie de hallazgos que se sintetizan en las siguientes conclusiones:

- La construcción de la guía metodológica, basada en estándares, herramientas y procedimientos internacionales, demostró en los casos de prueba (AWS y Microsoft 365) que es un recurso válido para orientar la investigación forense en la nube y garantizar procesos estructurados y replicables. Este resultado es coherente con la encuesta aplicada: el 66,7 % de los profesionales indicó no contar con procedimientos estandarizados en su institución, lo cual confirma que la guía atiende una necesidad operativa real. Su estructura es extensible a otros proveedores y servicios (Azure, Google Cloud Platform y Google Workspace/Gmail) con ajustes mínimos.
- El análisis comparativo de estándares, normas y procedimientos permitió establecer un conjunto de pasos ordenados (identificación, adquisición, preservación, análisis y presentación) que eleva la calidad probatoria de la evidencia digital, asegurando su fiabilidad, trazabilidad y utilidad judicial. La encuesta mostró que el 100 % de los participantes toma como referencia ISO/IEC 27037, lo que valida la pertinencia de la estructura de la guía. La secuencia metodológica se adapta correctamente a los distintos modelos de servicio (IaaS, PaaS y SaaS) y a escenarios de correo y colaboración (Microsoft 365 y Google Workspace/Gmail).

- La validación práctica evidenció que todas las herramientas seleccionadas fueron testeadas y probadas, verificándose sus potencialidades y aplicabilidad en entornos reales. Según la encuesta, Magnet AXIOM Cloud registra 100 % de uso, Cellebrite Cloud Analyzer 66,7 %, Oxygen Forensic Cloud Extractor 66,7 % y AWS CLI 33,3 %, lo que confirma la conveniencia de un enfoque instrumental mixto (herramientas nativas del proveedor y herramientas especializadas). En los escenarios SaaS de correo, Magnet AXIOM ofreció la cobertura más completa para descubrimiento, adquisición, filtrado/búsqueda y reporte forense; por tanto, para correo corporativo en SaaS se concluye que AXIOM fue la opción más integral, aplicable tanto a Microsoft 365 como a Google Workspace/Gmail.
- Con base en el análisis y en las encuestas a profesionales, la definición de roles y la asignación de responsabilidades dentro del equipo forense permiten dar seguimiento adecuado a cada fase de la investigación, garantizando coordinación, control de cambios y reducción de errores en la gestión de evidencias. La guía clarifica funciones como primer elemento que interactúa, analista forense, custodio de evidencia, administrador cloud y asesor legal, fortaleciendo la trazabilidad de actuaciones en proveedores como AWS, Azure, GCP, Microsoft 365 y Google Workspace/Gmail.
- Los principales retos identificados por la encuesta fueron la jurisdicción y los aspectos legales, así como la volatilidad de la evidencia, seguidos por la falta de herramientas especializadas y el acceso a datos por parte del proveedor. La guía aborda estos riesgos mediante preservación temprana, documentación exhaustiva y coordinación formal con los proveedores. Esta estrategia se traduce en

procedimientos más robustos para correo y colaboración (Microsoft 365 y Google Workspace/Gmail), almacenamiento y cómputo (AWS, Azure y GCP), y auditorías de acciones administrativas y de acceso.

5.2. Recomendaciones

En base a las conclusiones obtenidas, se pueden plantear las siguientes recomendaciones:

- Adoptar la guía como protocolo de referencia en ámbitos institucionales y académicos. Incorpórala en prácticas de laboratorio y simulaciones con múltiples proveedores (AWS, Azure, GCP, Microsoft 365 y Google Workspace/Gmail) y revísala al cierre de cada periodo académico u operativo para integrar lecciones aprendidas, cambios tecnológicos y ajustes normativos.

- Adoptar la guía como protocolo de referencia en ámbitos institucionales y académicos. Integrarla en prácticas de laboratorio y simulaciones con múltiples proveedores como AWS, Azure, Google Cloud Platform, Microsoft 365 y Google Workspace, y revisarla al cierre de cada periodo académico u operativo para incorporar lecciones aprendidas, avances tecnológicos y ajustes normativos. Para la Escuela de Ingeniería en TI, usar la guía como material base en asignaturas de seguridad y computación forense.

- Institucionalizar la secuencia metodológica mediante lineamientos mínimos y listas de verificación por fase —preservación temprana, verificación de hashes, cadena de custodia y anexos probatorios—, adaptando su aplicación a cada modelo de servicio y tipo de evidencia en IaaS, PaaS y SaaS.

- Mantener un catálogo institucional de herramientas con criterios claros de selección por plataforma y artefacto. Priorizar Magnet AXIOM para investigaciones de correo y colaboración en entornos SaaS, y complementarlo con soluciones de código abierto como Autopsy para análisis de archivos y, cuando corresponda,

Volatility para memoria, además de utilidades nativas de los proveedores como Microsoft Purview eDiscovery, Google Vault, AWS CloudTrail y Azure Monitor. Documentar compatibilidades, limitaciones y guías de uso por versión, y promover ejercicios comparativos entre suites.

- Fortalecer el trabajo del equipo forense con manuales claros y una matriz de responsabilidades que indique quién hace qué y cuándo (primer respondedor, analista, custodio de evidencia, administrador de la nube y asesor legal). Unificar los documentos de uso diario —actas, registros de hash, bitácoras, listas de verificación y plantillas de informe— y añadir pasos concretos para casos de correo y colaboración en Microsoft 365 y Google Workspace, desde la solicitud de datos hasta la exportación, el sellado con hash y la custodia segura de la evidencia.
- Implantar una preparación forense institucional efectiva. Habilitar y retener registros nativos en los principales proveedores, establecer canales formales para la solicitud de datos y ejecutar simulacros periódicos que repliquen incidentes en correo, colaboración y cargas en IaaS y PaaS. Acompañar estas acciones con métricas de desempeño —tiempos de preservación, integridad verificada, completitud de evidencias— para elevar la eficacia operativa y la admisibilidad probatoria.

Bibliografía

Arsys. (4 de Abril de 2024). Obtenido de El análisis forense en la nube, conocido también como cloud forensics, se define como el conjunto de investigaciones centradas en los delitos informáticos que tienen lugar principalmente en entornos de computación en la nube .

Asamblea Nacional del Ecuador. (20 de Octubre de 2008). *Constitución de la República del Ecuador. Registro Oficial Suplemento 449*. Obtenido de https://www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf

Asamblea Nacional del Ecuador. (10 de Febreo de 2024). *Código Orgánico Integral Penal (COIP). Registro Oficial Suplemento 180*. Obtenido de https://www.funcionjudicial.gob.ec/pdf/COIP.pdf

Báez, J. (13 de Febrero de 2025). *DREAMLAB TECHNOLOGIES*. Obtenido de Principales desafíos del análisis forense digital en entornos cloud: https://dreamlab.net/es/blog/principales-desafios-del-analisis-forense-digital-en-entornos-cloud/#:~:text=El%20forense%20tradicional%20y%20el,entornos%20en%20los%20que%20operan

Barahona Robayo, F., & Mayorga Mayorga, E. (30 de Mayo de 2024). *La regulación del derecho a la privacidad en la era de la tecnología y la digitalización en Ecuador*. Obtenido de 593 Digital Publisher CEIT, ISSN-e 2588-0705, Vol. 9, Nº. Extra 3-1, 2024 (Ejemplar dedicado a: Special Edition), págs. 19-30: https://dialnet.unirioja.es/servlet/articulo?codigo=9966695

Burgos, A. P., Cruzado, J. G., & Seclen, J. (s.f.). *Almacenamiento de la evidencia digital usando Cloud Computing: Una revisión sistemática de la literatura.* Obtenido de Revista Peruana de Computación y Sistemas, 6(2), 65-77.: https://core.ac.uk/download/pdf/639702426.pdf

Chiun, F., & Enrique, J. (2024). *ISO 27037:2012 para mejorar el análisis informático forense en la nube.* Obtenido de Universidad Nacional Federico Villarreal: https://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/9138/UNFV_EUPG_Farfan_Chiun_Julio_Enrique_Maestria_2024.pdf?sequence=1

Comercio, E. (25 de Julio de 2025). *3183 delitos informáticos se han registrado en el Ecuador, desde el 2020*. Obtenido de https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

Echeverría Espinoza, E. A. (2024). *Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos y su perspectiva legal en Ecuador. Una revisión sistemática*. Obtenido de Universidad Católica de Cuenca: https://dspace.ucacue.edu.ec/handle/ucacue/18818

Ehigiator , E.-P., Idahosa, S., Asante , G., & Okungbowa , A. (29 de Abril de 2024). *Scientific Publications*. Obtenido de Estándares de investigación forense digital en la computación en la nube: https://www.scipublications.com/journal/index.php/ujcsc/article/view/923#:~:text=The%20absence%20of%20consistent%20standards,a%20comprehensive%20framework%20and%20enhanced

Gallegos Yánez, S. L., & Andrade Ulloa, D. L. (2025). *Análisis de errores en la cadena de custodia y su impacto en la confiabilidad de la evidencia*. Obtenido de Polo del Conocimiento: https://polodelconocimiento.com/ojs/index.php/es/article/view/9334

Globatika Lab. (18 de Junio de 2025). Obtenido de Forensia en la nube e infraestructuras híbridas actuales: https://peritosinformaticos.es/forensia-nube-infraestructuras-hibridas/#:~:text=Uno%20de%20los%20mayores%20desaf%C3%ADos,o%20requerir%20cooperaci%C3%B3n%20jur%C3%ADdica%20internacional

Gómez Flores, V. M. (12 de enero de 2024). *Forense digital: Cadena de custodia en casos de almacenamiento en nube.* Obtenido de BIBLIOTECA INFOTEC: https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/642/1/INFOTEC_MDTIC_VMGF_20022024.pdf

IETF. (2002). *RFC 3227: Guidelines for evidence collection and archiving.* . Obtenido de https://datatracker.ietf.org/doc/html/rfc3227

ISO. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. Obtenido de ISO: https://www.iso.org/es/contents/data/standard/04/43/44381.html

ISO. (2015). *Tecnología de la información — Técnicas de seguridad — Directrices para el análisis e interpretación de la evidencia digital*. Obtenido de ISO/IEC 27042:2015: https://www.iso.org/standard/44406.html

Ley Orgánica de Protección de Datos Personales. (2021). *Registro Oficial Suplemento 459, 26 de mayo de 2021.* Obtenido de https://www.registroficial.gob.ec

Linthicum, D. (24 de Septiembre de 2024). *InfoWorld*. Obtenido de El desafío de la informática forense en la nube: https://www.infoworld.com/article/3537036/the-challenge-of-cloud-computing-forensics.html#:~:text=The%20NISTIR%208006%20document%20addresses,voices%20are%20developing%20these%20solutions

Mintel. (2019). *Estrategia nacional de ciberseguridad del Ecuador 2020–2023.* Obtenido de https://www.telecomunicaciones.gob.ec

NIST. (2006). *Guide to integrating forensic techniques into incident response (SP 800-86)*. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Orna Lora, J. A. (24 de Enero de 2024). *Elaboración de una metodología de buenas prácticas del perito informático en Telecomunicaciones bajo la norma ISO 27037 para su aplicación en el Ecuador*. Obtenido de Universidad Técnica del Norte: http://repositorio.utn.edu.ec/handle/123456789/15464

Patau, M. (26 de Julio de 2023). *ackcent*. Obtenido de Todo lo que necesitas saber sobre el análisis forense en la nube: https://www.scribbr.es/citar/generador/folders/7LUWWoxEp66gQqzz3TrNiI/lists/28uZbcN2TGo7tqfDJ6dGEb/

Pita Vera, C. A. (6 de Febrero de 2024). *Análisis forense de evidencias digitales en entornos iCloud.* Obtenido de Universidad Estatal Península de Santa Elena: https://repositorio.upse.edu.ec/handle/46000/10940

Sanchez, M. M. (2025). *Analisis Forense en la Nube.* Obtenido de Manual docente, IES San Clemente: https://manuais.pages.iessanclemente.net/apuntes/ciberseguridad/forense/_index.files/15%20-%20An%C3%A1lisis%20Forense%20en%20la%20nube.pdf

Suárez Liriano, D. E., & Rocafuerte Del Pezo, E. R. (28 de Agosto de 2024). *El phishing como delito informático en el ámbito de las legislaciones de Ecuador, Argentina y España, 2023*. Obtenido de Universidad Estatal Península de Santa Elena: https://repositorio.upse.edu.ec/handle/46000/12104

Universo, E. (28 de Agosto de 2024). *Ciberataques en Ecuador aumentaron un 30 % durante el 2023, según analistas*. Obtenido de https://www.eluniverso.com/noticias/ecuador/ciberataques-ecuador-analistas-aumento-seguridad-nota/

Vaca, P. A., & Dulce-Villarreal, E. R. (01 de agosto de 2024). *Blockchain para asegurar la integridad y trazabilidad en la cadena de custodia de evidencia digital en informática forense: un estudio de mapeo sistemático.* Obtenido de TecnoLógicas: https://revistas.itm.edu.co/index.php/tecnologicas/article/view/3049

Vera, P., & Adrián, C. (06 de febrero de 2024). *Universidad Estatal Penisula de Santa Elena.* Obtenido de Repositorio Universidad Estatal Península de Santa Elena: https://repositorio.upse.edu.ec/handle/46000/10940

Yepez, A. (19 de Febrero de 2025). *Studocu.* Obtenido de Análisis DOFA de la norma ISO/IEC 27037 en el contexto forense: https://www.studocu.com/latam/document/universidad-nacional-abierta/analisis-ii/analisis-forence/123255876

Anexos

Anexo A Encuestas

Encuesta sobre Capacidades de Investigación Forense en la Nube

La presente encuesta fue elaborada por Jefferson Fernando Ramírez Lozada, estudiante de la Universidad Internacional del Ecuador (UIDE), como parte del trabajo de titulación. Su objetivo es evaluar el estado actual de conocimientos, herramientas, procedimientos y desafíos que enfrenta el personal encargado de la investigación forense de incidentes informáticos en entornos de computación en la nube.

Los resultados de esta encuesta servirán como insumo fundamental para el desarrollo de una guía de mejores prácticas que permita estandarizar los procedimientos técnicos y científicos, garantizando la validez probatoria de la evidencia digital recolectada en dichos entornos.

Sección 1. Acerca de usted

1. Nombres y Apellidos Completos
2. Institución/Organización
3. Cargo Actual
4. Correo Electrónico

Sección 2. Conocimientos Técnicos

5. ¿Cómo evaluaría su nivel de conocimiento sobre computación en la nube?
    - Ninguno
    - Básico
    - Intermedio
    - Avanzado
    - Experto
    - Otro
6. ¿Ha participado anteriormente en investigaciones forenses que involucren entornos de nube?
    - Sí
    - No
7. Si respondió afirmativamente, ¿en cuántos casos aproximadamente?
    - 1–3 casos
    - 4–10 casos
    - Más de 10 casos

8. ¿Con qué proveedores de servicios en la nube está familiarizado? (Marque todas las que correspondan)
    - Amazon Web Services (AWS)
    - Microsoft Azure
    - Google Cloud Platform
    - IBM Cloud
    - Oracle Cloud
    - Otro
9. En su experiencia con investigaciones forenses en la nube, ¿qué tipos de delitos informáticos ha encontrado con mayor frecuencia? (Marque hasta 5)
    - Fraude y estafas en línea
    - Robo o filtración de datos personales
    - Violación de propiedad intelectual/piratería
    - Suplantación de identidad (phishing)
    - Extorsión digital / ransomware
    - Pornografía infantil / explotación de menores
    - Ciberterrorismo
    - Ataques DDoS
    - Ciberespionaje corporativo o estatal
    - Hackeo de cuentas o servicios en la nube
    - Lavado de dinero con criptomonedas
    - Acoso cibernético
    - Comercio ilegal en darknet
    - Vulneración de sistemas críticos
    - Otro

Sección 3. Herramientas y Metodologías

10. ¿Qué herramientas forenses en la nube ha utilizado? (Marque todas las que correspondan)

- AWS CLI para registros
- Azure Forensics Tools
- GCP Forensic Tools
- Cellebrite Cloud Analyzer
- Magnet AXIOM Cloud
- Oxygen Forensic Cloud Extractor
- Herramientas internas de la institución
- Otro

11. ¿Qué estándares o marcos metodológicos utiliza?

- ISO/IEC 27037
- NIST Cloud Computing Forensic Science Challenges
- CSA Cloud Security Alliance Guidelines
- RFC 3227
- Guías propias de la institución

- Otro

12. En una escala del 1 al 5, ¿cómo calificaría la dificultad del proceso de obtención de evidencia digital en la nube?

- 1 Muy difícil
- 2
- 3
- 4
- 5 Muy fácil

Sección 4. Desafíos y Necesidades

13. Principales desafíos en investigaciones forenses en la nube (máximo 3)

- Jurisdicción y aspectos legales
- Volatilidad de la evidencia
- Acceso a datos por parte del proveedor
- Falta de herramientas especializadas
- Falta de capacitación
- Falta de cooperación de proveedores
- Cadena de custodia
- Otro

14. Recursos necesarios para mejorar las investigaciones (marque todos los que correspondan)

- Guías procedimentales específicas
- Herramientas especializadas
- Capacitación técnica
- Acuerdos con proveedores
- Mejora del marco legal
- Otro

15. ¿Existe un procedimiento estandarizado en su institución?

- Sí
- No
- En desarrollo
- Desconozco

Sección 5. Marco Legal y Cooperación

16. Nivel de conocimiento sobre marco legal aplicable a la obtención de evidencia en la nube:

- Ninguno
- Básico
- Intermedio
- Avanzado
- Experto

17. ¿Ha solicitado datos a proveedores de nube en investigaciones?

- Sí
- No

18. Si respondió afirmativamente, ¿cómo calificaría el nivel de cooperación de los proveedores?

- Muy deficiente
- Deficiente
- Aceptable
- Bueno
- Excelente

19. ¿Son suficientes los acuerdos internacionales para facilitar la obtención de evidencia digital en la nube?

- Sí
- No
- Parcialmente
- Desconozco

Sección 6. Observaciones Finales

20. ¿Qué aspectos considera prioritarios en una guía de mejores prácticas para investigaciones forenses en la nube?
    (Texto de una sola línea)
21. ¿Alguna observación o sugerencia adicional?
    (Texto de una sola línea)

ENCUESTA SOBRE CAPACIDADES DE INVESTIGACIÓN FORENSE EN LA NUBE

La presente encuesta ha sido desarrollada por Jefferson Fernando Ramírez Lozada, estudiante de la Universidad Internacional del Ecuador (UIDE), como parte de su trabajo de tesis. Tiene como objetivo evaluar el estado actual de conocimientos, herramientas, procedimientos y desafíos que enfrenta el personal que se encarga de la investigación forense de incidentes informáticos ocurridos en entornos de computación en la nube. Los resultados obtenidos servirán como insumo fundamental para el desarrollo de una guía de mejores prácticas que estandarice los procedimientos técnicos y científicos, garantizando la validez probatoria de la evidencia digital obtenida en estos entornos.

Sección 1 ...

Acerca de usted

Su información es extremadamente confidencial, la siguiente información es solo para fines de investigación internos, toda la información no se compartirá externamente.

1. Nombres y Apellidos Completos *

Escriba su respuesta

2. Institución/Organización: *

Escriba su respuesta

3. Cargo Actual *

Escriba su respuesta

4. Correo Electrónico *

Sección 2

Conocimientos Técnicos

5. ¿Cómo evaluaría su nivel de conocimiento sobre computación en la nube?

*

- ◯ Ninguno
- ◯ Básico
- ◯ Intermedio
- ◯ Avanzado
- ◯ Experto
- ◯ Otras

6. ¿Ha participado anteriormente en investigaciones forenses que involucren entornos de nube?

*

- ◯ Sí
- ◯ No

7. Si respondió afirmativamente a la pregunta anterior, ¿en cuántos casos aproximadamente?

- ○ 1-3 casos
- ○ 4-10 casos
- ○ Más de 10 casos

8. ¿Con qué proveedores de servicios en la nube está familiarizado? (Marque todos los que correspondan)

*

Marque todas las opciones que correspondan.

- ☐ Amazon Web Services (AWS)
- ☐ Microsoft Azure
- ☐ Google Cloud Platform
- ☐ IBM Cloud
- ☐ Oracle Cloud
- ☐ Otras

9. En su experiencia con investigaciones forenses en entornos de nube, ¿cuáles son los tipos de delitos informáticos más frecuentes que ha encontrado? (Marque hasta 5 opciones)

*

Seleccione como máximo 5 opciones.

- [ ] Fraude y estafas en línea
- [ ] Robo o filtración de datos personales
- [ ] Violación de propiedad intelectual/piratería
- [ ] Suplantación de identidad (phishing)
- [ ] Extorsión digital/ransomware
- [ ] Pornografía infantil/explotación de menores
- [ ] Ciberterrorismo
- [ ] Ataques de denegación de servicio (DDoS)
- [ ] Ciberespionaje corporativo o estatal
- [ ] Hackeo de cuentas/servicios en la nube
- [ ] Lavado de dinero mediante criptomonedas
- [ ] Acoso cibernético
- [ ] Comercio ilegal en darknet
- [ ] Vulneración de sistemas críticos

10. ¿Qué herramientas de investigación forense para entornos en la nube ha utilizado? (Marque todas las que correspondan)

*

- [ ] AWS CLI para acceso a registros
- [ ] Azure Forensics Tools
- [ ] GCP Forensic Tools
- [ ] Cellebrite Cloud Analyzer
- [ ] Magnet AXIOM Cloud
- [ ] Oxygen Forensic Cloud Extractor
- [ ] Herramientas propias de la institución
- [ ] Otras

11. ¿Qué estándares o marcos metodológicos utiliza para la investigación forense en la nube? *

- ( ) ISO/IEC 27037
- ( ) NIST Cloud Computing Forensic Science Challenges
- ( ) CSA Cloud Security Alliance Guidelines
- ( ) RFC 3227
- ( ) Guías propias de la institución

12. En una escala del 1 al 5, donde 1 es "Muy difícil" y 5 es "Muy fácil", **¿cómo calificaría el proceso de obtención de evidencia digital de entornos en la nube?** *

1	2	3	4	5

Muy difíci Muy fácil

Sección 4

Desafíos y Necesidades

13. ¿Cuáles considera que son los principales desafíos al realizar investigaciones forenses en entornos de nube? (Marque hasta 3 opciones)

Seleccione como máximo 3 opciones.

- [ ] Jurisdicción y aspectos legales
- [ ] Volatilidad de la evidencia
- [ ] Acceso a los datos por parte de los proveedores
- [ ] Falta de herramientas especializadas
- [ ] Falta de capacitación
- [ ] Falta de cooperación de los proveedores de servicios
- [ ] Cadena de custodia

14. ¿Qué recursos o capacitaciones considera necesarios para mejorar las investigaciones forenses en la nube? (Marque todas las que correspondan)

*

- [ ] Guías procedimentales específicass
- [ ] Herramientas especializadas
- [ ] Capacitación técnica
- [ ] Acuerdos con proveedores de servicios
- [ ] Mejora del marco legal
- [ ] Otras

15. ¿Existe algún procedimiento estandarizado en su institución para la investigación forense en la nube?

- ( ) Sí
- ( ) No
- ( ) En desarrollo
- ( ) Desconozco

Sección 5

Marco Legal y Cooperación

16. ¿Cuál es su nivel de conocimiento sobre el marco legal aplicable a la obtención de evidencia digital en entornos de nube?

- ◯ Ninguno
- ◯ Básico
- ◯ Intermedio
- ◯ Avanzado
- ◯ Experto

17. ¿Ha tenido experiencia solicitando datos a proveedores de servicios en la nube durante investigaciones?

- ◯ Sí
- ◯ No

18. Si respondió afirmativamente a la pregunta anterior, ¿cómo calificaría el nivel de cooperación de los proveedores de servicios en la nube?

- ◯ Muy deficiente
- ◯ Deficiente
- ◯ Aceptable
- ◯ Bueno
- ◯ Excelente

19. ¿Considera que los acuerdos internacionales actuales son suficientes para facilitar la obtención de evidencia digital en la nube?

- ◯ Sí
- ◯ No
- ◯ Parcialmente
- ◯ Desconozco los acuerdos existentes

Sección 6

Observaciones Finales

20. ¿Qué aspectos considera prioritarios para incluir en una guía de mejores prácticas para la investigación forense en la nube?

Escriba su respuesta

21. ¿Alguna observación o sugerencia adicional que desee aportar?

Escriba su respuesta

⊕ Agregar nueva pregunta

Anexo B Informe Final de la Guía

Elaboración de una guía con las mejores prácticas entre estándares, herramientas y procedimientos para la investigación forense orientada a incidentes informáticos en la nube

Proyecto: Jefferson Fernando Ramirez Lozada

22/09/2025

Contenido

2 Descripción general

2.1 Perspectiva del producto

La guía metodológica es un producto independiente que actúa como manual de referencia para investigaciones forenses en entornos de computación en la nube. No forma parte de un software mayor, aunque puede ser utilizada en conjunto con herramientas forenses (Magnet AXIOM, FTK Imager, Autopsy, etc.) y con plataformas cloud (AWS, Microsoft 365, Google Workspace). Su rol es servir como un marco normativo, técnico y práctico, aplicable tanto en investigaciones reales como en procesos de formación académica.

2.2 Funcionalidad del producto

El propósito central de la guía es:

- Orientar paso a paso la investigación forense en la nube.
- Establecer protocolos claros para identificación, adquisición, preservación, análisis y presentación de evidencia.
- Integrar estándares internacionales (ISO/IEC 27037, ISO/IEC 27042, NIST SP 800-86, RFC 3227).
- Asegurar compatibilidad con el marco legal ecuatoriano (COIP, LOPDP, Ley de Comercio Electrónico).
- Proveer plantillas, formatos y checklists para facilitar la trazabilidad y uniformidad de la documentación.
- Ser un material didáctico en programas académicos de Ingeniería en TI y un recurso de consulta para profesionales forenses.

2.3 Características de los usuarios

Rol de usuario	Docentes, estudiantes de Ingeniería en Tecnologías de la Información, peritos forenses, personal de áreas de seguridad informática.
Tipo de usuario:	Académico y profesional.
Nivel de acceso:	Uso libre en el ámbito educativo; de aplicación formal en procesos judiciales cuando lo empleen peritos acreditados.
Actividades	Uso libre en el ámbito educativo; de aplicación formal en procesos judiciales cuando lo empleen peritos acreditados.

Descripción de los usuarios del producto

Los principales usuarios de la guía metodológica son estudiantes, docentes y profesionales vinculados al área de Tecnologías de la Información y la Informática Forense. Su perfil se caracteriza por los siguientes aspectos:

- Nivel educacional: La guía está orientada a estudiantes de pregrado en Ingeniería en Tecnologías de la Información, docentes universitarios y profesionales en ejercicio en áreas de ciberseguridad o peritaje digital. Se asume un nivel mínimo de formación técnica en informática, equivalente a los primeros ciclos de estudios universitarios.

- Experiencia previa: Los usuarios poseen conocimientos básicos o intermedios en el manejo de sistemas operativos, redes y servicios en la nube. En el caso de docentes y profesionales, cuentan además con experiencia en docencia, administración de infraestructuras TI o en la aplicación de procedimientos de seguridad informática.

- Experiencia técnica:

  El nivel de experticia técnica varía según el rol:

  - **Estudiantes**: Nivel inicial o medio; requieren guías paso a paso, plantillas y ejemplos prácticos para reforzar el aprendizaje.

  - **Docentes**: Nivel intermedio o avanzado; buscan en la guía un recurso didáctico que puedan aplicar en prácticas académicas y proyectos formativos.

  - **Profesionales forenses**: Nivel avanzado; utilizan la guía como marco metodológico y legal de referencia para la investigación de incidentes reales en entornos cloud.

En este sentido, la guía ha sido diseñada para adaptarse a distintos niveles de usuario: servir como recurso académico en la formación de futuros ingenieros en TI y, al mismo tiempo, constituirse en un manual de consulta aplicable en el ámbito profesional y judicial.

3 Requisitos específicos

Número de requisito	RF01
Nombre de requisito	La guía debe contar con una estructura adecuada, entendible para seguir el procedimiento del análisis forense en la nube.
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la fiscalía general del Estado
Prioridad del requisito	☐ Alta/Esencial ☒ Media/Deseado ☐ Baja/ Opcional

Número de requisito	RF02
Nombre de requisito	La guía debe detallar un protocolo apropiado para el manejo eficiente de la evidencia digital.
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la fiscalía general del Estado
Prioridad del requisito	☒Alta/Esencial ☐Media/Deseado ☐ Baja/ Opcional

Número de requisito	RF03
Nombre de requisito	La guía debe incluir procedimientos bajo normas y estándares internacionales que permita la investigación forense en la nube.
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☒Alta/Esencial ☐Media/Deseado ☐ Baja/ Opcional

Número de requisito	RF04
Nombre de requisito	La guía debe estar alineada con la normativa legal ecuatoriana vigente.
Tipo	X Requisito ☐ Restricción

Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☒Alta/Esencial ☐Media/Deseado ☐ Baja/ Opcional

Número de requisito	RF05
Nombre de requisito	La guía debe listar los tipos de delitos informáticos más frecuentes en la web.
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☐Alta/Esencial ☒Media/Deseado ☐ Baja/ Opcional

Número de requisito	RF06
Nombre de requisito	Se debe integrar en la guía las mejores herramientas para el análisis forense en la nube
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☒Alta/Esencial ☐Media/Deseado ☐ Baja/ Opcional

Número de requisito	RF07
Nombre de requisito	La guía debe establecer las plantillas y formatos adecuados para llevar el control en el proceso del análisis forense en la nube
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☐ Alta/Esencial ☒Media/Deseado ☐ Baja/ Opcional

Número de requisito	RF08
Nombre de requisito	Validar la guía por un perito informático.
Tipo	X Requisito ☐ Restricción
Fuente del requisito	Encuesta al responsable de investigación digital de la Fiscalía
Prioridad del requisito	☐ Alta/Esencial ☒Media/Deseado ☐ Baja/ Opcional

3.1 Requisitos funcionales

3.1.1 Requisito funcional 1: Definición de roles y responsabilidades

Este requisito establece que la guía debe definir de manera clara la estructura del equipo de trabajo encargado de la investigación forense en la nube. Incluye la asignación de funciones específicas para el Coordinador Forense, Analista Forense Digital, Especialista en Infraestructura Cloud, Asesor Jurídico y Custodio de Evidencias, con el fin de asegurar trazabilidad y coordinación en cada fase del proceso

3.1.2 Requisito funcional 2: Procedimientos para manejo de evidencia digital

La guía debe contener protocolos detallados para la identificación, adquisición, preservación, transporte y almacenamiento de la evidencia digital en la nube, garantizando la integridad de los datos mediante el uso de cadenas de custodia, verificación de hashes y documentación exhaustiva en bitácoras.

3.1.3 Requisito funcional 3: Metodología basada en estándares internacionales

El producto debe incorporar un marco metodológico alineado con normas internacionales como ISO/IEC 27037, ISO/IEC 27042, NIST SP 800-86 y RFC 3227, que aseguren procesos estructurados, reproducibles y con validez legal.

3.1.4 Requisito funcional 4: Alineación con normativa legal nacional

La guía debe estar en concordancia con el Código Orgánico Integral Penal (COIP), la Ley Orgánica de Protección de Datos Personales y la Ley de Comercio Electrónico, asegurando que la obtención y el análisis de la evidencia digital respeten el debido proceso y la legalidad vigente en Ecuador.

3.1.5 Requisito funcional 5: Identificación de delitos informáticos frecuentes

La guía debe incluir una clasificación de los principales delitos informáticos en entornos cloud, como phishing, ransomware, fraude electrónico y accesos no autorizados, sustentada en estadísticas oficiales y reportes de organismos especializados.

3.1.6 Requisito funcional 6: Identificación de delitos informáticos frecuentes

La guía debe integrar un catálogo comparativo de herramientas de uso práctico (Magnet AXIOM, FTK Imager, Autopsy, Volatility, AWS CloudTrail, entre otras), evaluando su compatibilidad, licenciamiento y aceptación judicial, para facilitar la selección según el tipo de incidente.

3.1.7 Requisito funcional 7: Identificación de delitos informáticos frecuentes

El documento debe proveer formatos oficiales para cadena de custodia, actas, checklists, bitácoras y reportes periciales, con el objetivo de uniformar la documentación y garantizar la trazabilidad de la evidencia en cada fase de la investigación.

3.1.8 Requisito funcional 8: Identificación de delitos informáticos frecuentes

La guía debe ser probada en entornos reales simulados, mediante casos prácticos aplicados en plataformas como AWS y Microsoft 365, verificando su pertinencia técnica, su utilidad académica y su viabilidad en procesos judiciales.

Anexo C Informe Final de la Guía

INFORME FINAL DEL ANÁLISIS FORENSE EN LA NUBE

18-9-2025

Guía metodológica para el análisis forense digital en plataformas de la nube

Jefferson Fernando Ramirez Lozada

[NOMBRE DE LA EMPRESA]

INFORME FINAL DEL ANALISIS FORENSE EN LA NUBE

PROCESO ESTIPULADO EN LA GUIA CON LAS MEJORES ESTANDARES, Y HERRAMIENTAS PARA EL ANALISIS FORENSE EN LA NUBE

Fecha y hora de recepción de la orden pericial: En este campo deberá consignarse la fecha y hora exacta en la que el perito recibió la orden judicial o fiscal que dispuso la práctica de la pericia.	**INFORME TÉCNICO PERICIAL Nro.** Aquí se registrará el número correlativo del informe pericial, conforme el sistema de control interno del perito o de la institución a la que pertenezca.
Número de proceso	Se deberá anotar el número de expediente judicial o de indagación previa con el que se relaciona el análisis forense.

1. OBJETIVO DE LA INVESTIGACIÓN

En este apartado se establecerá de manera clara el propósito de la pericia, especificando qué se busca determinar. Ejemplo: comprobar la existencia de accesos no autorizados, identificar la procedencia de los mismos, verificar la integridad de la evidencia digital o establecer la magnitud del incidente.

2. ANTECEDES

Se describirá el contexto que dio lugar a la investigación, precisando la denuncia presentada, la autoridad solicitante, las fechas relevantes y una breve exposición de los hechos reportados. Asimismo, se delimitará el objeto de la pericia conforme lo ordenado por la autoridad competente.

3. DATOS DEL PROVEEDOR DE SERVICIOS EN LA NUBE

Proveedor de Cloud: Se deberá consignar el nombre completo del proveedor (ej. Amazon Web Services,	Tipo de Plataforma: IaaS ☒PaaS ☐ SaaS ☒

Microsoft Azure, Google Cloud Platform, Microsoft 365).	
Servicio Afectado: Se especificará el servicio concreto en el que se detectó el incidente (ej. EC2, S3, OneDrive, Exchange Online)..	Región o Zona: **:** Se anotará la localización del servicio en la nube (ej. us-east-2, Europa Oeste).
Url: Dirección o endpoint del recurso comprometido.	Credenciales Otorgadas: Si ☐No ☐
Medio de preservación: Snapshot ☐ / Imagen RAW ☐ / Logs exportados ☒ / Otro ☒	Hash Calculado: Aquí se registrará el valor hash (SHA-256, SHA-512) correspondiente a la evidencia.
Fecha de activación (Tiempo cero): **Fecha y hora en que el perito inició formalmente el procedimiento forense.**	Estado de los servicios: Encendido ☐ / Apagado ☐ / Suspendido ☐
Id de la cuenta / Correo electrónico: Se anotará el identificador de la cuenta o el correo vinculado al servicio.	
Descripción: Breve reseña del recurso analizado (ej. “Servidor web vulnerado”, “Cuenta de correo comprometida”).	

4. **EVALUACIÓN DEL INCIDENTE**

Evidencias preliminares identificadas: Relación de archivos, logs o imágenes forenses recolectadas.
Clasificación del incidente: Tipología (intrusión, malware, fuga de información, phishing, ataque DDoS, etc.).
Activos comprometidos: Enumeración de los sistemas, bases de datos o servicios afectados.
Alcance inicial estimado del incidente: Determinación del impacto preliminar (un usuario, varios servidores, múltiples servicios).

Riesgo asociado: Evaluación del nivel de riesgo técnico, operativo o legal.

Medidas inmediatas de contención aplicadas: Acciones realizadas para evitar la propagación o agravar el incidente (ej. aislamiento de instancias, suspensión de credenciales).

Responsable de la evaluación: Identificación del perito o equipo a cargo de la fase de evaluación.

5. Metodología aplicada

Se describirán los estándares y normas empleadas, las herramientas utilizadas y el procedimiento metodológico seguido.
Se deberán detallar las fases aplicadas: identificación, preservación, adquisición, análisis y presentación de los hallazgos.

6. Conclusiones

En este punto se emitirán los resultados técnicos de la investigación, de manera clara, objetiva y sustentada. Las conclusiones deberán responder únicamente al objeto de la pericia y pueden referirse, entre otros, a:

- La confirmación o descarte de un incidente.
- La tipología del ataque o evento detectado.
- El alcance sobre los activos comprometidos.
- La integridad y autenticidad de la evidencia obtenida.

7. DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO.

Se adjuntará y describirá la documentación de soporte, tales como capturas de pantalla, bitácoras, registros de logs, tablas de hashes, copias de cadena de custodia, reportes de herramientas o diagramas explicativos.
Asimismo, se justificará técnicamente cómo cada documento respalda las conclusiones presentadas..

8. DECLARACIÓN DEL PERITO

El perito deberá declarar bajo juramento que el presente informe se elaboró de manera independiente, que corresponde a su real convicción profesional y que toda la información proporcionada es verdadera.

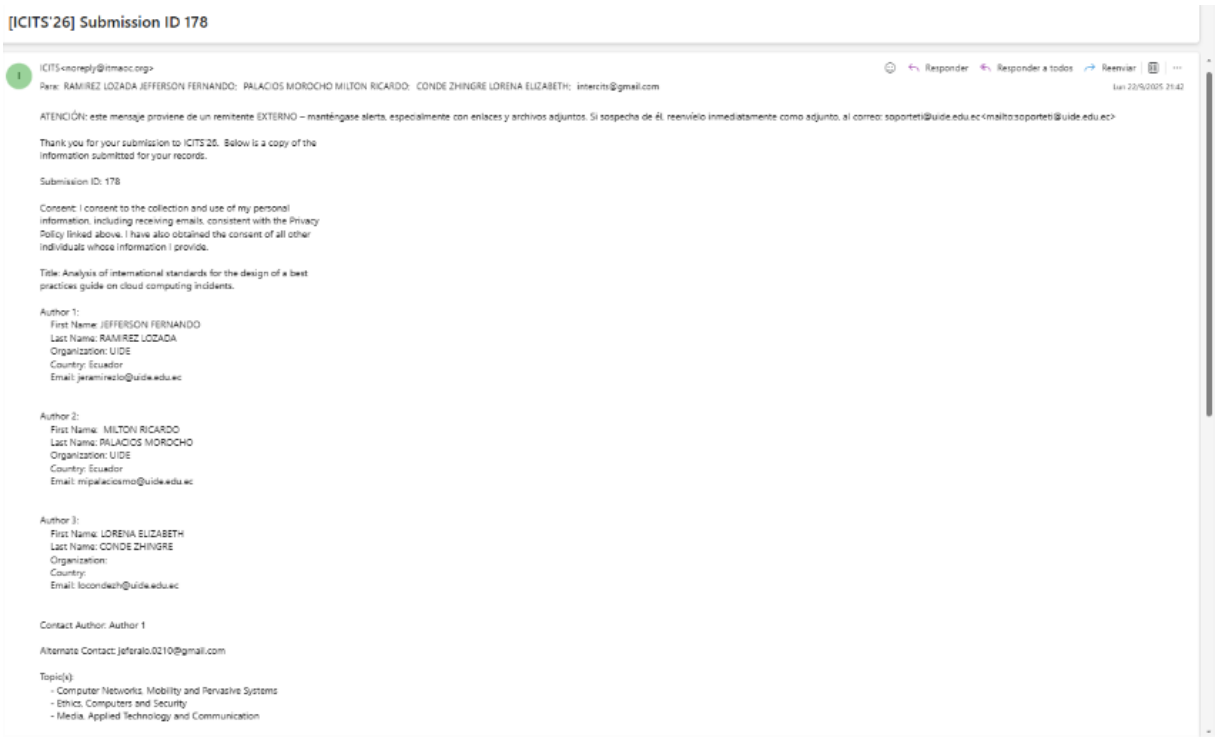
9. **FIRMA DE RESPONSABILIDAD**

Nombres Completos	Firma
Se consignará el nombre completo del perito.	
Especialidad: Se anotará el área profesional específica.	Área De Acreditación: Se indicará la entidad de acreditación
Teléfono: Número de contacto.	Correo: Dirección de correo electrónico válida.

Anexo D Evidencia del articulo

Evidencia Del Artículo Risti- información

Autor	Nombre completo	Afiliación institucional	País	Correo electrónico	Rol / Contribución
Autor 1	Jefferson Fernando Ramírez Lozada	Universidad Internacional del Ecuador (UIDE) – Campus Loja, Escuela de Ingeniería en Tecnologías de la Información	Ecuador	jeramirezlo@uide.edu.ec	Autor principal / Investigador
Autor 2	Milton Ricardo Palacios Morocho	Universidad Internacional del Ecuador (UIDE) – Campus Loja, Escuela de Ingeniería en Tecnologías de la Información	Ecuador	mipalaciosmo@uide.edu.ec	Tutor de tesis / Coautor
Autor 3	Lorena Elizabeth Conde Zhingre	Universidad Internacional del Ecuador (UIDE) – Campus Loja, Escuela de Ingeniería en Tecnologías de la Información	Ecuador	locondezh@uide.edu.ec	Directora de carrera / Coautora



[ICITS'26] Submission ID 178

ICITS<noreply@itmaoc.org>

Responder | Responder a todos | Reenviar

Para: RAMIREZ LOZADA JEFFERSON FERNANDO; PALACIOS MOROCHO MILTON RICARDO; CONDE ZHINGRE LORENA ELIZABETH; intercits@gmail.com

lun 22/9/2025 21:42

ATENCIÓN: este mensaje proviene de un remitente EXTERNO – manténgase alerta, especialmente con enlaces y archivos adjuntos. Si sospecha de él, reenvíelo inmediatamente como adjunto, al correo: soporteti@uide.edu.ec<mailto:soporteti@uide.edu.ec>

Thank you for your submission to ICITS'26. Below is a copy of the information submitted for your records.

Submission ID: 178

Consent: I consent to the collection and use of my personal information, including receiving emails, consistent with the Privacy Policy linked above. I have also obtained the consent of all other individuals whose information I provide.

Title: Analysis of international standards for the design of a best practices guide on cloud computing incidents.

Author 1:
- First Name: JEFFERSON FERNANDO
- Last Name: RAMIREZ LOZADA
- Organization: UIDE
- Country: Ecuador
- Email: jeramirezlo@uide.edu.ec

Author 2:
- First Name: MILTON RICARDO
- Last Name: PALACIOS MOROCHO
- Organization: UIDE
- Country: Ecuador
- Email: mipalaciosmo@uide.edu.ec

Author 3:
- First Name: LORENA ELIZABETH
- Last Name: CONDE ZHINGRE
- Organization:
- Country:
- Email: locondezh@uide.edu.ec

Contact Author: Author 1

Alternate Contact: jeferalo.0210@gmail.com

Topic(s):
- Computer Networks, Mobility and Pervasive Systems
- Ethics, Computers and Security
- Media, Applied Technology and Communication

Anexo E Guía con las mejores prácticas entre estándares, herramientas y procedimientos para investigación forense orientado a incidentes informáticos en la nube.

GUÍA PARA LA INVESTIGACIÓN FORENSE ORIENTADO A INCIDENTES INFORMÁTICOS EN LA NUBE.

Nombre: Jefferson Ramirez Lozada

01/09/2025

TABLA DE CONTENIDOS

Índice de Tablas

Índice de Ilustraciones

1. Introducción

La presente guía de mejores prácticas está diseñada para orientar el proceso técnico de investigación forense en incidentes informáticos ocurridos en entornos de computación en la nube. Su elaboración se basa en estándares internacionales reconocidos como ISO/IEC 27037:2012, ISO/IEC 27042:2015, ISO/IEC 27043:2015, la guía RFC 3227 y el NIST SP 800-86, que en conjunto establecen procedimientos para la identificación, preservación, análisis y presentación de evidencia digital.

Además, se toma en cuenta el marco legal ecuatoriano, específicamente el Código Orgánico Integral Penal (COIP), que regula la obtención y validez de la prueba digital dentro del país. El objetivo es que los procedimientos que se detallan en esta guía puedan ser aplicados por peritos informáticos, especialistas en seguridad y equipos de respuesta a incidentes, asegurando que la evidencia recolectada cumpla tanto con criterios técnicos como legales (Asamblea Nacional de Ecuador, 2014).

La guía incluye el análisis de estándares, la selección adecuada de herramientas forenses compatibles con entornos cloud, y la aplicación de protocolos adaptados a plataformas como Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP). También se detallan los roles y responsabilidades del personal forense, así como el proceso de acceso y extracción de datos en la nube, asegurando en todo momento la trazabilidad e integridad de la información (AWS Security Incident Response User Guide, 2024).

El cumplimiento de esta guía permite estandarizar las acciones durante una investigación, reducir errores durante la recolección de evidencia y facilitar la presentación de informes válidos ante procesos judiciales, fortaleciendo así la capacidad de respuesta ante incidentes informáticos en Ecuador.

2. Objetivos

Objetivo General

Establecer un procedimiento técnico y científico en la investigación forense de incidentes informáticos ocurridos en entornos de computación en la nube, con base en estándares internacionales, herramientas especializadas y el marco legal vigente en Ecuador.

Objetivo Especifico

a. Obtener todas las mejores prácticas que utilizan los expertos informáticos en casos de incidente informáticos en el entorno de la nube.
b. Proponer un procedimiento forense para los incidentes en la nube, que abarque las fases de identificación, recolección, adquisición, preservación, análisis y presentación de la evidencia digital, conforme a marcos normativos internacionales.
c. Recomendar herramientas forenses especializadas, que asegure la compatibilidad con infraestructuras cloud públicas, privadas e híbridas, y su capacidad de mantener la integridad de la evidencia digital.
d. Considerar el marco legal ecuatoriano, como el Código Orgánico Integral Penal (COIP), la Ley Orgánica de Protección de Datos Personales (LOPDP), y la Ley de Comercio Electrónico, garantizando el manejo adecuado de la prueba digital en el contexto judicial.
e. Proporcionar formatos y plantillas forenses editables, incluyendo cadena de custodia, bitácora forense y estructura de informe, que faciliten la trazabilidad y documentación durante todo el proceso investigativo

3. Alcance

La presente guía tiene como alcance principal establecer un conjunto de buenas prácticas, estándares y procedimientos para llevar a cabo investigaciones forenses en incidentes informáticos que involucren entornos de computación en la nube. Su aplicación está dirigida a profesionales forenses, equipos de respuesta a incidentes (CSIRT), peritos informáticos y personal técnico responsable de la recolección y análisis de evidencia digital en entornos virtualizados.

La guía contempla incidentes que afecten plataformas de servicios en la nube como Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS), incluyendo proveedores como Amazon Web Services (AWS), Microsoft Azure. También es aplicable a arquitecturas híbridas y privadas que utilicen tecnologías de virtualización, contenedores o servicios distribuidos.

Los procedimientos descritos en este documento cubren las fases esenciales del análisis forense digital: identificación, preservación, recolección, análisis y presentación de evidencia, bajo lineamientos internacionales y normativas nacionales. El contenido se ajusta al contexto legal de Ecuador, asegurando que las prácticas propuestas sean válidas y aplicables dentro del marco jurídico local.

No se incluye en esta guía el desarrollo de herramientas forenses propias ni la ejecución de pruebas de laboratorio especializadas. El enfoque está centrado en el uso de herramientas ya existentes, reconocidas y probadas en el ámbito profesional forense.

4. Roles y Responsables

Para asegurar una correcta ejecución del proceso forense en entornos de computación en la nube, se recomienda definir los roles y responsabilidades de cada miembro del equipo técnico. A continuación, se detallan los principales perfiles involucrados:

Mediante la documentación realizada en múltiples casos de estudios es recomendable trabajar con los siguientes grupos

A. Coordinador Forense / Líder de Investigación

- Supervisar todas las fases del proceso forense.
- Coordinar la comunicación entre las partes involucradas (empresa afectada, proveedores cloud, autoridades legales).
- Aprobar el plan de trabajo, asegurar el cumplimiento del marco legal y garantizar la integridad de la evidencia.
- Validar informes técnicos finales y presentaciones ante instancias judiciales si es necesario.

B. Especialista Forense Digital

- Ejecutar las tareas técnicas de identificación, recolección, preservación y análisis de evidencia digital.
- Utilizar herramientas forenses validadas y documentar cada paso conforme a estándares establecidos.
- Generar reportes preliminares sobre hallazgos técnicos.
- Garantizar la trazabilidad y autenticidad de la evidencia extraída del entorno cloud.

C. Especialista en Infraestructura Cloud

- Asistir en el acceso técnico a las plataformas afectadas (AWS, Azure, GCP, etc.).
- Brindar información sobre configuraciones, registros (logs), snapshots, tráfico de red y recursos desplegados.
- Colaborar en la identificación de vectores de ataque o fallas de configuración que hayan permitido el incidente.
- Generar respaldos de entornos críticos bajo supervisión del analista forense.

D. Responsable Legal / Asesor Jurídico

- Verificar que los procedimientos aplicados cumplan con el marco legal vigente (COIP).
- Asistir en la redacción de informes de validez jurídica de la prueba digital.

- Coordinar con autoridades judiciales o fiscales cuando se requiere autorización para intervención en sistemas o acceso a datos sensibles.
- Validar la cadena de custodia de la evidencia.

E. Custodio de la Evidencia

- Mantener y documentar la cadena de custodia de todo elemento recolectado.
- Almacenar de manera segura los medios digitales con evidencia, aplicando controles de acceso y registros de auditoría.
- Entregar evidencia solo bajo autorización del Coordinador Forense o por requerimiento legal.

Nota: En organizaciones pequeñas, un mismo individuo puede asumir múltiples roles, pero siempre se debe garantizar la independencia del análisis y la adecuada supervisión. Por ejemplo, el analista forense no debería ser la misma persona que custodia la evidencia sin una doble verificación, para asegurar objetividad y control.

5. Marco Legal Aplicable a la Investigación Forense en la Nube en Ecuador

La investigación forense digital en entornos de computación en la nube en Ecuador debe desarrollarse dentro de un marco legal que garantice la legalidad, integridad y admisibilidad de las evidencias digitales obtenidas. A continuación, se detallan las principales normativas nacionales que rigen esta materia:

5.1 Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)

La LOTAIP establece el derecho de los ciudadanos a acceder a la información pública y regula su manejo por parte de las instituciones del Estado. En el contexto forense, esta ley permite solicitar información relevante almacenada en la nube por entidades públicas, siempre que no esté clasificada como reservada o confidencial.

- **Artículo 2:** Define la información pública como todo documento en cualquier formato que repose en instituciones públicas o privadas que manejen fondos públicos.
- **Artículo 5:** Establece que la información pública debe ser accesible, oportuna, completa y fidedigna.
- **Artículo 6:** Señala que la información confidencial, como la personal, no está sujeta al principio de publicidad y su uso indebido puede dar lugar a acciones legales.

Aplicación forense: Los investigadores deben solicitar formalmente la información necesaria, garantizando la protección de datos personales y respetando las restricciones legales vigentes.

5.2 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Esta ley otorga validez jurídica a los documentos electrónicos, mensajes de datos y firmas electrónicas, equiparándolos a los documentos físicos tradicionales (Asamblea Nacional de Ecuador, 2014).

- **Artículo 8:** Establece que los mensajes de datos deben conservarse íntegros, accesibles y en su formato original o en uno que reproduzca con exactitud la información.
- **Artículo 52:** Reconoce los mensajes de datos, documentos y firmas electrónicos como medios de prueba válidos.
- **Artículo 54:** Regula la práctica de la prueba electrónica, exigiendo la presentación de soportes informáticos y transcripciones cuando sea necesario.

Aplicación forense: Las evidencias digitales obtenidas de entornos cloud deben conservarse de manera que se garantice su integridad y autenticidad, cumpliendo con los requisitos establecidos para su admisión como prueba en procesos judiciales.

5.3 Ley de Telecomunicaciones

Esta ley regula la instalación, operación y utilización de sistemas de telecomunicaciones en el país (Ecuador, Ley especial de Telecomunicaciones , 2014).

- **Artículo 10:** Prohíbe la interceptación o interferencia de sistemas de telecomunicaciones públicos sin autorización.
- **Artículo 11:** Prohíbe el uso de medios de telecomunicación contra la seguridad del Estado, el orden público, la moral y las buenas costumbres.
- **Artículo 14:** Garantiza el derecho al secreto y a la privacidad de las telecomunicaciones, prohibiendo su interceptación sin consentimiento.

Aplicación forense: Cualquier acceso a comunicaciones electrónicas almacenadas en la nube debe contar con la debida autorización legal, respetando el derecho al secreto de las telecomunicaciones.

5.4 Código Orgánico Integral Penal (COIP)

El COIP tipifica los delitos informáticos y establece las normas para la obtención y manejo de evidencias digitales (Asamblea Nacional de Ecuador, 2014).

- **Artículo 174:** Sanciona la oferta de servicios sexuales con menores de edad por medios electrónicos.
- **Artículo 190:** Penaliza la apropiación fraudulenta por medios electrónicos.
- **Artículo 232:** Tipifica el ataque a la integridad de sistemas informáticos.
- **Artículo 234:** Sanciona el acceso no consentido a sistemas informáticos, telemáticos o de telecomunicaciones.
- **Artículos 502 a 505:** Regulan la cadena de custodia de evidencias, incluyendo las digitales, exigiendo su preservación desde la obtención hasta su presentación en juicio.

Aplicación forense: Los procedimientos de investigación en la nube deben garantizar la integridad de los sistemas, documentar adecuadamente los accesos y mantener una cadena de custodia rigurosa para asegurar la validez de las evidencias digitales en procesos judiciales.

5.5 Ley Orgánica de Protección de Datos Personales

Esta ley regula el tratamiento de datos personales, estableciendo principios y obligaciones para su protección (Ecuador, Ley organica de proteccion de datos, 2021).

- **Artículo 1:** Garantiza el ejercicio del derecho a la protección de datos personales, incluyendo el acceso y decisión sobre información de este carácter.
- **Artículo 2:** Aplica a todo tratamiento de datos personales, automatizados o no, y a toda modalidad de uso posterior.
- **Artículo 48:** Establece la obligación de designar un delegado de protección de datos personales en ciertos casos.

*Aplicación forens*e: Para cumplir con las disposiciones de esta ley durante una investigación forense en la nube, se deben implementar medidas técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de los datos personales.

6. Protocolo de acceso a la información en la nube

6.1 Consideraciones generales

*6.*1.1 Principio de legitimidad

El acceso forense a datos en el cloud no es es una exploración a ciegas: todo examen técnico descansa sobre una base jurídica válida y documentada. La legitimación proviene de dos fuentes excluyentes:

- **Consentimiento informado** del titular, otorgado por escrito, con alcance y duración claramente delimitados.
- **Mandato judicial** emitido por juez de garantías penales, con motivación expresa sobre la relevancia, pertinencia y proporcionalidad de los datos solicitados (CPP 155-156).

6.1.2 Jurisdicción, soberanía y localización lógica

Los proveedores que prestan servicios en el cloud replican la información por razones de resiliencia. Un mismo archivo puede residir en discos de tres regiones distintas; la copia "primaria" o la que contenga los metadatos de auditoría, definirá la legislación vigente. Para cada activo se debe documentar:

1. **Región contractual** (la que elige la organización durante el aprovisionamiento).
2. **Región efectiva** (donde se almacena realmente la réplica activa).
3. **Región de respaldo** (cold storage, cross-region replication).

Si alguna reside fuera de territorio ecuatoriano, se activa el Convenio de Budapest. Mecanismo de Asistencia Jurídica Mutua (MLAT) o, a falta de tratado, la carta rogatoria a través de Cancillería.

6.1.3 Integridad y autenticidad

El art. 7 de la LCE define la integridad de un mensaje de datos como la conservación íntegra e inalterable de su contenido. En la práctica:

- antes de tocar un artefacto se congela mediante "legal hold";
- se obtienen dos hashes: SHA-256 por fragmento y SHA-512 global;
- ambos se firman con clave PGP del perito y se registran en la Bitácora Inalterable de Cadena de Custodia (BICC).

6.2 Procedimiento de acceso a la información en la nube

6.2.1 Detección del Incidente

La detección de incidentes de seguridad en la nube en Ecuador puede originarse desde diversas fuentes tanto instituciones públicas como privadas (áreas de TI/Seguridad, SOC, CSIRT institucionales, proveedores cloud y empresas especializadas). A nivel país, existe un CSIRT nacional coordinado por el Ministerio de Telecomunicaciones, que articula esfuerzos con equipos sectoriales como EcuCERT (sector telecomunicaciones, bajo ARCOTEL). Estas instancias reciben alertas, correlacionan eventos y emiten avisos de seguridad, pero no ejercen funciones de investigación penal.

Por su parte, cuando de la detección se desprenden indicios de delito informático, intervienen las autoridades competentes para investigar: la Fiscalía General del Estado, a través de su Unidad Nacional Especializada en Investigación de Ciberdelito, y la Policía Nacional, mediante sus unidades de delitos/ciberdelitos. Estas unidades investigan hechos presuntamente delictivos y conducen diligencias dentro del proceso penal; no son responsables del monitoreo ni de la seguridad informática de las organizaciones.

Fuentes y mecanismos de detección en Ecuador:

- **Equipos de respuesta a incidentes (CSIRT):** Ecuador cuenta con el EcuCERT a nivel público (CSIRT nacional) y con CSIRT institucionales en entidades clave (p. ej., Consejo de la Judicatura, Corporación Nacional de Telecomunicaciones), universidades y empresas privadas de sectores como financiero y telecomunicaciones. Aunque no existe un SOC único que preste monitoreo permanente para todas las instituciones del país, estos equipos reciben alertas, analizan eventos y coordinan la respuesta apoyándose en SIEM y reportes de terceros.
- **Notificación directa del titular o administrador de datos:** En muchos casos, especialmente en organizaciones pequeñas o medianas que no cuentan con un CSIRT formal, la detección parte del propio administrador del sistema, responsable de la infraestructura, o incluso de un usuario que reporta comportamientos anómalos en servicios cloud (por ejemplo, accesos inusuales a cuentas de correo, archivos eliminados o modificados sin autorización, cambios de configuración inesperados, etc.).
- **Reportes externos o judiciales:** Cuando el incidente involucra un posible delito informático, el reporte puede originarse en una denuncia ciudadana o empresarial ante

la Fiscalía o la Unidad de Investigaciones de Delitos Informáticos de la Policía Nacional. Desde allí se inicia un expediente judicial y se solicita la intervención de un perito forense especializado.

Activación del protocolo de investigación:

Una vez detectado un posible incidente, el responsable institucional (por ejemplo, el jefe de TI, un delegado del CSIRT, o la autoridad judicial competente) evalúa la información inicial y, si se considera que existe una afectación a activos informáticos o evidencias digitales alojadas en servicios en la nube, se activa el protocolo de investigación forense.

En el contexto ecuatoriano, este protocolo suele estar regulado por directrices internas de la institución y complementado por la normativa del Código Orgánico Integral Penal (COIP), que exige mantener la integridad de la evidencia desde su obtención hasta su presentación judicial (COIP, 2014, arts. 502–505). El procedimiento también considera las exigencias de la Ley Orgánica de Protección de Datos Personales (LOPDP, 2021) si el incidente involucra tratamiento de datos personales.

La activación del protocolo implica:

- Solicitar o emitir una orden de inicio formal de peritaje (si se trata de una investigación penal).
- Designar a un equipo forense institucional o externo acreditado por el Consejo de la Judicatura o entidad correspondiente.
- Registrar el incidente bajo un expediente formal con número de caso, fecha y hora de activación (conocido como "Tiempo Cero").
- Asegurar las primeras evidencias identificadas (por ejemplo, preservación, respaldos, logs, imágenes forenses, snapshots cloud, etc.).

El proceso se activa en el momento en que el centro de operaciones de seguridad (SOC), el equipo de respuesta a incidentes (CSIRT) o el propio titular de los datos confirma que el evento involucra activos alojados en la nube. El Coordinador Forense registra la hora de activación—llamada "Tiempo Cero"—y abre un expediente digital numerado, donde quedará constancia de todas las actuaciones posteriores.

6.2.2 Identificación de servicios y activos

El perito forense, asistido por personal de infraestructura si fuera necesario, elabora un inventario exhaustivo de las suscripciones, cuentas o proyectos vinculados con la organización

o con la persona investigada. En esa enumeración se incluyen máquinas virtuales, contenedores, bases de datos administradas, repositorios de archivos, copias de seguridad, registros de auditoría y cualquier otro recurso que pueda contener información relevante. El inventario se firma de forma o electrónica y se incorpora al expediente.

6.2.3 Obtención de la autorización legal

El Asesor Jurídico redacta una petición judicial detallada que explica la pertinencia y la necesidad de acceder a los datos. Si el titular presta consentimiento expreso, dicho consentimiento —con firma manuscrita o electrónica— se anexa. En los demás casos, la Fiscalía gestiona la orden ante un juez de garantías penales. La autorización o disposición judicial debe precisar:

- la identificación exacta de la cuenta, la tenencia o el proyecto involucrados;
- los servicios específicos afectados (p. ej., correo corporativo, almacenamiento de objetos, instancias virtuales);
- el intervalo temporal de la investigación;la fundamentación jurídica aplicable (p. ej., COIP para medidas de investigación penal y obtención lícita de registros digitales; LCE para la validez de mensajes de datos y firmas electrónicas; y, cuando corresponda, LOPDP respecto del tratamiento de datos personales en contexto de investigación penal).

Nota:

- COIP: Código Orgánico Integral Penal.
- LCE: Ley de Comercio Electrónico, Firmas y Mensajes de Datos.
- LOPDP: Ley Orgánica de Protección de Datos Personales.

Una vez expedida, la orden se digitaliza en formato PDF, se calcula su hash SHA-256 y ambos elementos (archivo y hash) se guardan en el expediente.

Una vez expedida la orden:

- Si está en soporte físico con firma manuscrita, se digitaliza a PDF (copia fiel), se calcula su hash SHA-256 y ambos (PDF y hash) se incorporan al expediente digital; el original físico se conserva bajo cadena de custodia.

- Si está firmada electrónicamente, se archiva el archivo original (p. ej., PDF firmado), sin escanear; se verifica la validez de la firma (certificado, integridad y sello de tiempo), se documenta el resultado y se calcula y registra el hash SHA-256 de ese archivo.

En ambos casos, el hash se anota en la bitácora forense y en el folio correspondiente del expediente.

6.2.4 Notificación al proveedor y congelación

Con la autorización judicial, Con la orden judicial en mano, el Perito Forense ingresa al canal oficial de cumplimiento del proveedor (p. ej., portal de solicitudes legales) y solicita la retención inmutable de todos los datos identificados en la orden.

El proveedor emite un acuse de recibo y, dentro del plazo establecido (p. ej., hasta 72 horas), remite un inventario detallado de los datos retenidos. Ese inventario es un listado de todo lo "congelado" para preservación, e incluye, como mínimo:

- Qué es cada elemento (tipo y nombre): p. ej., objeto S3, archivo de log, correo, snapshot, base de datos, instancia.
- Dónde está (ruta/ARN/ID/servicio y cuenta/proyecto).
- Tamaño y fecha/hora exacta de la retención.
- Identificador de versión (si aplica) y estado de retención/bloqueo.
- Valor hash en origen (si el servicio lo soporta) para acreditar integridad.
- Observaciones relevantes (p. ej., cifrado, custodia interna, excepciones).

El inventario se archiva de inmediato en el expediente y se usa como punto de referencia para verificar que los datos exportados por el proveedor coincidan con lo efectivamente retenido (nombres, rutas, tamaños, fechas y, cuando proceda, hash).

6.2.5 Extracción controlada de la evidencia

Para efectuar la descarga, el proveedor concede a la parte investigadora un perfil temporal de solo lectura con vencimiento automático —generalmente de veinticuatro horas— de modo que ningún actor humano pueda modificar o eliminar los datos. El Perito Forense descarga la información en segmentos manejables y, durante la transferencia, calcula un hash SHA-256 por cada segmento y un hash maestro SHA-512 de la colección completa. Los valores se comparan de inmediato con los hashes proporcionados por el proveedor; cualquier discrepancia se documenta como hallazgo y, si es posible, se subsana solicitando una segunda

descarga. Cada operación de copia queda asentada, con hora y minuto, en la Bitácora Inalterable de Cadena de Custodia.

6.2.6 Transferencia y custodia

Terminada la extracción, el Custodio de Evidencia aplica el esquema «tres-dos-uno»: mantiene tres copias idénticas, emplea al menos dos tipos de soporte distintos y conserva una de las copias fuera de línea en un entorno físico seguro. En todo movimiento —por ejemplo, del equipo de adquisición al almacén de soportes— el Custodio y un testigo firman el Formulario de Cadena de Custodia, donde se deja constancia de la fecha, la hora, la persona que entrega, la persona que recibe, la descripción de los soportes y los valores hash globales que aseguran la identidad de la evidencia.

6.2.7. Análisis Forense

Aunque el análisis técnico profundo pertenece a otra sección de la guía, es importante destacar que se realiza exclusivamente en un laboratorio aislado, sin conexión a redes de producción ni a Internet. En él se monta una copia de trabajo y se deja intacta la copia maestra.

El analista participante en la revisión preliminar redacta un Informe Técnico Parcial, el cual sirve de base para eventuales ampliaciones de la orden judicial.

6.2.8. Cierre y archivo definitivo

Aunque el análisis técnico profundo pertenece a otra sección de la guía, es importante destacar que se realiza exclusivamente en un laboratorio aislado, sin conexión a redes de producción ni a Internet. En él se monta una copia de trabajo y se deja intacta la copia maestra. Al menos dos analistas participan en la revisión preliminar y redactan un Informe Técnico Parcial que sirve de base para eventuales ampliaciones de la orden judicial.

Acceso a dispositivos personales sincronizados

En los casos en que la información cloud también se encuentra en dispositivos personales —por ejemplo, teléfonos con copia de seguridad en iCloud o Google Drive— la solicitud judicial debe mencionar de forma explícita la facultad de examinar dichos equipos.

El procedimiento exige:

1. la inmovilización física del dispositivo mediante acta suscrita por el titular o por la autoridad competente;
2. la obtención de una imagen lógica o física que incluya la carpeta de sincronización;

3. la verificación de que los hashes de los archivos locales coinciden con los de la copia remota preservada.

Si existiera divergencia de hashes, el hallazgo se anota y se conserva la versión con valor probatorio más íntegro, siempre sin alterar el contenido original.

7. Análisis de Estándares y Selección del Estándar

La aplicación de estándares internacionales en una investigación forense en la nube permite garantizar procedimientos técnicos confiables, reproducibles y admisibles legalmente. En este protocolo se realiza un análisis comparativo entre tres de los principales marcos normativos aplicables al proceso forense digital, con el fin de seleccionar el más adecuado para investigaciones en entornos cloud en Ecuador.

Estándar 1: ISO/IEC 27037:2012

Directrices para la identificación, recolección, adquisición y preservación de evidencia digital

Este estándar proporciona una guía para el manejo inicial de la evidencia digital, estableciendo principios fundamentales como:

- Preservación de la integridad de la evidencia desde su descubrimiento.
- Definición de roles: responsable de evidencia digital y especialista forense digital (SFD).
- Aplicación de controles en la adquisición: generación de funciones hash, uso de imágenes forenses, etc.
- Requisitos para garantizar la autenticidad, confiabilidad y legalidad de la evidencia digital.

Ventajas:

- Enfoque sistemático sobre la preservación inicial.
- Ideal para investigaciones que comienzan desde la identificación del incidente.

Limitaciones:

- No cubre de forma exhaustiva las fases posteriores como el análisis detallado o la presentación ante entes judiciales.

Aplicación en la nube:

Se usa especialmente para guiar la adquisición inicial de datos en entornos virtuales, como snapshots de máquinas virtuales, registros de logs o volúmenes de almacenamiento.

Estándar 2: ISO/IEC 27042:2015

Directrices para el análisis e interpretación de evidencia digital

Complementa al estándar anterior, centrándose en cómo analizar e interpretar la evidencia recolectada. Algunos de sus puntos clave incluyen:

- Procedimientos para reconstrucción de eventos digitales.
- Análisis técnico de dispositivos, archivos, logs y tráfico de red.
- Recomendaciones sobre herramientas y formatos de informes forenses.

Ventajas:

- Establece lineamientos claros para el análisis forense profundo.
- Requiere una documentación meticulosa para mantener validez legal.

Limitaciones:

- No cubre procedimientos de obtención inicial ni procesos de cadena de custodia previos.

Aplicación en la nube:

Es útil en fases de correlación de datos, detección de comportamiento anómalo, reconstrucción de eventos sobre plataformas como AWS CloudTrail o Azure Monitor

Estándar 3: NIST SP 800-86 (National Institute of Standards and Technology)

Guide to Integrating Forensic Techniques into Incident Response

Emitido por el NIST, este documento es una guía práctica para integrar técnicas forenses en las respuestas a incidentes. Está organizado en cuatro fases:

1. Recolección.
2. Examen.
3. Análisis.
4. Reporte.

Ventajas:

- Enfoque operativo, con procedimientos detallados.
- Diseñado para aplicarse en entornos modernos, incluyendo sistemas distribuidos y cloud.
- Fuerte enfoque en integración con equipos de respuesta a incidentes (CSIRT).

Limitaciones:

- No es un estándar certificable como ISO; es una guía técnica.

Aplicación en la nube:

Altamente aplicable para investigaciones en servicios IaaS y SaaS, donde es necesario integrar forense digital con respuesta a incidentes en tiempo real (por ejemplo, ataques en GCP, filtraciones en Office 365, etc.).

Tabla 1

Comparación entre estándares

Criterio	ISO/IEC 27037	ISO/IEC 27042	NIST SP 800-86

Fase principal que cubre	Identificación y adquisición	Análisis e interpretación	Todo el ciclo forense
Enfoque	Normativo y técnico	Interpretativo técnico	Operativo y práctico
Cobertura en la nube	Parcial	Media	Alta
Recomendado para	Preservación inicial	Análisis avanzado	Respuesta a incidentes y análisis integral
Compatibilidad con Ecuador (COIP)	Alta	Alta	Alta

Nota. Comparación de los estándares ISO/IEC 27037, ISO/IEC 27042 y NIST SP 800-86, según los criterios de fase principal cubierta, enfoque, cobertura en la nube, aplicaciones recomendadas y compatibilidad con la normativa ecuatoriana (COIP)

Selección del Estándar Recomendado

Para efectos de esta guía, y considerando el entorno actual de la computación en la nube en Ecuador, se propone un modelo híbrido que integre:

- **ISO/IEC 27037:2012** para la recolección inicial de datos.
- **ISO/IEC 27042:2015** para el análisis técnico detallado.
- **NIST SP 800-86** como base operativa para respuesta a incidentes y articulación con los equipos técnicos y legales.

Este enfoque mixto garantiza un proceso completo, desde la detección del incidente hasta la presentación de la evidencia digital, cumpliendo tanto estándares internacionales como requerimientos legales del Código Orgánico Integral Penal (COIP).

8. Herramientas Forenses en la Nube

El uso de herramientas especializadas es fundamental en el análisis forense digital en entornos de computación en la nube. A diferencia del análisis tradicional, el entorno cloud presenta desafíos técnicos como la virtualización, la elasticidad de los recursos y la dispersión geográfica de la información, lo que exige el uso de soluciones adaptadas a estas condiciones.

Este protocolo presenta un análisis técnico y funcional de las principales herramientas forenses utilizadas en investigaciones de incidentes informáticos en la nube, clasificadas según su función, compatibilidad y validación internacional.

Criterios para la selección de herramientas forenses en la nube

Para que una herramienta forense sea válida en el contexto de una investigación en la nube, debe cumplir con los siguientes criterios:

- Compatibilidad con entornos cloud (IaaS, PaaS, SaaS).
- Capacidad de preservar la integridad de la evidencia.
- Generación de hash criptográfico (SHA-256, SHA-512).
- Exportación de reportes admisibles legalmente.
- Auditoría y registro de actividades (logs).
- Soporte técnico y actualizaciones frecuentes.

Herramientas Forenses Recomendadas

A continuación, se presenta una tabla con las herramientas más utilizadas en investigaciones forenses en la nube, detallando sus características principales:

Tabla 2

Herramientas más utilizadas en investigaciones forenses en la nube

Herramienta	Función principal	Compatibilidad cloud	Características clave	Uso típico en la nube
Magnet AXIOM Cloud	Análisis forense completo en entornos SaaS	Office 365, Google Workspace	Extracción de correos, chats, drive, metadatos, análisis de	Ataques internos, filtración de datos

			historial, integridad hash	
Elcomsoft Cloud eXplorer	Recolección y análisis de datos de cuentas Google	Google Drive, Gmail, Google Photos	Recupera registros eliminados, GPS, backups, datos sincronizados desde Android	Dispositivos personales sincronizados
FTK Imager / FTK	Adquisición forense y análisis local	IaaS (AWS, Azure con disco montado)	Imagen de volúmenes virtuales, generación de hash, exploración por palabras clave	Captura de disco en máquinas virtuales
X-Ways Forensics	Análisis forense avanzado	Compatible con discos extraídos	Bajo consumo de recursos, análisis hexadecimal, búsqueda avanzada	Procesamiento local de evidencia extraída
AWS CloudTrail / Azure Monitor	Registro de actividad y auditoría en la nube	Amazon Web Services, Azure	Seguimiento de logs de seguridad, accesos, configuraciones, cambios en recursos	Correlación de eventos, reconstrucción de ataque
Cellebrite UFED Cloud	Extracción de datos móviles sincronizados	iCloud, Google Cloud, redes sociales	Captura directa desde cuentas conectadas, respaldos en la nube, tokens	Casos donde el sospechoso sincronizó su dispositivo
Velociraptor	Monitoreo y respuesta forense remota	Infraestructura híbrida / cloud	Código abierto, análisis de	Vigilancia forense activa

	endpoints remotos en tiempo real	durante un incidente

Nota. Comparación de herramientas forenses digitales (*Magnet AXIOM Cloud, Elcomsoft Cloud eXplorer, FTK Imager/FTK, X-Ways Forensics, AWS CloudTrail/Azure Monitor, Cellebrite UFED Cloud* y *Velociraptor*), de acuerdo con su función principal, compatibilidad en entornos cloud, características clave y usos típicos en investigaciones en la nube.

Tabla 3

Recomendaciones de uso según tipo de servicio cloud

Modelo cloud	Recomendación de herramientas principales
IaaS	FTK, X-Ways, Volatility, AWS CLI, snapshot tools
PaaS	Logs nativos, Velociraptor, Magnet AXIOM (limitado)
SaaS	Magnet AXIOM Cloud, Elcomsoft, Cellebrite, API forense

Nota. Relación entre los modelos de servicio en la nube (*IaaS, PaaS y SaaS*) y las herramientas forenses más recomendadas para cada uno, considerando sus aplicaciones en adquisición, análisis y monitoreo de evidencias digitales.

Aspectos legales y técnicos al utilizar herramientas

- **Licencias:** Se debe verificar que las herramientas estén legalmente adquiridas y se encuentren actualizadas.
- **Registro de acciones:** Toda actividad realizada debe ser documentada en los reportes forenses.
- **Validación:** Las herramientas deben estar reconocidas por la comunidad forense o validadas en procedimientos previos judiciales.
- **Cadena de custodia:** Toda evidencia obtenida con herramientas debe ser asegurada y vinculada con su hash original.

Consideraciones específicas en el contexto ecuatoriano

- En Ecuador, cualquier evidencia extraída con herramientas forenses debe cumplir lo estipulado en el COIP (artículos 500-505) sobre cadena de custodia.

- Las herramientas que permiten análisis remoto o cloud deben usarse únicamente bajo orden judicial o consentimiento del titular, conforme a la Ley de Comercio Electrónico y la Ley de Protección de Datos Personales.
- Las instituciones públicas deben verificar la compatibilidad de estas herramientas con sus políticas de seguridad y normativas de contratación de software.

9. Procedimiento Forense en Entornos de Nube

El proceso forense en la nube mantiene las mismas fases fundamentales que en cualquier investigación forense digital, pero con adaptaciones importantes debido a las características de la computación en la nube. Las fases clásicas que son identificación, preservación, recolección (adquisición), análisis, presentación, se aplican en la guía, incorporando las mejores prácticas descritas en la sección de estándares. A continuación, se detalla cada fase en contexto cloud, destacando qué pasos adicionales o diferentes deben considerarse, incluyendo la posibilidad de recolección directa o mediante proveedor y algunos comandos o técnicas relevantes.

9.1 Identificación de Evidencias en la Nube

En esta fase, el objetivo es reconocer que ha ocurrido un incidente y determinar qué fuentes de datos digitales pueden contener evidencia del mismo. En un entorno de nube, la identificación implica:

- **Detección del incidente:** Puede provenir de alertas de seguridad (ej. un aviso en AWS GuardDuty o Azure Security Center indicando actividad sospechosa), de anomalías en el monitoreo (picos de tráfico, uso de CPU), de reportes de usuarios (p.ej., "no encuentro mis archivos, creo que alguien borró cosas"), o de la notificación de un tercero (proveedor o autoridad).

Tabla 4

Detección del Incidente

Detección del Incidente	
Campo	**Detalle**
Número de caso	
Institución / Entidad notificante	
Fuente de detección (CSIRT, SOC, administrador, usuario, Fiscalía, Policía)	
Tipo de alerta recibida (anomalía en logs, reporte de usuario, denuncia, monitoreo SIEM)	
Descripción inicial del incidente	
Hora y fecha de activación ("Tiempo Cero")	
Evidencia preliminar asegurada (logs, respaldos, snapshots, capturas)	
Autoridad que dispone la investigación	
Perito designado	
Firma	
Fecha	

Nota. Formato de registro para la detección inicial de un incidente de seguridad informática

- **Clasificación del incidente:** Como se describió en la sección 6, determinar el tipo de incidente ayuda a orientar la investigación. Por ejemplo, ¿es una intrusión externa, un abuso interno, un fallo técnico con pérdida de datos, un uso indebido de la plataforma para delito? Identificar esto permite listar las evidencias potenciales: logs de acceso, configuraciones, contenidos de cuentas, etc.

Tabla 5

Evaluación Inicial del Incidente

Evaluación Inicial del Incidente	
Campo	**Detalle**

Evidencias preliminares identificadas
Clasificación del incidente (intrusión, abuso interno, fraude, sabotaje, etc.)
Activos comprometidos (cuentas, instancias, bases de datos, SaaS, etc.)
Alcance inicial estimado del incidente (usuarios, regiones, servicios)
Riesgo asociado (pérdida de disponibilidad, integridad, confidencialidad, continuidad)
Medidas inmediatas de contención aplicadas
Responsable de la evaluación
Firma
Fecha

Nota. Formato de evaluación inicial de incidentes de seguridad informática

- **Fuentes de evidencia en cloud:** Esta es la parte medular de la identificación en la nube: establecer qué elementos de la infraestructura o servicios cloud están involucrados y pueden proveer datos. Algunos ejemplos:
    - Instancias de cómputo (*VMs*): Si fue comprometido un servidor virtual en AWS/Azure, la evidencia residirá en su disco virtual, en su memoria (si aún está encendida), y en logs de su sistema operativo, además de logs de orquestación (CloudTrail/Azure logs sobre esa instancia).
    - Servicios gestionados (PaaS/SaaS): Si el incidente ocurrió en un servicio tipo base de datos cloud, las evidencias vendrán de los logs de consultas, registros de auditoría del servicio, configuraciones de usuarios/roles en ese servicio. Si fue en un correo en la nube), habrá evidencias en los encabezados de correo, registros de accesos a la cuenta, contenido de correos.
    - Redes y almacenamiento: Identificar si hay evidencias en el tráfico de red cloud (p.ej., VPC Flow Logs en AWS, NSG Flow Logs en Azure) o en almacenamiento (archivos modificados en S3, Azure Blob,etc.).
    - **Metadatos de la nube:** La nube genera metadatos útiles, por ejemplo: qué IP públicas tuvo una VM y cuándo, qué acciones realizó cada usuario en la consola de administración, qué dispositivos se conectaron a una cuenta, etc. Estos metadatos son a veces tan importantes como los datos en sí.

Tabla 6

Identificación de Plataformas Involucradas

Identificación de Plataformas Involucradas	
Campo	**Detalle**
Número de caso	
Proveedor en la nube (AWS, Azure, GCP, SaaS)	
Servicios identificados (EC2, S3, Azure SQL, GDrive, etc.)	
Recursos afectados (VMs, contenedores, buckets, bases de datos, repositorios)	
Región contractual (configurada por el cliente)	
Región efectiva (donde se almacenan los datos)	
Región de respaldo (replicación, cold storage)	
Cuentas / Suscripciones vinculadas (ID de cuenta, tenant, proyecto)	
Metadatos relevantes (logs de auditoría, direcciones IP, roles, credenciales)	
Estado del servicio (activo, detenido, comprometido, eliminado)	
Responsable de la identificación	
Firma de validación	
Fecha	

Nota. Formato de identificación de plataformas y servicios en la nube relacionados con un incidente de seguridad

- **Delimitación del alcance:** A menudo se comienza delimitando un alcance de la investigación. En cloud esto significa concretamente: qué cuentas de usuario investigar, qué instancias, qué servicios. Por ejemplo, ante un indicio de intrusión, se podría determinar: "Incidente X parece limitarse a la cuenta AWS de la empresa, específicamente a las instancias del frontend web en la región us-east-1." Esa delimitación inicial puede ajustarse luego, pero ayuda a enfocar esfuerzos.
- **Identificación de custodios o responsables:** En entornos corporativos cloud, identificar quién administra el sistema afectado o quién tiene las llaves del reino (credenciales privilegiadas) es crucial. Ellos pueden ser informantes para conocer

configuración, y a la vez posibles sospechosos en casos de fallo interno. También es importante identificar si se requerirá involucrar al proveedor cloud (CSP) desde esta fase: por ejemplo, en un caso de fraude por Facebook o Instagram, uno reconoce que la evidencia está principalmente en poder de Meta, por lo que desde ya se contempla una solicitud formal a la empresa.

En esta fase de identificación, no se toca la data aún en lo posible, solo se ubica dónde está. Se documenta todo lo aprendido: lista de instancias, IDs, nombres de cuentas, servicios impactados, temporalidad del incidente (cuándo inició/detectó), etc. Esta documentación es la base para la siguiente fase.

9.2 Preservación de Datos en la Nube

La preservación consiste en asegurar que la evidencia identificada no se pierda ni altere antes de poder ser recolectada y analizada. En entornos on-premise esto implicaba acciones como aislar un computador, evitar apagados bruscos, etc. En la nube, se aplican medidas equivalentes:

- **Evitar la volatilización de datos:** En cloud, ciertas evidencias son altamente volátiles/efímeras. Por ejemplo, el contenido en memoria de una VM se pierde al apagarla; asimismo, logs efímeros que no se exportan a tiempo pueden rotar y quedar inaccesibles. Por ello, una de las primeras tareas es capturar la evidencia volátil. Si la instancia está encendida y se sospecha compromiso, es válido realizar un "live response" controlado para recolectar cierta información. Sin embargo, esto debe hacerse cuidadosamente para no modificar evidencias clave (Soto, 2022) . Un enfoque es utilizar herramientas de respuesta a incidentes en memoria (e.g., usar AWS Systems Manager Agent para ejecutar comandos de volcado de memoria en la VM).
- **Aislamiento del entorno afectado:** Similar a acordonar una escena del crimen. En la nube significa, por ejemplo: quitar una máquina virtual de producción para que no siga procesando ni alterando datos. En AWS, se recomienda habilitar protección contra terminación en instancias comprometidas para que no sean terminadas accidentalmente (Services, 2020). También, aislar la red: cambiar la instancia a un Security Group (grupo de seguridad) más restrictivo o sacar la máquina de la balanza de carga, para que no reciba más tráfico (Services, 2020). Estas acciones preservan el estado del sistema tal como estaba al momento del incidente, evitando que siga corriendo transacciones o que un atacante en curso haga más cambios.

- **Snapshots y copias de seguridad inmediatas:** Una de las primeras medidas de preservación es tomar instantáneas (snapshots) de los volúmenes de almacenamiento relevantes (AWS Security Incident Response User Guide, 2024). Tanto AWS como Azure permiten tomar snapshots de discos en caliente. En AWS, por ejemplo, se puede ejecutar:

```
aws ec2 create-snapshot --volume-id <ID_de_Volumen> --description "Snapshot forense caso XYZ"
```

Esto crea una copia de la unidad EBS en ese momento (AWS Security Incident Response User Guide, 2024). En Azure, de forma similar:

```
az snapshot create -g GrupoRecursos --source <ID_del_Disco> --name SnapshotCasoXYZ
```

Estos snapshots se deben marcar o etiquetar claramente como evidencia (muchos equipos usan etiquetas como "Forensic" o "Quarantine" en los recursos) (AWS Security Incident Response User Guide, 2024). Importante: si la instancia está comprometida por malware, es recomendable deshabilitar temporariamente la eliminación automática de volúmenes al terminar la instancia (en AWS esto es DisableApiTermination y quitar el flag DeleteOnTermination de los volúmenes) (AWS Security Incident Response User Guide, 2024), para no perderlos en caso de que alguien apague la VM inadvertidamente.

- **Preservación de registros y auditorías:** Muchos proveedores tienen políticas de retención de logs (por ejemplo, CloudTrail en AWS por defecto guarda 90 días si no se envía a S3). Para preservar logs más allá de su retención normal, se deben exportar o extender retención. En AWS: configurar la exportación de CloudTrail a un bucket S3 tan pronto se detecta el incidente, para asegurar que todos los eventos queden guardados (Báez, 2025). En Azure: habilitar la retención de logs en Azure Monitor/Log Analytics, exportar Activity Logs a almacenamiento o eventos a un SIEM. Estas acciones preventivas garantizan que la información histórica no se pierda por ciclos de retención.
- **Asegurar cuentas y credenciales:** Si la evidencia puede incluir información de credenciales (ej. tokens de API, claves secretas), o si hay riesgo de que un atacante activo borre datos, es parte de la preservación revocar accesos o congelar cuentas sospechosas. Esto es delicado: Por un lado, se quiere preservar (que el atacante no borre logs), por otro, si se cierra su acceso, puede ocurrir que en represalia borre cosas si aún

tiene alguna ventana. Sin embargo, generalmente se procede a bloquear credenciales comprometidas inmediatamente tras recolectar lo más urgente. También se pueden aplicar hold legales: por ejemplo, en G Suite/Office 365 se pueden colocar buzones en "Litigation Hold" (retención) para que, aunque usuarios borren correos, queden preservados en la carpeta oculta de eDiscovery.

- **Notificaciones internas y legales:** En esta etapa también entra la preservación desde el punto de vista de cadena de custodia legal: se notifica a las personas adecuadas que se ha iniciado un proceso forense, para que nadie toque esos sistemas sin autorización. Si se trata de un ambiente corporativo, el área de TI es instruida para no reiniciar servidores ni modificar configuraciones hasta que el equipo forense lo indique. En ocasiones, se precintan (digitalmente hablando) recursos: por ejemplo, no hacer deploys ni cambios en ciertas instancias en la nube bajo investigación.

Un punto crítico en la nube es que a veces la preservación completa no es posible sin la intervención del proveedor. Por ejemplo, si la evidencia está en un servicio SaaS multiarrendatario (digamos WhatsApp o Facebook), el investigador no puede por sí solo congelar esa data; debe solicitar formalmente al proveedor que la preserve (lo que se llama un "*preservation request*"). Muchas grandes compañías tienen procedimientos para que las entidades de ley les solicite que retengan cierto contenido mientras se tramita la orden de divulgación. En Ecuador, a través de la Fiscalía y la unidad policial especializada, se pueden enviar oficios para que la empresa cloud preserve los datos de una cuenta específica antes de que sean eliminados (Soto, 2022).

La preservación en la nube es una combinación de acciones técnicas inmediatas (snapshots, aislar instancias, extraer logs) y acciones administrativas/legales (retención de datos, órdenes de preservación) para mantener la evidencia intacta hasta que pueda ser analizada formalmente.

Tabla 7

Plantilla de Cadena de Custodia

FORMULARIO DE CADENA DE CUSTODIA	
Edición N° 01	**Pág. 1**

INFORMACIÓN GENERAL

Institución, (o persona):	Caso N°
Servidor que interviene:	
Lugar del Hecho	
Dirección:	Coordenadas:
Fecha:	Hora:
Tipo de hecho:	Autoridad:

DATOS DEL INDICIO / EVIDENCIA / BIEN INCAUTADO

Tipo: Indicio ( ) Evidencia ( ) Bien ( )	Número:	Embalaje utilizado:	
Marca:	Hash:	Serie:	
Color:	Tamaño:	Volumen:	Peso:
Estado: Bueno ( ) Regular ( ) Malo ( )	Orgánico ( ) Inorgánico ( )	Perecible: Si ( ) No ( )	
Localización del Indicio:	Detalle del Indicio:		
Sellado por:	N° cinta de seguridad:		

	INSTITUCIÓN	**GRADO/NOMBRES Y APELLIDOS**	**C.C./C.I./PA**	**MOTIVO**	**FIRMA DE RESPONSABILIDAD**
ENTREGA				**Custodia ☐ Peritaje ☐ Traspaso ☐**	
RECIBE					
ENTREGA: FECHA Y HORA:			OFICIO:		
OBSERVACIONES:…… …… …… ……					

	INSTITUCIÓN	**GRADO/NOMBRES Y APELLIDOS**	**Cédula de Identidad**	**MOTIVO**	**FIRMA DE RESPONSABILIDAD**
ENTREGA				**Custodia ☐ Peritaje ☐ Traspaso ☐**	
RECIBE					
ENTREGA: FECHA Y HORA:			OFICIO:		

OBSERVACIONES:…… …… …… ……					
	INSTITUCIÓN	**GRADO/NOMBRES Y APELLIDOS**	**Cédula de Identidad**	**MOTIVO**	**FIRMA DE RESPONSABILIDAD**
ENTREGA				**Custodia ☐ Peritaje ☐ Traspaso ☐**	
RECIBE					
ENTREGA: FECHA Y HORA:			OFICIO:		
OBSERVACIONES…… …… …… ……					

9.3 Recolección y Adquisición de Evidencia Digital

Una vez identificadas y preservadas las fuentes de evidencia, se procede a la recolección/adquisición, es decir, la obtención efectiva de copias de evidencia digital de forma forense. En entornos de nube, esto puede realizarse de dos maneras principales: *recolección directa* (por parte del equipo forense, usando accesos disponibles) o recolección a través del proveedor (cuando el acceso directo no es posible y se necesita la colaboración del CSP). A continuación, se detalla el procedimiento general, subdividido en casos según la situación:

9.3.1 Recolección Directa en lugar

Este caso aplica cuando en una operación se encuentra un dispositivo físico relacionado con la nube. Por ejemplo, un servidor en una empresa que resulta ser un nodo local de la nube privada, o un empleado con su laptop abierta conectada a servicios cloud corporativos. En tales situaciones:

- **Captura de memoria RAM:** Si el dispositivo está encendido y operando, se debe considerar la obtención de una imagen de memoria RAM, ya que puede contener claves de cifrado de sesiones cloud, tokens de acceso, o datos no guardados. Herramientas como Belkasoft Live RAM Capturer, DumpIt, WinPmem (en Windows) o dd/LiME (Linux) pueden usarse. Esta acción debe ser de las primeras, antes de desconectar el equipo (Services, 2020).

- **Preservar sesiones abiertas:** Si, por ejemplo, en la computadora incautada hay una sesión abierta a la consola web de AWS o a la cuenta de Google Drive del sospechoso, no cerrar la sesión ni apagar el equipo hasta registrar la información de esa sesión. Puede ser valioso sacar capturas de pantalla (evidencia documental) de lo que está viendo el usuario, anotar qué cuentas están logueadas, etc. Incluso, si legalmente procede, navegar dentro de la cuenta para identificar evidencia (aunque generalmente se prefiere duplicar el entorno para no modificar nada).
- **Imagen forense del disco local:** Luego de la memoria, si corresponde, se realiza una imagen del disco duro del equipo usando herramientas tradicionales (FTK Imager, por ejemplo, o hardware write-blockers). Esta imagen contendrá posiblemente cachés de navegador (con artefactos de uso de aplicaciones cloud), archivos sincronizados en carpetas locales (OneDrive, Google Drive Sync), correos en Outlook (si es O365) etc. Son evidencias indirectas de la actividad en la nube y deben analizarse.
- **Anotaciones de contexto:** En una escena, recoger también notas escritas, tokens físicos (2FA keys), dispositivos móviles, etc., que puedan facilitar el acceso a las cuentas cloud involucradas. Todo ello entra en cadena de custodia.
- **Cadena de custodia desde el momento cero:** La documentación debe iniciarse desde el primer contacto con la evidencia: registrar fecha y hora, lugar, responsables y acciones realizadas, identificadores del dispositivo o recurso (número de serie, etiqueta, ID/ARN, ruta), estado inicial y condiciones de preservación. Esto excede lo técnico, pero es crucial para demostrar que el equipo o artefacto del cual se obtuvieron los datos es el mismo que se analizó posteriormente, manteniendo trazabilidad, integridad y admisibilidad.

Este apartado, en esencia, equivale a la forensia tradicional, con la salvedad de que los datos en la nube pueden materializarse en artefactos locales (p. ej., carpetas sincronizadas como Dropbox/OneDrive/Drive, tokens o credenciales en directorios de aplicación, cachés y archivos de configuración). Por ello, el perito debe mantener una búsqueda orientada a indicadores en los dispositivos físicos, identificando y preservando aquellos elementos que vinculen el entorno local con el entorno cloud.

9.3.2 Recolección Directa desde Cuentas/Servidores en la Nube (Credenciales proporcionadas)

En muchos casos, no hay un dispositivo físico de por medio, sino que la organización afectada o la víctima proporciona acceso a sus cuentas en la nube para apoyar la investigación. Por ejemplo: una empresa da al perito acceso a su consola AWS; un usuario víctima de delito autoriza acceder a su cuenta de Microsoft; o el incidente ocurre en la propia infraestructura cloud de la organización a la que el perito ya tiene credenciales de administrador. Aquí el procedimiento es:

- **Acceso controlado:** Ingresar a la plataforma cloud con una cuenta que tenga los permisos necesarios para extraer la información, preferiblemente creando credenciales forenses específicas. Por ejemplo, en AWS se podría pedir al cliente que cree un usuario IAM nuevo con permisos de solo lectura a todos los recursos (o uso de roles de auditoría). Esto queda registrado y una vez finalizado el caso, se elimina el usuario/rol. Así se evita usar cuentas operativas de la empresa y se puede monitorizar lo que hace la cuenta forense.
- **Enumeración de recursos:** Un primer paso es listar sistemáticamente los recursos en la nube asociados al incidente. Por ejemplo, si se investiga una supuesta eliminación de datos en Google Drive, listar todas las unidades de drive, historial de archivos eliminados, registros de auditoría de Google. Si es AWS, enumerar instancias EC2, buckets S3, logs CloudTrail disponibles, etc. Esto se puede hacer mediante la interfaz web y también con comandos CLI para tener un registro. Por ejemplo:

```
aws ec2 describe-instances --filters "Name=tag:Incidente,Values=XYZ"
aws s3 ls --human-readable --summarize
aws cloudtrail lookup-events --start-time <fecha> --end-time <fecha>
```

  La idea es inventariar qué hay y qué podría contener evidencia.
- **Adquisición de imágenes de sistemas en IaaS:** Si hay máquinas virtuales implicadas (por ej., un servidor que fue atacado), se procede a crear imágenes forenses de estos sistemas. El camino recomendado es:
  1. **Snapshot de disco** (ya mencionado en preservación).
  2. **Copiar snapshot a un almacenamiento controlado:** A veces se copia el snapshot a otra cuenta o región para aislarlo. En AWS, se puede usar copy-

snapshot para duplicarlo, o crear un volumen nuevo desde el snapshot en una cuenta forense segregada (AWS Security Incident Response User Guide, 2024).

3. **Montaje y descarga:** Se puede montar ese volumen en una instancia forense y luego exportarlo a formato RAW/E01. O bien, en Azure, descargar el VHD del snapshot (Azure permite exportar un URL temporal del VHD). Una vez que se tiene el archivo imagen del disco, ese archivo se maneja como cualquier imagen forense.

Ejemplo AWS: usando AWS CLI se podría automatizar:

```
# Obtener metadata de instancia comprometida:
aws ec2 describe-instances --instance-id i-1234567890abcdef
# Crear snapshot del volumen principal:
aws ec2 create-snapshot --volume-id vol-0987654321fedcba --description "Forensic snapshot caso XYZ"
# Compartir snapshot con cuenta forense (si se usa estrategia multi-cuenta)
aws ec2 modify-snapshot-attribute --snapshot-id snap-1234abcd --attribute createVolumePermission --operation-type add --user-ids <CuentaForenseID>
```

(Luego en la cuenta forense:)

```
# Copiar snapshot a la cuenta forense (opcional, se podría montar directo si hay permiso):
aws ec2 copy-snapshot --source-region us-east-1 --source-snapshot-id snap-1234abcd --description "Copy for analysis" --encrypted --kms-key-id <KMS_forense>
# Crear volumen desde snapshot
aws ec2 create-volume --snapshot-id snap-abcd1234 --availability-zone us-east-1a --volume-type gp3
# Adjuntar volumen a instancia forense
aws ec2 attach-volume --volume-id vol-11112222 --instance-id i-forensic123 --device /dev/sdf
```

A partir de ahí, dentro de la instancia forense (que puede ser una máquina con Kali Linux en AWS, por ejemplo), se puede montar /dev/sdf de solo lectura y hacer un dd o usar dcfldd para generar una imagen local o enviarla a S3. Todo acceso se documenta.

- **Extracción de logs y registros:** Para evidencia como logs de acceso, eventos, etc., se utilizan tanto herramientas nativas como utilidades externas:
    - En AWS, logs relevantes incluyen CloudTrail, CloudWatch Logs (logs de aplicaciones), AWS Config, Elastic Load Balancer logs, VPC Flow Logs, etc.

Muchos de estos se pueden descargar mediante la consola o AWS CLI. Ejemplo:

```
aws s3 cp s3://my-cloudtrail-logs/AWSLogs/123456789012/CloudTrail/us-east-1/2025/08/04/ <directorio_local> --recursive
```

(Asumiendo que CloudTrail estaba enviando logs a S3). Si no, se puede usar lookup-events (limitado a 90 días de historial) (Fonseca, 2023). Para logs de instancias, si la instancia está encendida, podría usarse SSM (RunCommand) para ejecutar comandos que extraigan /var/log y lo suban a S3.

- En Azure, se recolectan los Azure Activity Logs (que cubren operaciones a nivel control-plane), logs de Azure AD (inicios de sesión, etc.), y logs específicos de recursos (diagnostic logs). Azure ofrece exportar estos logs a un área de trabajo Log Analytics o a archivos CSV/JSON desde el portal. También con Azure CLI se puede consultar:

```
az monitor activity-log list --resource-group GrupoX --offset 30d > activitylogs.json

az monitor log-analytics query -w <WorkspaceID> --analytics-query "SecurityEvent | where TimeGenerated > ago(7d)"
```

(Este segundo requiere que los logs se hubieran enviado a Log Analytics). Alternativamente, muchas veces más práctico es usar el portal: Azure permite descargar registros filtrados en CSV.

- En SaaS (O365, G Suite, etc.), la extracción de logs suele hacerse vía funciones de auditoría: por ejemplo, Office 365 Unified Audit Log puede buscarse vía PowerShell o interfaz y exportar resultados (correos enviados, actividades en OneDrive, etc.). G Suite tiene un *Access Transparency* logs y Admin Audit logs que se pueden descargar. Herramientas como Magnet Axiom Cloud ya hacen esta recolección utilizando las API oficiales subyacentes.

- **Recolección de datos de usuario (contenido):** Además de logs, muchas investigaciones requieren obtener el contenido en sí: archivos, correos, base de datos. Aquí hay que balancear volumen vs relevancia. Estrategias:

1. Para storages (ej. Amazon S3, Azure Blob, Google Cloud Storage): identificar qué contenedores (buckets) son relevantes y hacer dumps de su contenido. Por ejemplo, si se sospecha que un bucket S3 fue accedido indebidamente, se puede ejecutar:

```
aws s3 sync s3://nombre-bucket./evidencia/bucket_nombre
```

para descargar todo su contenido (cuidando no alterar metadatos; *sync* en modo lectura es seguro). Esto puede ser pesado, pero garantiza tener copia local. Alternativamente, si el bucket es enorme, filtrar por prefijos o fechas. Generar listados (aws s3 ls) para inventario y luego decidir.

2. Para bases de datos en la nube (RDS, Azure SQL, Firestore): siempre que sea posible, generar un backup o snapshot de la base de datos. En RDS MySQL, por ejemplo, crear un snapshot manual o usar la opción de database snapshot. Ese snapshot se puede montar en otra instancia de base de datos para extraer datos específicos. Otra vía es realizar *dumps* lógicos (mysqldump, pg_dump) pero eso ya es un análisis dentro.
3. Para servicios SaaS: descargar contenidos mediante exportaciones nativas (Google Takeout for enterprise, eDiscovery de Office 365) o con herramientas especializadas. Por ejemplo, en un caso de investigación de correo electrónico en Office 365, usar la herramienta de eDiscovery Content Search para exportar todos los correos de ciertos buzones en formato PST. O en GMail, usar Google Takeout para cuenta específica (si se tiene credenciales del usuario cooperante). **Importante:** dichas exportaciones deben ser recibidas sin alteración y verificadas con hash.

- **Documentación durante la recolección:** Cada elemento recolectado se registra: qué es, de dónde proviene (fuente cloud, servicio, ruta), cuándo se obtuvo, quién lo obtuvo. Se calculan hashes a todo lo descargado (por ejemplo, si se descargó un log en JSON, se calcula hash SHA-256 del archivo JSON guardado). Si la recolección es remota y voluminosa, a veces conviene usar scripts que generen los hashes sobre la marcha o dividan en partes (p.ej., descargar en archivos segmentados de 1GB y hash cada uno). Esto por qué: la descarga podría corromperse o ser incompleta sin darse cuenta; el hash

verifica integridad y permite en juicio demostrar que lo que se analizo es exactamente lo que se extrajo.

En síntesis, la recolección directa en la nube requiere habilidades tanto en el uso de APIs/CLI del proveedor, como en manejo de herramientas forenses tradicionales una vez los datos están fuera. Es una fase muy técnica y con riesgo de cometer errores (por ejemplo, omitir un volumen, exportar mal un log). Por ello suelen usarse checklists para asegurarse de capturar todo lo necesario: snapshots de todas las instancias relevantes, todos los logs de X días alrededor del incidente, etc.

9.3.3 Recolección mediante Solicitud a Proveedores Cloud (vía Autoridades)

Hay situaciones en las que el equipo forense, por sí solo, no puede recolectar la evidencia porque ésta reside completamente en la infraestructura del proveedor y no se dispone de credenciales de acceso. Ejemplos: un delito cometido a través de una cuenta de Facebook, una investigación de mensajes de WhatsApp, la necesidad de recuperar archivos eliminados en Google Drive donde ni el usuario tiene ya acceso, o averiguar la identidad detrás de una cuenta anónima en algún servicio. En estos casos, se debe recurrir al procedimiento legal de solicitud de información al proveedor de servicios, normalmente a través de la Fiscalía y con orden judicial.

Pasos generales de este proceso:

- **Coordinación con Fiscalía/Autoridad competente:** El perito (o la unidad investigativa) comunica a la Fiscalía los detalles del caso y qué información se requiere del proveedor. Por ejemplo: *"Se solicita a la Fiscalía gestionar ante Facebook Inc. la obtención del historial de conversaciones de la cuenta <usuario>, entre el 01/07/2025 y el 30/07/2025, por presunta extorsión digital"*. La Fiscalía prepara un oficio formal, respaldado en los artículos legales pertinentes.
- **Canales oficiales con los CSP:** Empresas como Meta, Google, Microsoft tienen portales y departamentos legales para tratar requerimientos de gobiernos. En Ecuador, la unidad de delitos informáticos se encarga la Fiscalía General del Estado. Dependiendo del delito, la Fiscalía emite un requerimiento escrito que se envía a estos proveedores mediante los canales designados (a veces embajadas, a veces directamente vía correo electrónico seguro o portal web de cumplimiento legal) (Red Seguridad, 2020).

- **Contenido de la solicitud:** Debe ser lo más específica posible: identificar claramente la cuenta (ej. dirección de correo asociada, ID de usuario si se conoce), el tipo de datos requeridos (contenido de mensajes, metadatos de acceso, registros de creación de cuenta, direcciones IP usadas, etc.) y el marco legal que respalda la petición (p. ej., "estos datos son requeridos en investigación previa No. 123-2025, por el presunto delito de acceso no autorizado, tipificado en el Art. 234 COIP"). También se adjunta la orden judicial o fiscal que autoriza la diligencia.
- **Preservación previa:** Muchas veces primero se envía una orden de preservación (preservation letter) para que la compañía guarde los datos antes de que sean borrados por su ciclo normal o por el usuario. Esto es crucial, ya que el proceso legal puede tardar días o semanas, y un usuario malicioso podría mientras tanto eliminar evidencias. Las empresas suelen acatar estas órdenes de preservación por un periodo (90 días es común).
- **Recepción de la evidencia:** Una vez aprobada la solicitud, la empresa entrega la información. Puede ser mediante un enlace seguro de descarga o por envíos físicos cifrados. Por ejemplo, Google puede proporcionar un archivo comprimido cifrado con los datos de una cuenta, y envía la contraseña separadamente a la autoridad requirente. La Fiscalía/Policía recibe esto y lo ingresa en cadena de custodia. *Es esencial que al recibirse la información, el perito calcule inmediatamente sus hashes y los registre*, y verifique que los datos corresponden a lo pedido.
- **Análisis de la información proporcionada:** El proveedor suele entregar un informe desglosado o datos en bruto. Por ejemplo, Facebook entrega un archivo con toda la información de la cuenta (Friends, Messages, IP logs). El trabajo del perito es analizar esos contenidos: buscar en las conversaciones la evidencia del delito, ver qué IPs aparecen y si se pueden geolocalizar, etc. Muchas veces, la información viene voluminosa; se puede entonces cargar en herramientas forenses para bases de datos o texto (Magnet AXIOM importa datos de Facebook, por ejemplo, o se puede escribir scripts).
- **Autenticidad de datos de tercero:** Un desafío es demostrar que esos datos no fueron alterados en el camino. Por eso, es bueno que, en la respuesta, la empresa proveedora certifique los datos (sello o firma digital, o al menos una carta oficial adjunta) y que el perito documente todo el trayecto (de qué correo llegó, quién descargó, etc.). En juicio,

puede ser necesario que un representante del proveedor ratifique la autenticidad vía exhorto o similar, aunque a veces la documentación es suficiente.

En Ecuador, este procedimiento está amparado por cooperaciones internacionales en delitos informáticos (Budapest, etc., del cual el país es Parte, sí colabora con Interpol y acuerdos bilaterales). Un punto a resaltar: el perito local no "toca" directamente los sistemas del proveedor, todo se hace por vía legal. No se podría, por ejemplo, hackear una cuenta criminal para obtener evidencia, ya que sería ilegal y vulneraría la seguridad (además de no ser admisible). Cada unidad debe trabajar según sus competencias, como bien señaló un experto entrevistado: *"lo que no podemos nosotros realizar es aquello que está más arriba... no podemos vulnerar la seguridad de esos sistemas; se coordina con la empresa dueña de la información con las debidas disposiciones legales"*. Siempre con paciencia y trámites, pero es la forma legítima.

Este subprocedimiento, si bien puede resultar menos expedito, es eficaz: las empresas proveedoras pueden entregar datos eliminados siempre que subsistan en sus copias de seguridad o registros y medie la orden judicial correspondiente. Por ejemplo, Google mantiene por un tiempo cierta información tras el borrado; si el caso del señor que eliminó su carpeta de Google Fotos se gestiona con celeridad, es posible recuperar esos archivos desde backups y entregarlos vía Fiscalía. De manera análoga, WhatsApp podría poner a disposición historiales de chat cuando exista respaldo en iCloud o Google Drive, según corresponda. En todos los supuestos, la disponibilidad efectiva depende de las políticas de retención del proveedor, de la fecha del borrado y de la oportunidad con que se curse la solicitud de preservación y entrega.

9.4 Examen y Análisis de la Evidencia Digital

Con la evidencia en mano, comienza la fase de examen (preparación) y luego análisis en profundidad. En la nube, esta fase puede ser especialmente compleja debido a la gran cantidad de datos y a la necesidad de correlacionar eventos en múltiples plataformas. A continuación, se describe cómo abordarla:

9.4.1 Examen o procesamiento inicial de datos:

Antes de interpretar, a menudo hay que procesar los datos brutos para hacerlos manejables:

- **Montaje de imágenes y extracción de datos relevantes:** Por ejemplo, si se obtuvo una imagen forense de una máquina virtual Linux comprometida, se monta esa imagen (preferentemente de solo lectura) en una estación de análisis. Se puede usar X-Ways,

FTK o simplemente herramientas nativas (mount -o ro en Linux) para acceder al sistema de archivos. Luego se extraen ciertos artefactos: registros de sistema (/var/log/...), archivos de configuración, historiales de bash (.bash_history), etc. Si la VM era Windows: extraer registros de eventos (Security.evtx, etc.), SAM, Sysmon logs si existieran, archivos de usuarios (Documentos), prefetch, etc. Esta extracción puede ser manual o usando automatización (por ej., Volatility plugins para SAM, o Plaso/*Log2Timeline* para generar un super-timeline de la imagen). En entornos cloud, a veces se debe tener cuidado con formatos (p.ej., si la VM usaba LVM o varios volúmenes).

¿Qué hace mount -o ro en Linux?

La opción -o ro monta el sistema de archivos en modo solo lectura. Eso significa que el kernel bloquea cualquier operación de escritura (crear, borrar o modificar archivos y metadatos), ayudando a preservar la integridad forense.

Recomendaciones por tipo de FS:

1. ext4: usar -o ro,noload para evitar cargar/reproducir el journal.
2. XFS: usar -o ro,norecovery para evitar replay del log.
3. NTFS: usar ntfs-3g -o ro.

Imágenes de disco: preferir losetup -r (read-only) y luego montar:

1. losetup -rP /dev/loop0 imagen.dd → mount -o ro /dev/loop0p1 /mnt/evidencia
2. Si hay LVM: kpartx -av imagen.dd → vgchange -ay --readonly → montar con -o ro.

- **Conversión de formatos de registro:** Muchos logs cloud vienen en JSON, CSV o formatos propietarios. Es útil convertirlos a un formato apto para análisis. Por ejemplo, cargar los logs de CloudTrail (JSON) en una herramienta SIEM o en una base de datos para hacer consultas. O convertir los Activity Logs de Azure (JSON) a CSV para filtrarlos en Excel. Esto se considera examen, no análisis, ya que solo estamos transformando datos, no concluyendo aún.
- **Filtrado inicial – scope reduction:** Si el volumen de datos es enorme (imaginemos miles de horas de logs, o terabytes de archivos), se aplica un filtro según lo definido en fases previas. Por ejemplo, centrarse en las fechas del incidente. Un caso típico: se sabe que la intrusión ocurrió el 5 de agosto de 2025 a las 10:00pm. Entonces, al preparar CloudTrail, uno filtra eventos del 5 y 6 de agosto principalmente. Sin descartar por

completo lo demás (podría ser relevante), pero priorizando. Herramientas de análisis permiten estos filtros fácilmente.

- **Verificación de integridad durante examen:** Cada vez que se extrae un archivo de una imagen o se convierte un log, es prudente asegurar que no se altere. Por ello, se trabaja sobre copias, y en lo posible se recalculan hashes de lo importado y se comparan con el original para estar seguros. Por ejemplo, si se exportó un archivo de evidencias, comprobar que su hash coincide con cuando fue adquirido.
- **Uso de herramientas de timeline:** En incidentes complejos, es muy útil construir **líneas de tiempo** unificadas. Existen utilidades (p. ej., Plaso, SleuthKit mactime) que a partir de la imagen de disco generan eventos (por marcas de tiempo de archivos). En la nube, complementariamente, se integran esos timelines con los logs de auditoría cloud. Así se puede ver, por ejemplo: A las 10:05pm CloudTrail muestra que el atacante inició la instancia; a las 10:06pm en la línea de tiempo del sistema aparece un nuevo proceso en la VM (que coincide con malware), etc. Esta correlación en timeline es potente para reconstruir la narrativa.

9.4.2 Análisis Forense e Interpretación:

Con la evidencia preservada y adquirida, se inicia la fase de análisis, cuyo propósito es interpretar los datos para responder a las preguntas forenses clave: qué ocurrió, cómo ocurrió, quién intervino y cuáles fueron las consecuencias. Si bien las técnicas específicas dependen del tipo de incidente, pueden observarse las siguientes:

- **Reconstrucción de eventos:** Siguiendo metodologías como las de ISO 27042, se va reconstruir la secuencia de acciones. Por ejemplo, en una intrusión:
    1. Vector de ingreso: buscar evidencias de cómo entró el atacante. Esto puede ser en logs (un login sospechoso, una elevación de privilegios, un exploit vía un puerto abierto).
    2. Acciones durante la intrusión: identificar comandos ejecutados (analizando shell histories, comandos registrados en CloudTrail como *InvokeSSM*, etc.), movimientos laterales (acceso a otras instancias, creación de nuevos usuarios, etc.).
    3. Exfiltración o daño: evidencias de que datos fueron extraídos (ej. volúmenes montados y volcados, uso inusual de comandos de copia a S3, gran tráfico saliente en Flow Logs) o de sabotaje (comandos de borrado, volúmenes eliminados).

4. Cobertura de huellas: revisar si hay indicios de que el atacante intentó borrar logs o instalar puertas traseras. En la nube, por ejemplo, ver si CloudTrail fue deshabilitado temporalmente (eso quedaría registrado antes de apagarse), o en la VM, si se borraron archivos de log (huecos en fechas, reinicios inexplicables).

Todo lo anterior se apoya en herramientas:

- **Búsqueda de indicadores**: Utilizar *IoCs* (Indicators of Compromise) conocidos. Por ejemplo, si se sabe que cierto malware de cryptojacking deja un binario xmrig, buscarlo en la imagen de disco. O si cierto atacante usa una dirección IP particular, buscar en logs de conexión esa IP.
- **Análisis de malware**: Si se halló un ejecutable sospechoso en la VM, se extrae para análisis estático o dinámico en un ambiente controlado. Entender qué hace, si se conectaba a algún servidor, etc., ayudará a completar la historia. Esto a veces se hace en colaboración con especialistas de malware.
- **Análisis de comunicaciones y correlación con otros eventos:** En entornos distribuidos, quizás el intruso tocó varios sistemas. Comparar logs de distintas fuentes: por ejemplo, en Azure AD se ve que la misma IP hizo login en la cuenta admin; en AWS CloudTrail la misma IP aparece en llamadas a la API. Esa correlación confirma que es el mismo actor y amplía el alcance.
- **Análisis de cuentas de usuario:** Si la hipótesis es un abuso interno, se analizará el patrón de actividad del sospechoso en la plataforma cloud vs usuarios normales. Herramientas de SIEM o incluso Excel pueden servir para ver tendencias.

- **Interpretación y atribución:** Más allá de qué pasó, muchas veces interesa quién fue. La nube provee ciertos datos que ayudan a atribuir:
  - Direcciones IP de origen de accesos (que se pueden geolocalizar o asociar a proveedores de Internet). Por ejemplo, ver que el atacante se conectó desde una VPN o desde otro país. Esto se documenta y eventualmente se puede coordinar con proveedores de Internet para identificar al suscriptor de esa IP (ya sería extensión de investigación).
  - Identificadores únicos: en algunos casos, un mismo atacante puede reutilizar nombres de instancia, o IDs de cuenta. Si se investiga a un grupo organizado, se puede comparar con otros casos.

- Patrón de comportamiento: la técnica utilizada, el horario de ejecución y las rutas de acceso pueden ofrecer indicios sobre la autoría del incidente. Por ejemplo, un empleado con acceso legítimo (insider) suele conocer con precisión la ubicación de los datos sensibles y utilizar credenciales o permisos internos, mientras que un atacante externo tiende a recurrir a métodos como fuerza bruta, explotación de vulnerabilidades o uso de credenciales filtradas. Estos elementos, contrastados con información de inteligencia sobre amenazas y patrones de modus operandi previamente documentados, permiten orientar hipótesis más sólidas respecto al origen del ataque.
- Importante: la atribución definitiva puede requerir acciones adicionales (órdenes judiciales a ISP, etc.), pero el análisis forense en la nube da las pistas iniciales. Por ejemplo, se logro saber que la cuenta atacante fue "Jeff123" y usó IP de X, de tal ciudad, a tal hora. Con eso la policía puede luego ubicar al titular de la línea.

- **Análisis forense de evidencias provistas por el proveedor:** Cuando la evidencia viene de un tercero, el análisis consiste en revisar esa información con miras a responder preguntas del caso. Muchas veces los informes de empresas vienen ya estructurados: por ejemplo, "Datos de Suscriptor: nombre, email, teléfono asociado"; "Historial de conexiones: IPs y timestamps"; "Contenido de conversaciones: ...". El perito debe:
  - Verificar consistencia (¿las fechas concuerdan con los hechos denunciados?, ¿se observa la conducta ilícita en el contenido?, ¿hay lagunas de información?).
  - Resumir hallazgos relevantes. No es necesario volcar *todo* el contenido en el informe final, pero sí extraer las partes clave (p.ej., captura de pantalla o transcripción de los mensajes amenazantes, enumerar las 5 IP que más se usaron y su origen geográfico).
  - No alterar la evidencia: Si hay lenguaje inapropiado o datos sensibles, se debe consignar tal cual está en la evidencia, quizás con reserva en el informe público, pero anexar la transcripción completa bajo cadena custodia). Esto ya es parte de presentación, pero se decide en análisis qué incluir y cómo.
- **Mantenimiento de la trazabilidad en análisis:** Conforme se analizan los datos, se debe mantener una bitácora de qué se hace. Por ejemplo: "Se realizó búsqueda de la cadena 'DELETE FROM' en los logs de SQL, hallando 3 resultados". De preferencia,

conservar querys, comandos ejecutados (script utilizados). Muchas herramientas generan reportes o permiten exportar los resultados encontrados (e.g., FTK reporta archivos encontrados con cierto hash, Splunk permite exportar resultados de una consulta). Estos outputs deben guardarse. Así, si se requiere que otro analista o un tercero revise, tienen las mismas bases.

9.4.3 Elaboración de Conclusiones Técnicas:

Tras el análisis detallado, el equipo forense extrae conclusiones sobre lo sucedido. Por ejemplo:

- "El día X a las 22:05 GMT, el usuario administrador Jefferson Maradona fue comprometido mediante contraseña robada, permitiendo al atacante conectarse desde la IP 203.0.113.5 (ubicada en Brasil) al portal de Azure. Luego, el atacante creó una nueva máquina virtual llamada BackdoorVM desde la cual extrajo información de la base de datos corporativa. Se evidenció la descarga de ~500 MB de datos confidenciales. Finalmente, intentó borrar rastros eliminando la VM el día X+1 a las 03:00 GMT, pero los logs de Azure evidenciaron su actividad. No se hallaron indicios de que hubiera persistencia posterior al incidente."

Estas conclusiones se basan en la evidencia concreta hallada. Deben ser sólidas: cada afirmación idealmente respaldada por uno o más artefactos (p. ej., *"log entry ID 12345 muestra login exitoso desde IP tal con user tal"*). Además, es necesario señalar cualquier incertidumbre. Por ejemplo: *"No se pudo determinar el medio exacto por el cual se obtuvo la contraseña (pudo haber sido phishing, dado que no se registraron intentos de fuerza bruta)"*, o *"No fue posible recuperar dos archivos porque el proveedor informó que ya habían sido sobrescritos"*.

9.5 Presentación de la Evidencia y Elaboración de Informes

La fase final consiste en presentar los hallazgos de manera clara, completa y objetiva, usualmente mediante un informe pericial forense escrito, acompañado de anexos con las evidencias pertinentes y, de ser requerido, la comparecencia del perito ante la autoridad competente para ratificar su informe.

- **Estructura del informe:** Debe seguir las pautas institucionales o judiciales. Típicamente incluye: Introducción (objetivo del peritaje, quién lo solicita, alcances), Descripción del caso (resumen del incidente investigado), Procedimientos realizados (paso a paso de identificación, recolección, análisis – sin agobiar con detalles técnicos pero sí los importantes para legalidad), Resultados u hallazgos (lo que se encontró,

evidencias principales), Conclusiones (respondiendo a las preguntas investigativas, confirmando o descartando hipótesis), y Recomendaciones (en casos técnicos, sugerir mejoras o acciones para evitar futuros incidentes, si es parte del encargo). La guía NIST 800-86 enfatiza incluir también cualquier limitación encontrada y el grado de confianza de los hallazgos.

- **Incorporación de evidencias en el informe:** Es fundamental adjuntar o insertar las evidencias digitales más relevantes que soportan las conclusiones (Soto, 2022). Por ejemplo, si se afirma que "el usuario borró la carpeta a tal hora", adjuntar la porción de log que lo muestra, o una captura de pantalla del registro. En entornos cloud, muchas evidencias son texto (logs) pero también pueden ser imágenes (captura de configuración, foto de la pantalla de la VM en el momento del allanamiento, etc.). Se pueden incluir fragmentos de código o comandos ejecutados, para ilustrar metodología, pero el informe principal debe ser legible para personas no técnicas, por lo que quizás esos detalles van en anexo técnico.
- **Cadena de custodia en la presentación:** Se debe describir brevemente cómo se mantuvo la cadena de custodia. A veces se anexa una tabla con el registro de custodia (ver plantilla en sección 12.1). Esto muestra al juez que, desde la obtención en la nube hasta tenerlo en el escritorio del analista, todo estuvo controlado. Algunos informes incluyen un apartado "Integridad de la evidencia digital", donde se listan los hashes de las principales piezas (imágenes de disco, etc.), indicando que se verificaron antes y después del análisis, etc.
- **Consideraciones legales en el informe:** Además de los hallazgos técnicos, hay que enmarcarlos en la legalidad. Por ejemplo, indicar que la intervención en la cuenta tal fue autorizada por orden No. X, o que tal evidencia fue obtenida mediante cooperación de la empresa Y en fecha Z. Esto blinda el informe ante cuestionamientos de obtención ilícita. También, si se omitió algo por respeto a la ley (ej: "no se accedió al contenido de ciertos correos por estar fuera del alcance del caso y contener posiblemente información personal no relacionada, en cumplimiento de LOPDP"), señalarlo.
- **Lenguaje claro y exactitud:** La presentación debe ser entendible para personas sin conocimiento profundo en cloud. Por ello, se evita en lo posible jerga técnica sin explicar. Si se menciona "snapshot forense", probablemente se agrega "(copia exacta de un disco virtual en la nube)". Se debe ser muy exacto en nombres y valores: ID de

cuentas, fechas con zona horaria, unidades (MB, GMT, etc.). Un truco es incluir un glosario de términos técnicos como anexo si el informe es extenso.

- **Popularización de incidentes en medios o audiencias:** En casos de alto interés, los informes pueden hacerse públicos. El perito debe ceñirse estrictamente a los hechos acreditados y evitar especulaciones. Las conclusiones deben ser verificables y estar sustentadas en artefactos concretos.
  – Ejemplo de conclusión válida: "El ataque se realizó el 15/08/2025 a las 03:14 UTC, utilizando el usuario svc-backup, desde la IP 203.0.113.17, credenciales confirmadas en el registro AuthLog ID 987654 y correlacionadas con CloudTrail Event ID abc-123."
  – Si existe información faltante, debe indicarse de forma explícita, sin conjeturas: "No fue posible determinar el mecanismo exacto de obtención de la contraseña; no se observó fuerza bruta en los registros analizados."
- **Trazabilidad del análisis en la presentación:** Si la contraparte (defensa) u otro perito leen el informe, deben idealmente poder reproducir los pasos que se dieron para llegar a los hallazgos, si tuvieran acceso a las mismas evidencias. Esto no solo da validez, sino que demuestra profesionalismo y objetividad.
- **Conclusiones firmes, pero dentro de alcance:** Las conclusiones deben ceñirse a lo investigado. Evitar extralimitarse. Por ejemplo, si se investigó un incidente en AWS de X empresa, no concluir sobre la seguridad general de AWS (no viene al caso, y podría malinterpretarse). Sí dar recomendaciones directas: "Se sugiere implementar autenticación de dos factores en las cuentas administradoras para prevenir incidentes similares" – eso muestra un valor agregado y cierra el ciclo aprendiendo del incidente.

Informe Final

18-9-2025

INFORME FINAL DEL ANÁLISIS FORENSE EN LA NUBE

Guía metodológica para el análisis forense digital en plataformas de la nube

Jefferson Fernando Ramirez Lozada
UNIVERSIDAD INTERNACIONAL DEL ECUADOR

INFORME FINAL DEL ANALISIS FORENSE EN LA NUBE

PROCESO BASADO EN LA GUÍA, ESTÁNDARES Y HERRAMIENTAS FORENSES APLICADAS

Fecha y hora de recepción del análisis forense: En este campo deberá consignarse la fecha y hora exacta en la que el perito recibió la orden judicial o fiscal que dispuso la práctica de la pericia.	**INFORME TÉCNICO DEL ANÁ-LISIS FORENSE Nro.** Aquí se registrará el número correlativo del informe pericial, conforme el sistema de control interno del perito o de la institución a la que pertenezca.
Número de proceso	Se deberá anotar el número de expediente judicial o de indagación previa con el que se relaciona el análisis forense.

1. OBJETIVO DE LA INVESTIGACIÓN

En este apartado se establecerá de manera clara el propósito de la pericia, especificando qué se busca determinar. Ejemplo: comprobar la existencia de accesos no autorizados, identificar la procedencia de los mismos, verificar la integridad de la evidencia digital o establecer la magnitud del incidente.

2. ANTECEDES

Se describirá el contexto que dio lugar a la investigación, precisando la denuncia presentada, la autoridad solicitante, las fechas relevantes y una breve exposición de los hechos reportados. Asimismo, se delimitará el objeto de la pericia conforme lo ordenado por la autoridad competente.

3. DATOS DEL PROVEEDOR DE SERVICIOS EN LA NUBE

Proveedor de Cloud: Se deberá consignar el nombre completo del proveedor (ej. Amazon Web Services, Microsoft Azure, Google Cloud Platform, Microsoft 365).	Tipo de Plataforma: IaaS ☒PaaS ☐ SaaS ☒
Servicio Afectado: Se especificará el servicio concreto en el que se detectó el incidente (ej. EC2, S3, OneDrive, Exchange Online)..	Región o Zona: : Se anotará la localización del servicio en la nube (ej. us-east-2, Europa Oeste).
Url: Dirección o endpoint del recurso comprometido.	Credenciales Otorgadas: Si ☐No ☐
Medio de preservación: Snapshot ☐ / Imagen RAW ☐ / Logs exportados ☒ / Otro ☒	Hash Calculado: Aquí se registrará el valor hash (SHA-256, SHA-512) correspondiente a la evidencia.

Fecha de activación (Tiempo cero): **Fecha y hora en que el perito inició formalmente el procedimiento forense.**	Estado de los servicios: Encendido ☐ / Apagado ☐ / Suspendido ☐
Id de la cuenta / Correo electrónico: Se anotará el identificador de la cuenta o el correo vinculado al servicio.	
Descripción: Breve reseña del recurso analizado (ej. "Servidor web vulnerado", "Cuenta de correo comprometida").	

4. EVALUACIÓN DEL INCIDENTE

Evidencias preliminares identificadas: Relación de archivos, logs o imágenes forenses recolectadas.
Clasificación del incidente: Tipología (intrusión, malware, fuga de información, phishing, ataque DDoS, etc.).
Activos comprometidos: Enumeración de los sistemas, bases de datos o servicios afectados.
Alcance inicial estimado del incidente: Determinación del impacto preliminar (un usuario, varios servidores, múltiples servicios).
Riesgo asociado: Evaluación del nivel de riesgo técnico, operativo o legal.
Medidas inmediatas de contención aplicadas: Acciones realizadas para evitar la propagación o agravar el incidente (ej. aislamiento de instancias, suspensión de credenciales).
Responsable de la evaluación: Identificación del perito o equipo a cargo de la fase de evaluación.

5. Metodología aplicada

Se describirán los estándares y normas empleadas, las herramientas utilizadas y el procedimiento metodológico seguido.
Se deberán detallar las fases aplicadas: identificación, preservación, adquisición, análisis y presentación de los hallazgos.

6. Conclusiones

En este punto se emitirán los resultados técnicos de la investigación, de manera clara, objetiva y sustentada. Las conclusiones deberán responder únicamente al objeto de la pericia y pueden referirse, entre otros, a:

1. La confirmación o descarte de un incidente.
2. La tipología del ataque o evento detectado.
3. El alcance sobre los activos comprometidos.
4. La integridad y autenticidad de la evidencia obtenida.

7. DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO.

Se adjuntará y describirá la documentación de soporte, tales como capturas de pantalla, bitácoras, registros de logs, tablas de hashes, copias de cadena de custodia, reportes de herramientas o diagramas explicativos.
Asimismo, se justificará técnicamente cómo cada documento respalda las conclusiones presentadas..

8. DECLARACIÓN DEL EXPERTO EN ANÁLISIS FORENSE

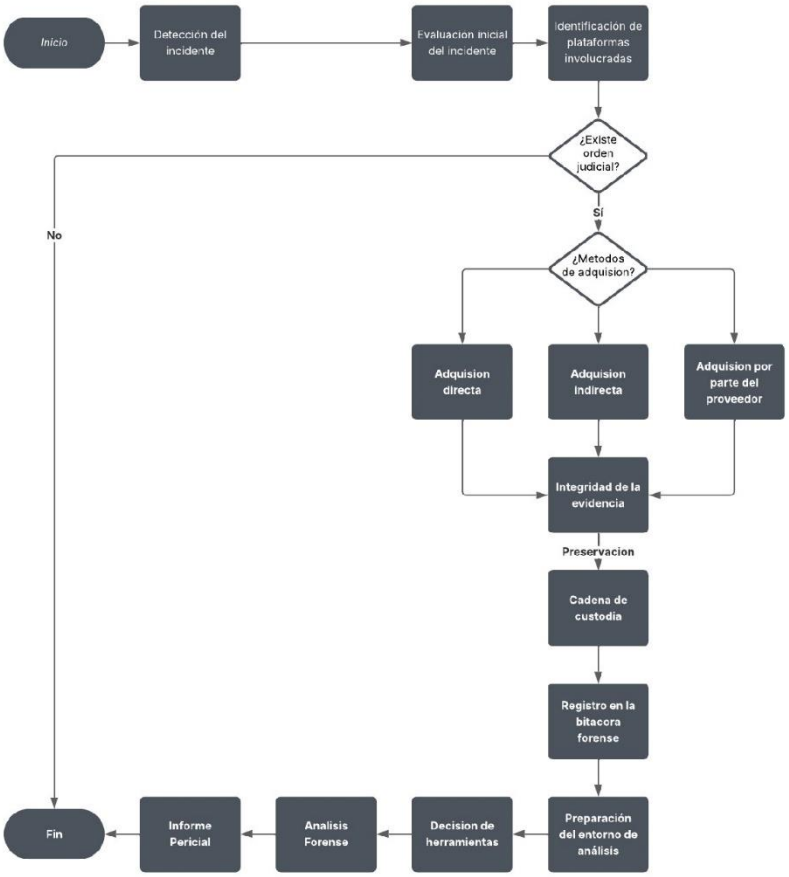
El experto en análisis forense declara bajo juramento que el presente informe se elaboró de manera independiente, que responde a su real convicción profesional y que toda la información proporcionada es verdadera. Asimismo, deja constancia de que los procedimientos aplicados, los resultados obtenidos y las conclusiones expuestas se encuentran debidamente documentados y sustentados en la evidencia técnica incorporada al expediente.

9. **FIRMA DE RESPONSABILIDAD**

Nombres Completos	Firma
Se consignará el nombre completo del perito.	
Especialidad: Se anotará el área profesional específica.	**Área De Acreditación:** Se indicará la entidad de acreditación
Teléfono: Número de contacto.	**Correo:** Dirección de correo electrónico válida.

Ilustración 1

Diagrama de flujo de la Guía Forense Digital en la Nube



10. Conclusiones

La guía se presenta como un documento de buenas prácticas para investigaciones forenses en entornos cloud, dirigido específicamente a expertos forenses, equipos de respuesta a incidentes (CSIRT) y peritos informáticos. Su alineación con estándares internacionales (ISO/IEC 27037, 27042, 27043, RFC 3227, NIST SP 800-86) aporta rigor técnico al proceso de identificación, preservación, adquisición, análisis y presentación de evidencia digital. Al mismo tiempo, incorpora de manera explícita el marco legal ecuatoriano (COIP, LOPDP, LOTAIP, Ley de Comercio Electrónico, etc.), garantizando que las prácticas propuestas sean válidas y admisibles en el contexto judicial local. Esto asegura que los hallazgos forenses obtenidos con esta guía cumplan tanto criterios técnicos como legales.

Metodológicamente, la guía está estructurada de forma clara y detallada: cubre todas las fases esenciales del análisis forense digital (identificación de incidentes, recolección y preservación de evidencia, análisis técnico y presentación de resultados) bajo lineamientos globales y nacionales. Se describen roles definidos (analista forense, coordinador, experto cloud, asesor legal, custodio, etc.) y se proporcionan protocolos concretos (por ejemplo, cadenas de custodia, flujos de acceso a datos cloud) que estandarizan el procedimiento. En la práctica, esto contribuye a reducir errores durante la recolección de evidencia y facilita la elaboración de informes judiciales sólidos.

En cuanto a herramientas, la guía recomienda soluciones especializadas ya reconocidas (por ejemplo, Magnet AXIOM Cloud, Cellebrite UFED Cloud, X-Ways, etc.) adaptadas a plataformas como AWS, Azure y GCP. Se enfatiza el uso de software validado, con registro de hashes y logs para mantener la integridad de la evidencia. Esta orientación práctica hacia herramientas compatibles con la nube aumenta notablemente la aplicabilidad del documento en escenarios reales. En conjunto, la guía demuestra ser un recurso de gran utilidad para el ámbito ecuatoriano de ciberseguridad: al integrar estándares internacionales con la normativa local, fortalece la capacidad de respuesta ante incidentes informáticos en Ecuador.

11. Recomendaciones

La guía se centra en herramientas existentes reconocidas, pero el campo cloud evoluciona constantemente. Se recomienda ampliar y revisar regularmente el listado de software (incluyendo nuevas versiones y soluciones de código abierto) para mantener al día las recomendaciones.

Actualmente se presentan dos ejemplos de informe final en el anexo. Ampliar esta sección con casos de estudio adicionales (por ejemplo, incidentes en diferentes servicios cloud, proveedores menos comunes o contextos híbridos) reforzaría el aprendizaje práctico y mostraría la versatilidad del procedimiento en situaciones reales.

Dado que el documento está enfocado al contexto ecuatoriano, sería útil incorporar referencias comparativas a legislaciones o estándares internacionales (por ejemplo, directrices de la Cloud Security Alliance u otros códigos penales) para facilitar su uso en entornos jurídicos distintos. Esto permitiría que la metodología propuesta sea adaptable a otros países o regiones con normativas de privacidad y ciberseguridad diferentes.

Complementar la guía con talleres, simulaciones y capacitaciones periódicas, de manera que los equipos forenses y de respuesta a incidentes mantengan actualizados sus conocimientos y habilidades en el uso de procedimientos y herramientas.

12. Bibliografía

(1 de Diciembre de 2024). Obtenido de AWS Security Incident Response User Guide: https://docs.aws.amazon.com/pdfs/security-ir/latest/userguide/sir-ug.pdf#collect-relevant-artifacts

Asamblea Nacional de Ecuador. (10 de Febrero de 2014). *Codigo organico integral penal.* Obtenido de Registro oficial suplemento 180: https://www.asambleanacional.gob.ec/es/system/files/document.pdf

Báez, J. (13 de Febrero de 2025). *DREAMLAB TECHNOLOGIES.* Obtenido de Principales desafios del analisis forense digital en entornos cloud: https://dreamlab.net/en/blog/principales-desafios-del-analisis-forense-digital-en-entornos-cloud/#:~:text=complejidades%20adicionales,la%20necesidad%20de%20herramientas%20especializadas

Ecuador, A. N. (12 de Septiembre de 2014). Obtenido de Ley especial de Telecomunicaciones : https://www.telecomunicaciones.gob.ec/wp-content/uploads/2015/04/LEY-ESPECIAL-TELECOMUNICACIONES.pdf

Ecuador, A. N. (26 de Mayo de 2021). Obtenido de Ley organica de proteccion de datos: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Fonseca, M. R. (10 de Febrero de 2023). *SANS.* Obtenido de AWS Cloud Log Extraction: https://www.sans.org/blog/aws-cloud-log-extraction

red seguridad . (28 de Octubre de 2020). Obtenido de Introducción al análisis forense en entornos 'cloud': https://www.redseguridad.com/especialidades-tic/cloud-y-virtualizacion/introduccion-al-analisis-forense-en-entornos-cloud_20201028.html#:~:text=1,a%20facilitar%20seg%C3%BAn%20qu%C3%A9%20evidencias

Red Seguridad. (28 de Octubre de 2020). Obtenido de Introducción al análisis forense en entornos 'cloud': https://www.redseguridad.com/especialidades-tic/cloud-y-virtualizacion/introduccion-al-analisis-forense-en-entornos-cloud_20201028.html#:~:text=1,a%20facilitar%20seg%C3%BAn%20qu%C3%A9%20evidencias

Services, A. W. (23 de Noviembre de 2020). Obtenido de Guía de respuesta ante incidentes de seguridad de AWS: Guía : https://d1.awsstatic.com/whitepapers/es_ES/aws_security_incident_response.pdf#:~:text=%3E%20aws%20ec2%20describe,scaling

Soto, M. G. (2022). *Analisis Forense Informatico.* Obtenido de https://books.google.com.ec/books?hl=es&lr=&id=7D-iEAAAQBAJ&oi=fnd&pg=PA7&dq=Todo+lo+que+necesitas+saber+sobre+el+an%C3%A1lisis+forense+en+la+nube&ots=rl3FdJiFO4&sig=OUwc2451v3XPvMahayXzvQhZUZI&redir_esc=y#v=onepage&q=Todo%20lo%20que%20necesitas%20saber%2

13. Anexo:

Informe Final Caso 1

18-9-2025

INFORME FINAL DEL ANÁLISIS FORENSE EN LA NUBE

Guía metodológica para el análisis forense digital en plataformas de la nube

Jefferson Fernando Ramirez Lozada
UNIVERSIDAD INTERNACIONAL DEL ECUADOR

INFORME FINAL DEL ANALISIS FORENSE EN LA NUBE
PROCESO BASADO EN LA GUÍA, ESTÁNDARES Y HERRAMIENTAS FORENSES APLICADAS

Fecha y hora de recepción de la orden pericial: 21/07/2025 09:00:00	**INFORME TÉCNICO PERICIAL Nro.** **001-2025-FGE-IF**
Número de proceso	FGE-UI-DIT-2025-0913-002

1.- OBJETIVO DE LA INVESTIGACIÓN

Determinar la existencia de accesos no autorizados en la instancia AWS EC2 denominada "CasoPractico", establecer la tipología del ataque, identificar los activos comprometidos, verificar la integridad de la evidencia recolectada y sustentar técnicamente los hallazgos para el proceso penal en curso.

2.- ANTECEDES

El 21 de julio de 2025, la fiscalía provincial de Loja recibió denuncia formal interpuesta por el ciudadano Santiago Emilio Pérez López (35 años), quien reportó un presunto delito informático relacionado con accesos no autorizados a su servidor en la nube de Amazon Web Services (AWS). Dicho servidor, identificado como "CasoPractico", alojaba información sensible de su empresa y presentaba indicios de manipulación indebida.

El denunciante indicó que, desde el 15/07/2025, observó conexiones sospechosas en los registros de Apache, provenientes de direcciones IP desconocidas, así como modificación de archivos críticos sin autorización. El 16/07/2025 detectó la presencia de scripts maliciosos en directorios del servicio Apache, lo que reforzó la hipótesis de una intrusión. Como medida preventiva, procedió a reiniciar el servidor y cambiar las credenciales de acceso, temiendo que datos confidenciales de clientes hubieran sido comprometidos.

Ante la denuncia, la Fiscalía abrió investigación por la infracción tipificada en el artículo 234 del Código Orgánico Integral Penal (COIP), relativa al acceso no consentido a sistemas informáticos. Para el efecto, se emitió oficio mediante el cual se ordenó la práctica de un análisis forense especializado, con los siguientes requerimientos: acceder de manera controlada al entorno AWS, identificar la instancia y su volumen asociado, realizar una adquisición forense bit a bit de la información, calcular valores de hash criptográfico, analizar los registros de acceso y documentar la totalidad del proceso conforme a protocolos de cadena de custodia.

3.- DATOS DEL PROVEEDOR DE SERVICIOS EN LA NUBE

Proveedor de Cloud: Amazon Web Services	**Tipo de Plataforma:** IaaS ☒PaaS ☐ SaaS ☒
Servicio Afectado: Amazon EC2 / Amazon EBS	**Región o Zona:** us-east-2 (Ohio)
Url: http://c2-3-143-215-170.us-east-2.compute.amazonaws.com/	**Credenciales Otorgadas:** Si ☒No ☐

Medio de preservación: Snapshot ☐ / Imagen RAW ☒ / Logs exportados ☐ / Otro ☐	**Hash Calculado:** Aquí se registrará el valor hash (SHA-256, SHA-512) correspondiente a la evidencia.
Fecha de activación (Tiempo cero): 21/07/2025 10:30:00	**Estado de los servicios:** Encendido ☒ / Apagado ☐ / Suspendido ☐
Id de la cuenta / Correo electrónico: jeferalo.0210@gmail.com	
Descripción: EC2 tipo t2.micro con Apache2 y DVWA alojada, reportada como comprometida.	

4.- EVALUACIÓN DEL INCIDENTE

Evidencias preliminares identificadas: access.log, error.log (Apache), exportación AWS CloudTrail, snapshot del volumen EBS.

Clasificación del incidente: Intrusión externa con posible explotación de inyección SQL (SQLi).

Activos comprometidos: Instancia EC2 (Ubuntu + Apache + DVWA), volumen EBS asociado, base de datos local de DVWA (pendiente de confirmación).

Alcance inicial estimado del incidente: 1 servidor web en us-east-2; impacto acotado a la aplicación DVWA.

Riesgo asociado: Compromiso de confidencialidad (exposición de datos), integridad (alteración potencial de archivos/BD) y disponibilidad (degradación eventual del servicio).

Medidas inmediatas de contención aplicadas: Aislamiento de la instancia mediante Security Group restrictivo, creación de snapshot de EBS, exportación de registros y emisión de credenciales forenses de solo lectura.

Responsable de la evaluación: Jefferson F. Ramírez Lozada – Perito Informático Forense acreditado.

5.- METODOLOGÍA APLICADA

1. ISO / IEC 27037, ISO/IEC 27042, RFC 32027, la cual determina los procesos de recopilación de evidencias y su almacenamiento in situ, información técnica que ha permitido desarrollar un proceso metodológico de trabajo pericial en base a las siguientes etapas:
   a) Identificación.
   b) Adquisición.
   c) Preservación.
   d) Análisis.
   e) Presentación del contenido digital.

2. ISO/IEC 27040. (2015). Information technology — Security techniques — Guidelines for the analysis and interpretation of digital. Iso/Iec, 2015. Directrices para el análisis e interpretación de datos.

3. Request For Comments - RFC 3227, "Guía para Recolectar y Archivar Evidencia" Directrices para la recopilación de evidencias y su almacenamiento.

6.- CONCLUSIONES

Tras el examen detallado de la evidencia, se concluye que sí se produjeron accesos no autorizados en la instancia AWS "CasoPractico". Las pruebas obtenidas (imágenes de disco, registros de log, hashes verificados, línea de tiempo de eventos) documentan de manera confiable que un actor externo comprometió el servidor: inyectó comandos SQL en la aplicación DVWA, subió archivos maliciosos y estableció sesiones remotas SSH sin consentimiento del propietario. Estos hechos encajan plenamente en el tipo penal de "acceso no consentido" previsto en el artículo 234 del Código Orgánico Integral Penal (COIP) de Ecuador, el cual sanciona con pena de tres a cinco años a quien acceda indebidamente a un sistema informático o telemático ajeno. En base a las normas de la materia, se considera demostrada la ocurrencia del delito denunciado. Los registros demuestran que el atacante principal es la IP 157.100.58.26, que siguió la cadena lógica: errores de BD (500) ⇒ ejecutar setup ⇒ login exitoso ⇒ reducir seguridad ⇒ SQLi ⇒ exfiltración. Especialmente, el uso de UNION SELECT user, password FROM users coincide con el comportamiento conocido de un exploit de SQLi en DVWA. El análisis forense concluye que este acceso comprometió la base de datos de DVWA, listando usuarios y contraseñas. En cambio, los escaneos de otras IP no obtuvieron éxitos (respuestas 4xx) y parecen independientes (ruido de Internet).

7.- DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO.

1.- Identificación

Detección del incidente

El 21 de julio de 2025, la Fiscalía Provincial de Loja notificó un presunto acceso no autorizado a un servidor AWS EC2 (región us-east-2) que alojaba Apache y la aplicación DVWA con fines didácticos. La alerta se originó por denuncia formal y fue corroborada con anomalías en los registros de Apache que evidencian solicitudes inusuales y posibles intentos de inyección SQL (SQLi). Se estableció como "Tiempo Cero" la hora de activación del protocolo tras la denuncia, y se aseguraron de inmediato los artefactos preliminares. La Fiscalía dispuso la apertura de la investigación pericial y designó al perito responsable, dejando constancia del número de caso y de la autoridad requirente.

Evaluación inicial del incidente

Con los indicios iniciales, el hecho se clasifica como intrusión externa sobre una aplicación web vulnerable (DVWA) con posible explotación SQLi desde la IP 157.100.58.26. Los activos comprometidos abarcan la instancia EC2 y su volumen EBS (que

contiene webroot, configuración y logs), sin evidencia de impacto en otros servicios de la cuenta AWS al momento de la evaluación. El alcance inicial se delimita a un (1) servidor en us-east-2 y a la capa de aplicación; el riesgo afecta principalmente la confidencialidad (posible exposición de datos de DVWA) y, en menor grado, la integridad y disponibilidad. Como contención inmediata se aplicó aislamiento de red mediante Security Group restrictivo, generación de snapshot, retención/exportación de registros y emisión de credenciales forenses temporales de solo lectura.

Identificación de plataformas involucradas

La infraestructura bajo análisis corresponde a AWS como proveedor IaaS. Los servicios identificados incluyen EC2 (VM afectada), EBS (volumen principal), S3 (export/retención de registros) y CloudTrail (auditoría de API). Los recursos afectados son la VM EC2 con Apache+DVWA y su volumen EBS; la región contractual y efectiva es us-east-2. La región de respaldo o replicación se consignará en caso de existir políticas de backup (cold storage). Deben anotarse las cuentas/suscripciones involucradas (ID de cuenta AWS, tenant/proyecto si aplica) y los metadatos relevantes: IP 157.100.58.26, rutas/IDs de logs, roles/credenciales forenses, IDs de snapshot/volumen y estado actual del servicio (aislado en cuarentena).

2.- Adquisición

El procedimiento técnico se llevó a cabo en varias fases secuenciales, siguiendo las mejores prácticas de informática forense para entornos en la nube. A continuación, se describen dichas fases y los comandos utilizados:

Fase 1 – Acceso a AWS con credenciales

En primer lugar, se realizó el acceso remoto a la instancia EC2 de AWS objeto de la pericia. Utilizando las credenciales proporcionadas, el perito estableció una conexión SSH segura hacia el servidor Linux en AWS. Para ello se empleó la clave privada (clave.pem) suministrada en el oficio, asegurando la autenticación sin contraseña. El comando utilizado fue:

```
ssh -i clave.pem ubuntu@ec2-3-143-215-170.us-east-2.compute.amazonaws.com
```

ubuntu@ec2-3-143-215-170.us-east-2.compute.amazonaws.com corresponde al usuario y la dirección pública de la instancia EC2 bajo investigación. Este paso permitió ingresar al sistema de archivos del servidor en modo consola, con privilegios suficientes (usuario ubuntu con capacidad de usar sudo) para realizar las siguientes tareas forenses. Cabe destacar que el acceso se efectuó en modo lectura de la evidencia, evitando en lo posible modificaciones al sistema original. Se documentó la fecha y hora exacta de la conexión inicial, cumpliendo con las exigencias de trazabilidad de la evidencia.

Fase 2 – Creación de carpeta de evidencias

Una vez dentro de la instancia, se procedió a preparar el entorno para la recolección de datos. Es una buena práctica destinar un directorio específico para almacenar la evidencia digital dentro del sistema analizado, minimizando la posibilidad de contaminación de otros archivos. Por ello, se creó una carpeta de evidencias dedicada. El comando empleado fue:

```
sudo mkdir -p /evidencias
```

Con sudo se obtuvieron privilegios de superusuario para asegurarse de que la carpeta pudiera contener copias de todos los archivos necesarios (incluyendo aquellos del sistema operativo que requieren permisos elevados). La ruta elegida fue /evidencias. Tras crearla, se verificó su existencia y se establecieron los permisos adecuados. En esta carpeta se volcarían todos los productos de la adquisición forense (imágenes de disco, hashes, logs extraídos, etc.), manteniendo así organizado el material probatorio dentro de la instancia antes de su transferencia al laboratorio.

Fase 3 – Adquisición de imagen forense

En esta fase crítica, se realizó la adquisición forense de la información principal: una imagen bit a bit del disco del servidor en AWS. El objetivo fue obtener una copia íntegra de la unidad de almacenamiento (/dev/xvda) tal como existía en el momento de la intervención, para luego poder analizarla en laboratorio sin alterar el original. Para lograr esto, se utilizó la herramienta estándar dd, ampliamente empleada en informática forense para clonar discos a nivel de bloques. El comando ejecutado fue:

sudo dd if=/dev/xvda of=/evidencias/imagen_dvwa.dd bs=4M conv=fsync status=progress

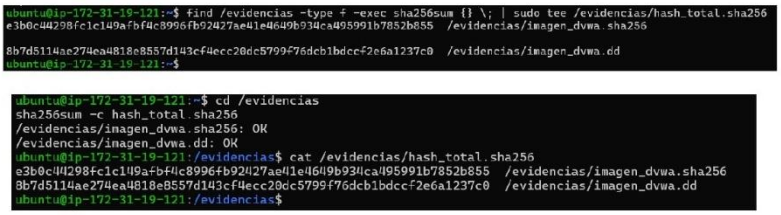
```
ubuntu@ip-172-31-19-121:~$ sudo mkdir -p /evidencias
sudo dd if=/dev/xvda of=/evidencias/imagen_dvwa.dd bs=4M conv=fsync status=p
rogress
16928210944 bytes (17 GB, 16 GiB) copied, 257 s, 65.9 MB/s
dd: error writing '/evidencias/imagen_dvwa.dd': No space left on device
4039+0 records in
4038+0 records out
16937639936 bytes (17 GB, 16 GiB) copied, 257.35 s, 65.8 MB/s
ubuntu@ip-172-31-19-121:~$
```

if=/dev/xvda indica que la entrada (input file) es el dispositivo de disco de la instancia (que en AWS típicamente se presenta como /dev/xvda para el volumen raíz), y of=/evidencias/imagen_dvwa.dd designa el archivo de salida donde se almacenará la imagen forense. Se usó un tamaño de bloque (bs) de 4 megabytes para optimizar la velocidad de copia, conv=fsync para forzar la escritura completa de los datos al finalizar (asegurando que el sistema vacíe cualquier caché pendiente al disco) y status=progress para monitorear en tiempo real el progreso de la clonación. Durante este proceso, se tuvo especial cuidado de no montar ni interactuar con el sistema de archivos de origen más de lo necesario, previniendo modificaciones. El resultado fue un archivo imagen bit-a-bit raw (formato DD) que contiene todo el contenido del disco (espacio usado y no usado) tal cual estaba en el momento del análisis, garantizando una copia fiel del estado del servidor. Esta imagen constituye la evidencia primaria para el análisis forense posterior.

Fase 4 – Cálculo de hash SHA-256

Con la imagen forense generada, el siguiente paso fundamental fue calcular un hash criptográfico de la misma para asegurar su integridad. En ciencias forenses digitales, el hash (a menudo MD5, SHA-1 o SHA-256) actúa como una "huella digital" única del archivo; cualquier alteración por mínima que sea en la evidencia cambiaría este valor, alertando de posible contaminación. En este caso se optó por SHA-256 por su mayor resistencia a colisiones. El comando utilizado fue:

find /evidencias -type f -exec sha256sum {} \; | sudo tee /evidencias/hash_total.sha256



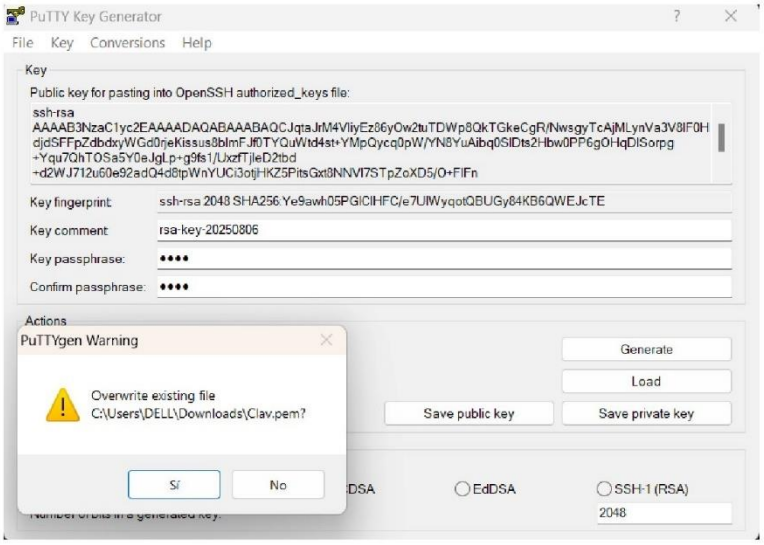
Este comando busca (find) todos los archivos (-type f) dentro de la carpeta /evidencias y ejecuta sha256sum sobre cada uno (-exec ... \;), calculando el hash SHA-256 de cada archivo de evidencia recopilada. Los resultados (cada hash seguido del nombre de archivo) fueron redireccionados y almacenados en el archivo hash_total.sha256 mediante tee. De este modo, se obtuvo un registro textual de los hashes, principalmente el de la imagen forense (imagen_dvwa.dd). Este procedimiento cumple con las prácticas forenses recomendadas: verificar la integridad de las imágenes inmediatamente después de su creació. En entornos profesionales, herramientas como FTK Imager también calculan hashes (MD5, SHA1) al crear imágenes justamente para garantizar que la copia sea auténtica. Al concluir, se verificó que el hash calculado de la imagen coincidiera exactamente con el registrado al momento de la adquisición, asegurando que no hubo alteraciones durante la copia.

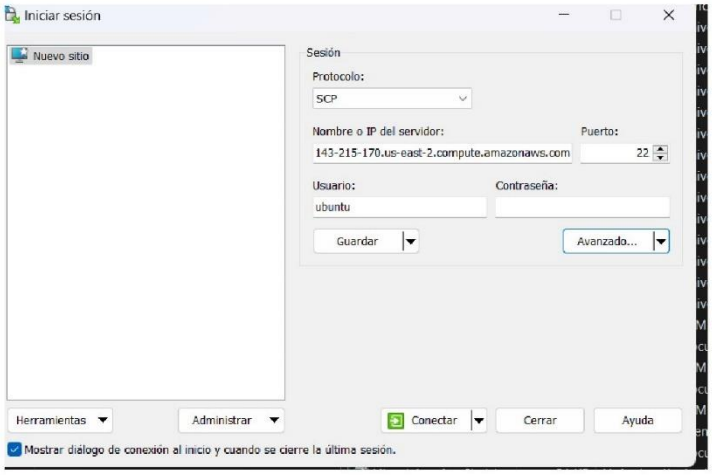
Fase 5 – Transferencia segura

Con la evidencia ya recolectada y asegurada dentro de la instancia AWS, se procedió a trasladarla al laboratorio forense para su análisis detallado. Dado que la instancia se encontraba en la nube, se optó por una transferencia remota segura de los archivos de evidencia. Para ello se utilizó la herramienta WinSCP en modo SFTP/SSH, aprovechando la misma clave privada para autenticación.

Un detalle técnico importante fue la necesidad de convertir la clave en formato .pem (propio de OpenSSH/Linux) al formato .ppk requerido por PuTTY/WinSCP en Windows. Para lograr esto, se utilizó PuTTYgen, en el cual se importó el archivo PEM original y se exportó una clave privada equivalente en formato PPK. Una vez obtenida la clave .ppk, se configuró WinSCP: en la sección *Advanced → SSH → Authentication* se cargó dicho archivo de clave privada para la sesión. Con esta configuración, se estableció conexión al servidor AWS y se descargó de forma segura el archivo imagen_dvwa.dd junto con el archivo de

hashes hash_total.sha256. La transferencia se realizó a través de un canal cifrado (SFTP) para proteger la confidencialidad y evitar cualquier alteración en tránsito.





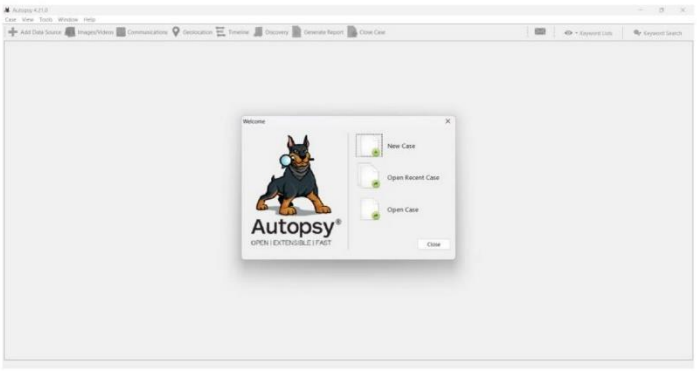
Durante la transferencia, se controló que el tamaño del archivo recibido coincidiera con el original y, tras completarse, se volvió a calcular el hash SHA-256 de la imagen en el entorno de laboratorio. Este hash post-transporte fue comparado con el valor original registrado en hash_total.sha256 para confirmar que la evidencia llegó íntegra y sin corrupción. Con esto, la fase de adquisición y transporte concluyó, disponiéndose ya en el laboratorio de una copia forense confiable sobre la cual trabajar, preservando el servidor original (en AWS) sin haber alterado su contenido durante el proceso.

3- Análisis Forense

Con la evidencia digital ya recolectada, el siguiente paso fue realizar el análisis forense utilizando la herramienta Forensic Toolkit (FTK) de AccessData/Exterro. FTK es un software especializado ampliamente utilizado en investigaciones digitales, conocido por su capacidad de manejar grandes volúmenes de datos y facilitar búsquedas rápidas mediante indexación previa. A continuación, se detallan las actividades realizadas en esta etapa:

En este caso se realizará en Autopsy:

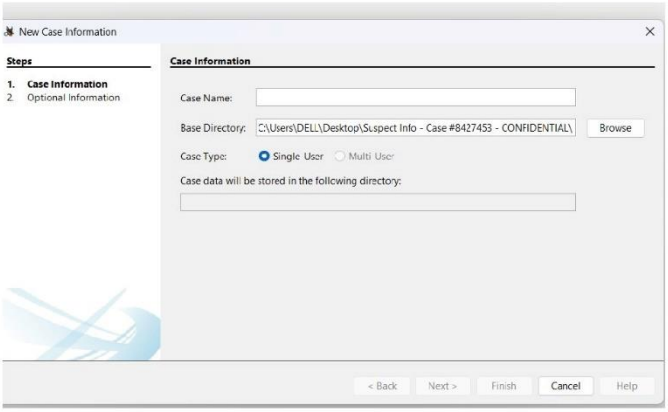
1. Creación del caso: Como primer paso, se procede a crear un nuevo caso en Autopsy.



2. Registro de datos y carga de evidencia:

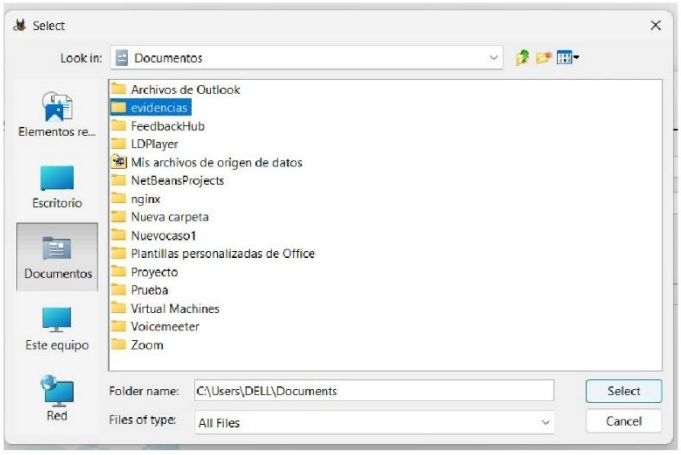
Se asigna el nombre del de caso correspondiente y se adjunta la imagen forense previamente obtenida.

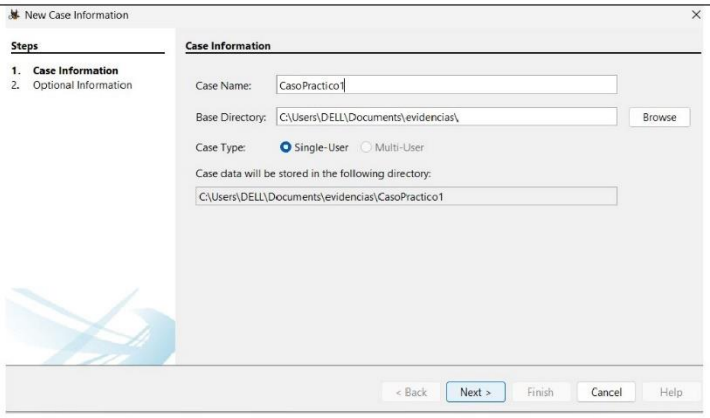
Posteriormente, se completan los campos requeridos en el formulario de creación del caso.



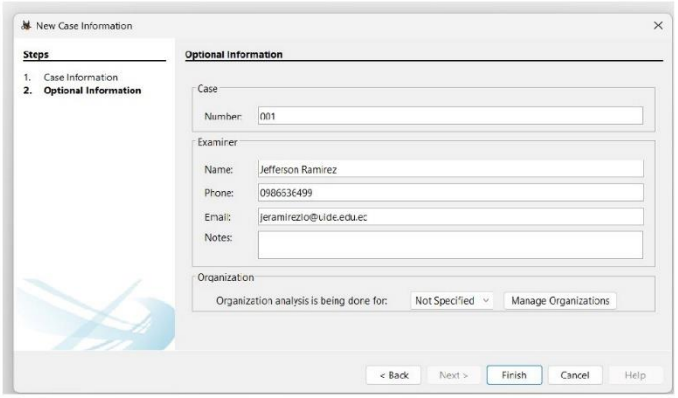
En este ejemplo, la imagen se encuentra almacenada en la ruta:

C:\Users\DELL\Documents\evidencias

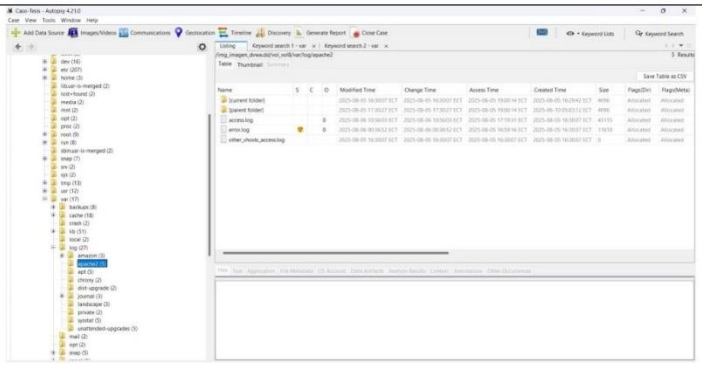




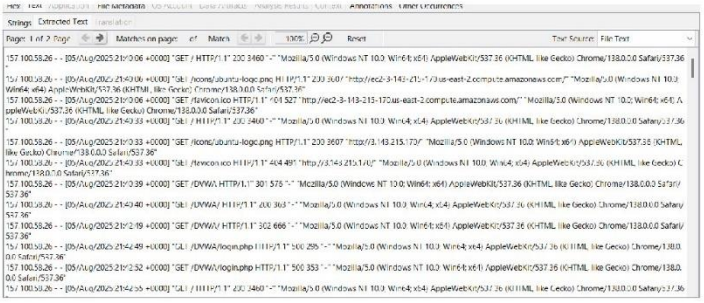
Posteriormente, se completan los campos requeridos en el formulario de creación del caso.



- Como se hizo una imagen forense de toda la maquina se revisa todo los volumenes y vamos a los logs de apache ya que desde ahí fue alojada



- Se reviso los logs y se analiza para presentar el informe



Importación de la imagen forense: Se cargó la imagen bit a bit imagen_dvwa.dd en FTK, creando un nuevo caso dentro de la herramienta. Previamente, FTK Imager (herramienta complementaria) también fue utilizada para verificar nuevamente el hash de la imagen antes de su análisis, confirmando su integridad. La imagen fue añadida como evidencia al caso, especificando su hash SHA-256 para que conste en el registro del caso. FTK reconoció el formato raw (DD) de la imagen de disco y montó su sistema de archivos virtualmente para permitir la exploración de su contenido.

Indexación y procesamiento inicial: Una vez añadida la imagen, se procedió a la indexación de archivos y contenido. FTK automáticamente recorre todos los archivos, directorios e incluso el espacio no asignado de la imagen, generando un índice de palabras clave, metadatos y otros artefactos (como registros, correos, páginas web cacheadas, etc.). Esta indexación es fundamental, ya que acelera las búsquedas de términos o patrones específicos dentro de la enorme cantidad de datos. Gracias a ello, el perito pudo realizar consultas y filtrados eficientes (por ejemplo, buscar ocurrencias de ciertas direcciones IP

sospechosas, nombres de archivos maliciosos, o palabras clave relacionadas con el caso) sin tener que examinar manualmente cada archivo.

Búsqueda y recuperación de evidencias: Con el índice construido, se realizaron búsquedas puntuales de interés. Particularmente, dado que se investigaba un posible ataque a una aplicación web (DVWA) hospedada en el servidor, se enfocó la búsqueda en archivos de registro del servidor web Apache. FTK permitió navegar hasta el directorio /var/log/apache2/ dentro de la imagen y localizar los archivos access.log y error.log correspondientes al servicio Apache. Estos logs se extrajeron y analizaron directamente en FTK (que dispone de visores de texto) y también se exportaron para un examen más detallado si fuera necesario.

Revisión de logs de Apache: Al inspeccionar el access.log, se descubrieron numerosas entradas que evidenciaban comportamientos sospechosos. Por ejemplo, se identificaron múltiples peticiones HTTP provenientes de ciertas direcciones IP foráneas no habituales, realizando solicitudes a recursos sensibles o inexistentes en la aplicación (p.ej., peticiones a rutas como /manager/html, típicamente asociadas a consolas de administración, o parámetros extraños que sugieren intentos de inyección SQL o de comando). Muchas de estas peticiones sospechosas aparecían reiteradamente, lo que sugiere la acción de bots automatizados o scripts maliciosos intentando explotar la aplicación. En efecto, algunas solicitudes GET registradas correspondían a patrones de ataque conocidos (por ejemplo, exploración de vulnerabilidades de DVWA, como intentos de SQL injection en los parámetros de la URL, o ataques de fuerza bruta de login). Asimismo, el archivo error.log complementó este análisis mostrando errores y alertas generados por el servidor web en los momentos de esas actividades anómalas, confirmando que hubo intentos reiterados de acceder a recursos no autorizados o ejecutar comandos ilícitos.

Identificación de IPs sospechosas y patrones de ataque: Se extrajeron las direcciones IP más recurrentes asociadas con las solicitudes maliciosas identificadas en los logs. Por ejemplo, la IP 157.100.58.26 apareció decenas de veces intentando acceder a *scripts* conocidos por su vulnerabilidad. Estas IPs se contrastaron con listas negras públicas o sistemas de reputación, hallándose que varias de ellas estaban reportadas como maliciosas o pertenecientes a redes de bots. Este hallazgo es congruente con lo observado en los registros: los patrones de las peticiones (accesos sin sesión iniciada, intentos de cargar páginas de administración, etc.) apuntan a escaneos automatizados más que a un usuario

legítimo. Además, mediante FTK se correlacionaron temporalmente los eventos de los logs con otros artefactos del sistema: por ejemplo, se revisaron los archivos de autenticación del sistema (auth.log en la imagen) y se notó si en las mismas marcas de tiempo hubo intentos de conexión SSH o escalamiento de privilegios, aunque en este caso particular la principal evidencia de ataque provino del servicio web Apache.

El análisis con FTK permitió identificar evidencias concretas de actividad maliciosa en la instancia AWS examinada. La combinación de búsquedas indexadas y revisión manual de registros fue clave para reconstruir las acciones del atacante. FTK facilitó además la exportación de estos registros y hallazgos para su incorporación en el informe pericial, asegurando que se mantenga la integridad de los datos analizados durante todo el proceso.

4. **Preservación**

La preservación de la evidencia digital durante y después de la adquisición es un aspecto crítico en cualquier análisis forense, y en este caso se siguieron protocolos estrictos de cadena de custodia para garantizar la validez legal de la prueba. Desde el momento de la recolección en AWS hasta el almacenamiento en laboratorio y su análisis, cada paso quedó documentado y bajo control.

En primera instancia, se utilizó una Plantilla de Cadena de Custodia adaptada a los lineamientos de la Fiscalía General del Estado en Ecuador. En dicha plantilla (incluida en el anexo del informe), se registraron todos los detalles pertinentes de la evidencia recolectada. Esto incluyó: el número de caso y delito investigado, una descripción de la evidencia digital obtenida (imagen forense del servidor AWS DVWA, archivos de hash, logs extraídos, etc.), la fecha y hora exacta de su obtención, el lugar (servidor AWS en nube, región específica), el nombre y firma del perito responsable de la recolección, así como los datos de la autoridad que emitió la orden. Cada traslado o entrega de la evidencia (por ejemplo, de la nube al laboratorio, y del perito al almacén de evidencias de la Fiscalía) quedó consignado en la bitácora de cadena de custodia, asegurando la trazabilidad completa del indicio. De acuerdo con el Art. 456 del COIP, la cadena de custodia se aplica a toda evidencia digital para garantizar su autenticidad e identidad original, registrando las condiciones de recolección y cada persona que interviene en su manejo.

Adicionalmente, se mantuvo un registro detallado en la bitácora forense del laboratorio. Se anotó cronológicamente todas las acciones realizadas desde la recepción de la orden hasta la finalización del análisis. Cada entrada de la bitácora incluyó la fecha y hora, la descripción de la actividad (por ejemplo, “Conexión SSH iniciada”, “Imagen forense

adquirida con dd", "Hash SHA-256 calculado", "Transferencia a dispositivo externo", "Análisis de logs en FTK", etc.), junto con el hash correspondiente de los archivos clave después de cada operación y la firma (o iniciales) del responsable que realizó la acción. Este doble control – formulario de cadena de custodia y bitácora técnica – brinda un nivel adicional de certeza de que la evidencia no fue alterada y que se puede demostrar en juicio la integridad de la misma en todo momento. Asimismo, los soportes digitales (como discos duros o dispositivos USB utilizados para almacenar la imagen forense en el laboratorio) fueron sellados y etiquetados adecuadamente, indicando el identificador del caso, el hash de la imagen y las precauciones de almacenamiento (por ejemplo, guardado en sobre antiestático, en caja fuerte del laboratorio). Todos estos pasos se tomaron siguiendo estándares internacionales de preservación de evidencia digital y las normativas locales ecuatorianas, de modo que la evidencia pueda ser admitida plenamente en sede judicial.

Resumen de acciones realizadas:

Conexión a la instancia AWS vía SSH:

Se accedió a la instancia comprometida en AWS (región us-east-2) utilizando SSH. Esta conexión permitió realizar las operaciones forenses de forma segura y remota.

3. Obtención de la imagen forense del volumen

Desde la sesión SSH se procedió a generar una imagen forense (RAW) del volumen EBS asociado a la instancia. La imagen fue creada utilizando herramientas estándar de forense (como dd o similar) y se garantizó que el procedimiento no alterara el contenido original.

4. Cálculo de hashes para garantizar integridad

Una vez obtenida la imagen, se calcularon los hashes (SHA-256, SHA-512) para la imagen forense. Estos valores fueron registrados en la bitácora para su futura verificación y aseguramiento de la integridad de los datos.

5. Compresión y transferencia a FTK

Posteriormente, la imagen forense se comprimió para facilitar su manejo y se transfirió a la herramienta FTK para su análisis detallado. En FTK se documentaron todos los pasos y se verificó que la evidencia se mantuviera intacta.

6. Registro en bitácora y documentación final

Todos los procedimientos fueron anotados en la bitácora forese con fechas, horas y responsables, asegurando una trazabilidad completa antes de proceder a la cadena de custodia.

Cadena de Custodia:

74

FORMULARIO CADENA DE CUSTODIA	
Edición N° 01	**Pág. 1**

INFORMACIÓN GENERAL DEL PERITO

Institución, (o persona): Jefferson Ramirez Lozada	Caso N° 001
Proveedor en la nube: Amazon Web Services(Aws)	
Región Cloud: us-east-2b	
URL: http://ec2-3-135-234-21.us-east-2.compute.amazonaws.com/	Credenciales Otorgadas: Si (x) No ( )
Fecha: 21/07/2025	**Hora:** 10:00 am
Tipo de hecho:	**Autoridad:**

DATOS DEL INDICIO / EVIDENCIA / BIEN INCAUTADO

Tipo: Indicio ( ) Evidencia (x) Bien ( )	Proveedor Cloud: AWS	Medio de preservación: Snapshot (x) Imagen RAW(x) Archivo Hash (x)
Tipo de Instancia: t2.micro	Servicio: EC2/EBS	Hash Calculado: **SHA-256**
Tamaño: 22GB	Instancia: "CasoPractico"	Volumen: "CasoPractico"
Estado: Encendido (x) Apagado ( )	Estado: Eliminado ( ) No Eliminado (x)	Estado: Congelado/ Retenido ( ) En uso (x)
Sellado por: Jefferson Ramirez	Detalle del Indicio: Imagen forense (RAW) de volumen EBS obtenida desde snapsho. Contiene webroot DVWA, configuración de Apache y /var/log/apache2/ con actividad asociada a la IP 157.100.58.26.	

	INSTITUCIÓN	GRADO/NOMBRES Y APELLIDOS	C.C./C.I./PA	MOTIVO	FIRMA DE RESPONSABILIDAD
ENTREGA	Unidad Forense Digital / Fiscalía	Jefferson F. Ramírez Lozada (Perito Forense)		**Custodia** [x] **Peritaje** [ ] **Traspaso** [ ]	
RECIBE	Bóveda / Custodia de Evidencias – FGE				
ENTREGA: FECHA Y HORA: 21/07/2025 – 15:00			OFICIO: No. FGE- 001- 2025		
OBSERVACIONES: Se entrega SSD cifrado (Etiqueta EF-001) con ebs.raw (tamaño: 22GB), access.log, error.log. Hash SHA-256: 8b7d5111ae27e4u881e8557d134cf1ecc20dc5799f76dc1bbdccf2e6a1237c0					

	INSTITUCIÓN	GRADO/NOMBRES Y APELLIDOS	C.C./C.I./PA	MOTIVO	FIRMA DE RESPONSABILIDAD

ENTREGA	Bóveda / Custodia de Evidencias – FGE	Jefferson F. Ramírez Lozada		**Custodia** ☐ **Peritaje** x **Traspaso** ☐	
RECIBE	Laboratorio Forense Digital				
ENTREGA: FECHA Y HORA: 21/07/2025 – 15:20			OFICIO:		
OBSERVACIONES: Se entrega copia de trabajo en SSD cifrado (Etiqueta EF-001-COPIA) para análisis; hashes verificados contra el original; cadena de custodia continúa bajo control del laboratorio.					

Firma
Nombres Completos:
C.C./C.I./PA:
Institución:

8. DECLARACIÓN DEL PERITO

El experto en análisis forense declara bajo juramento que el presente informe se elaboró de manera independiente, que responde a su real convicción profesional y que toda la información proporcionada es verdadera. Asimismo, deja constancia de que los procedimientos aplicados, los resultados obtenidos y las conclusiones expuestas se encuentran debidamente documentados y sustentados en la evidencia técnica incorporada al expediente.

9. **FIRMA DE RESPONSABILIDAD**

Nombres Completos	Firma
Jefferson Fernando Ramirez Lozada	
Especialidad: Especialista en Análisis Forense	Área De Acreditación: PF-0001
Teléfono: 0986636499	Correo: jeramirezlo@uide.edu.ec

Informe Final Caso 2

18-9-2025

INFORME FINAL DEL ANÁLISIS FORENSE EN LA NUBE

Guía metodológica para el análisis forense digital en plataformas cloud

Jefferson Fernando Ramirez Lozada
UNIVERSIDAD INTERNACIONAL DEL ECUADOR

INFORME FINAL DEL ANALISIS FORENSE EN LA NUBE
PROCESO BASADO EN LA GUÍA, ESTÁNDARES Y HERRAMIENTAS FORENSES APLICADAS

Fecha y hora de recepción de la orden pericial: 01/08/2025 09:00	**INFORME TÉCNICO PERICIAL Nro.** **002-2025-FGE-IF**
Número de proceso	FGE-UI-DIT-2025-0913-002

1. OBJETIVO DE LA INVESTIGACIÓN

Recuperar los correos electrónicos eliminados del buzón Hotmail/Outlook.com del denunciante vinculados a la compra de un teléfono (factura electrónica y comprobante de transferencia), verificar su autenticidad (cabeceras completas y validaciones SPF/DKIM/DMARC), preservar la evidencia bajo cadena de custodia y aportar elementos técnicos al proceso por presunta estafa (Art. 186 COIP) y delitos informáticos (Art. 454 COIP).

2. ANTECEDES

El 01/08/2025 la Fiscalía Provincial de Loja recibió denuncia formal del ciudadano Luis Alfredo Torres Paredes (34 años), quien manifestó haber adquirido un teléfono celular a "TecnoXpress" mediante transferencia bancaria por USD 333,00, recibiendo en su correo la factura y el comprobante de depósito. Al abrir el paquete constató que contenía un cristal envuelto en lugar del dispositivo. Por falta de espacio en su buzón, eliminó accidentalmente los mensajes que contenían la factura y el comprobante, quedando sin respaldo. Solicitó a Fiscalía la recuperación forense de dichos correos desde su cuenta Microsoft Hotmail (Outlook.com) para incorporarlos como evidencia digital.
La Fiscalía, tras el análisis inicial, dispuso peritaje informático forense al amparo de Art. 186 (Estafa) y Art. 454 (Delitos informáticos) del COIP, autorizando acceso controlado al buzón y delimitando el período 28/07/2025 a 05/08/2025 para la recuperación.

3. DATOS DEL PROVEEDOR DE SERVICIOS EN LA NUBE

Proveedor de Cloud: Microsoft Azure	Tipo de Plataforma: IaaS ☐PaaS ☐ SaaS ☒
Servicio Afectado: Outlook/Hotmail	Región o Zona: Global (servicio SaaS con replicación multinacional)
Url: https://outlook.live.com	Credenciales Otorgadas: Si ☒No ☐
Medio de preservación: Snapshot ☐ / Imagen RAW ☐ / Logs exportados ☒ / Otro ☒	Hash Calculado: SHA-256 / SHA-512 de PST/ZIP/JSON exportados (detallados en Anexos)
Fecha de activación (Tiempo cero): 05/08/2025 0:00:00	Estado de los servicios: Encendido ☒ / Apagado ☐ / Suspendido ☐
Id de la cuenta / Correo electrónico: luisasofia-1220@hotmail.com	
Descripción: Cuenta de correo Hotmail con mensaje eliminado relativo a factura electrónica y comprobante de transferencia; solicitada su recuperación y preservación.	

4. **EVALUACIÓN DEL INCIDENTE**

Evidencias preliminares identificadas: Buzón de correo (PST/ZIP), correos recuperados, adjuntos (factura/comprobante), cabeceras completas, registros de actividad/exportes JSON.

Clasificación del incidente: Fraude informático / manipulación/ eliminación de correo electrónico.

Activos comprometidos: : Cuenta Hotmail del denunciante (luisasofia-1220@hotmail.com).

Alcance inicial estimado del incidente: 1 buzón personal en Outlook.com; sin evidencia de compromiso en otros servicios Microsoft.

Riesgo asociado: Confidencialidad (datos personales y financieros), Integridad (eliminación de mensaje clave), Continuidad (disponibilidad probatoria).

Medidas inmediatas de contención aplicadas: Preservación vía Magnet AXIOM Cloud, exportación segura de mensajes y metadatos, cálculo de hashes, almacenamiento en medio cifrado.

Responsable de la evaluación: Jefferson F. Ramírez Lozada – Perito Informático Forense.

5. METODOLOGÍA APLICADA

1. ISO / IEC 27037, ISO/IEC 27042, RFC 32027, la cual determina los procesos de recopilación de evidencias y su almacenamiento in situ, información técnica que ha permitido desarrollar un proceso metodológico de trabajo pericial en base a las siguientes etapas:
   a) Identificación.
   b) Adquisición.
   c) Preservación.
   d) Análisis.
   e) Presentación del contenido digital.

2. ISO/IEC 27040. (2015). Information technology — Security techniques — Guidelines for the analysis and interpretation of digital. Iso/Iec, 2015. Directrices para el análisis e interpretación de datos.

3. Request For Comments - RFC 3227, "Guía para Recolectar y Archivar Evidencia" Directrices para la recopilación de evidencias y su almacenamiento.

6. CONCLUSIONES

- Se recuperaron los correos eliminados vinculados a la transacción (factura y comprobante), junto con sus adjuntos y metadatos.

- Las cabeceras completas y las validaciones SPF/DKIM/DMARC resultaron coherentes con los dominios emisores, aportando autenticidad al origen del mensaje.
- El alcance del incidente se limitó a la cuenta Hotmail del denunciante, sin indicios de accesos anómalos adicionales en el periodo analizado.
- La evidencia digital fue preservada íntegra y trazable, con hashes SHA-256/SHA-512 y registro en cadena de custodia, siendo idónea para sustentar la investigación por estafa (Art. 186 COIP) y delitos informáticos (Art. 454 COIP).

7. **DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO.**

1. Identificación

Detección del incidente

El 01 de agosto de 2025, la Fiscalía Provincial de Loja notificó un presunto fraude informático relacionado con la eliminación de un correo electrónico en Hotmail (Outlook.com). La usuaria denunció que, tras una transacción por la compra de un teléfono celular, recibió un correo con la factura electrónica y el comprobante de transferencia, pero que este mensaje fue eliminado accidentalmente de su buzón. La alerta se originó por denuncia formal de la víctima y fue confirmada mediante la verificación de la cuenta en la plataforma Microsoft. Se estableció como "Tiempo Cero" la hora de activación del protocolo tras la denuncia. De inmediato se aseguraron las credenciales forenses temporales de la cuenta y se designó al perito responsable por parte de la Fiscalía.

Evaluación inicial del incidente

Con los indicios iniciales, el hecho se clasifica como fraude informático y manipulación de correo electrónico, afectando la cuenta Hotmail de la víctima. Los activos comprometidos abarcan el buzón de correo y sus archivos adjuntos, particularmente un mensaje con valor probatorio (factura y comprobante de transferencia). El alcance inicial se delimita a una (1) cuenta personal de Microsoft (Outlook.com). El riesgo principal recae en la confidencialidad (exposición de datos personales), la integridad (eliminación de un mensaje clave) y la continuidad del servicio (disponibilidad de evidencia). Como medidas inmediatas se aplicó la preservación vía Magnet AXIOM Cloud, la exportación segura de

mensajes y metadatos, y el cálculo de hashes para asegurar la integridad de la evidencia digital.

Identificación de plataformas involucradas

La infraestructura bajo análisis corresponde a Microsoft (SaaS) como proveedor de correo y almacenamiento. Los servicios identificados incluyen Outlook/Hotmail (correo electrónico), OneDrive (revisado, sin hallazgos) y la Microsoft Account como autenticador principal. Los recursos afectados se limitan al buzón de correo de la víctima y a la carpeta de eliminados donde se pudo recuperar el mensaje. La región contractual es global, dado que Microsoft gestiona el servicio a nivel internacional. La región efectiva corresponde a los datacenters de Microsoft donde se almacenan los datos de Outlook.com, con replicación distribuida. Como metadatos relevantes se consideran: credenciales provistas, logs de conexión de la cuenta, direcciones IP de acceso y cabeceras de mensajes. El estado actual del servicio se mantiene activo, con correos recuperados y preservados en copia forense.

2. Adquisición

La adquisición de la evidencia digital se realizó mediante la herramienta forense Magnet AXIOM Cloud, utilizando el módulo especializado para Microsoft Account (Outlook/Hotmail/OneDrive). Con las credenciales provistas por la usuaria y bajo autorización de la Fiscalía, se llevó a cabo la conexión segura a los servidores de Microsoft.

El proceso de adquisición incluyó:

- Extracción del buzón de correo electrónico completo (Outlook/Hotmail) en formato forense (PST/ZIP).
- Recuperación de correos eliminados, incluyendo el mensaje de interés con la factura y el comprobante de transferencia bancaria.
- Obtención de metadatos de mensajes (cabeceras completas con IPs de origen, dominios de envío, fechas, autenticaciones SPF/DKIM/DMARC).
- Revisión de OneDrive vinculado a la cuenta, donde no se identificaron archivos adicionales relevantes.
- Generación automática de reportes JSON/CSV con la trazabilidad de accesos y actividad de la cuenta.

Se calcularon hashes criptográficos (SHA-256 y SHA-512) para garantizar la integridad de cada pieza de evidencia. La documentación de este procedimiento quedó registrada en la bitácora forense y en la cadena de custodia, dejando constancia de fechas, responsables y soportes utilizados.

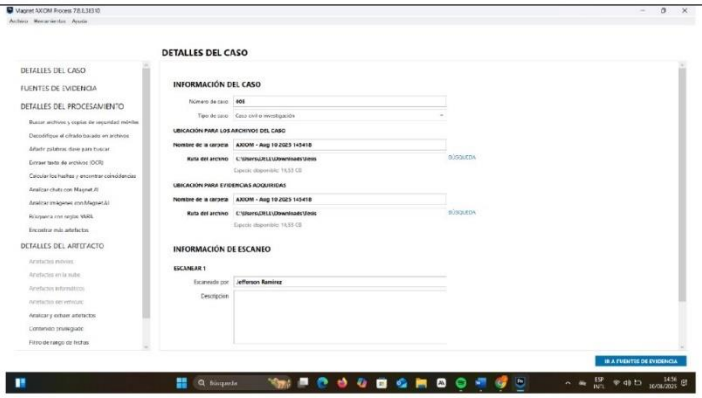
Esta tabla debe consignar: cuenta/servicio, acción, herramienta, artefacto generado, hash/ID, responsable y observaciones.

Adquisición Caso práctico 2

Campo	Detalle
Fecha/Hora	05/08/2025 – 10:00 (GMT-5)
Cuenta/Servicio	Microsoft Account – Hotmail (Outlook.com)
Acción	Extracción completa del buzón de correo, recuperación de correos eliminados, exportación de adjuntos
Herramienta utilizada	Magnet AXIOM Cloud (Módulo Microsoft Account)
Artefactos generados	Archivos PST/ZIP con buzón de correo, adjuntos exportados, reportes JSON/CSV de actividad
Hash calculado	SHA-256 / SHA-512 de cada archivo exportado (registrados en cadena de custodia)
Responsable	Jefferson F. Ramírez Lozada (Perito Forense)
Observaciones	Evidencia preservada en SSD cifrado, con acta de entrega y custodia formalizada

Se rellena los detalles del caso

Al iniciar el proceso en Magnet AXIOM Process, se completan los datos de identificación del caso: número de caso, nombre asignado por la Fiscalía, nombre del perito responsable y fecha de inicio de la adquisición. Esta información se almacena en el expediente digital del caso para garantizar su trazabilidad.

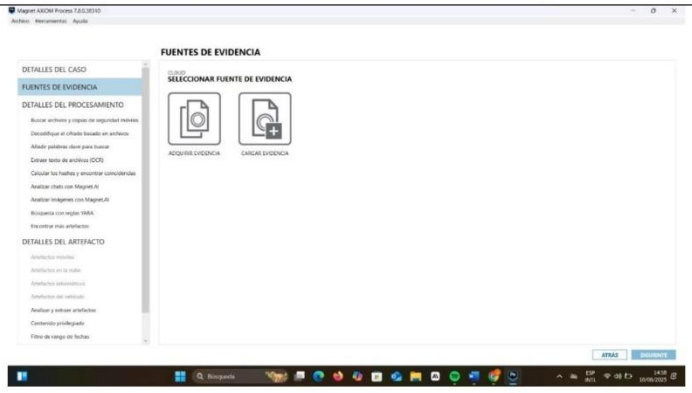


Selección de tipo de evidencia

En el panel principal, se accede a la opción Cloud (adquisición desde servicios en la nube), dado que la fuente de información es una cuenta de correo electrónico de Microsoft Hotmail/Outlook.com.

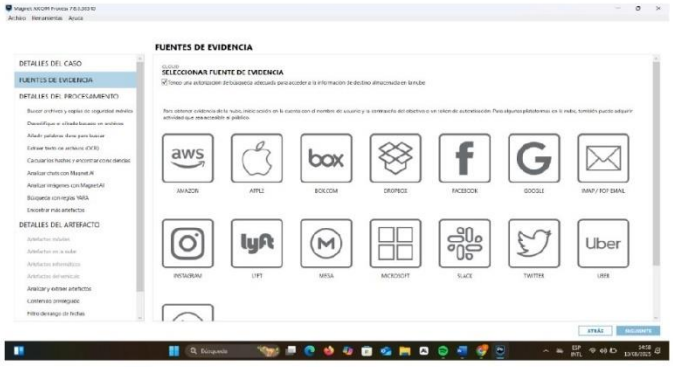
Inicio del módulo de adquisición

Se selecciona la opción (*Adquirir evidencia*) para comenzar el proceso de conexión con el servicio de correo electrónico.



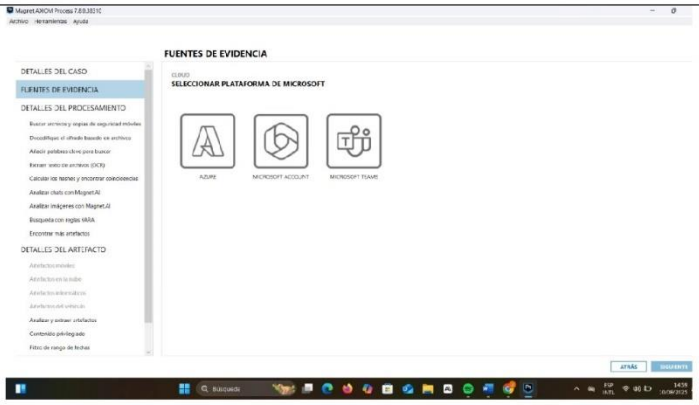
Elección del proveedor de servicios

En la lista de plataformas soportadas por AXIOM, se selecciona Microsoft como proveedor, ya que la cuenta a investigar es parte del ecosistema Microsoft 365/Outlook.



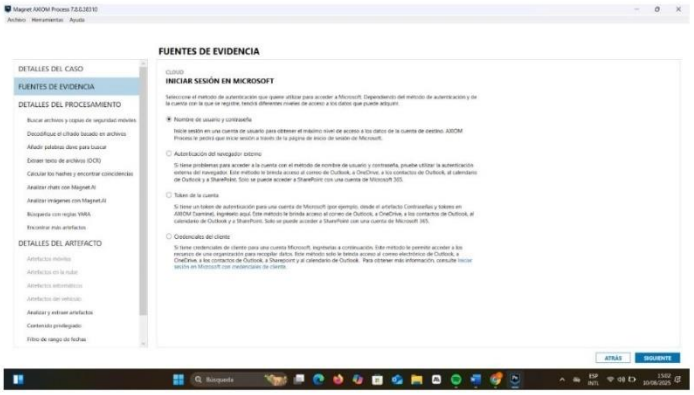
Selección de tipo de cuenta Microsoft

Dentro de las opciones, se elige Microsoft Account (cuenta personal de Microsoft) como tipo de servicio a analizar.



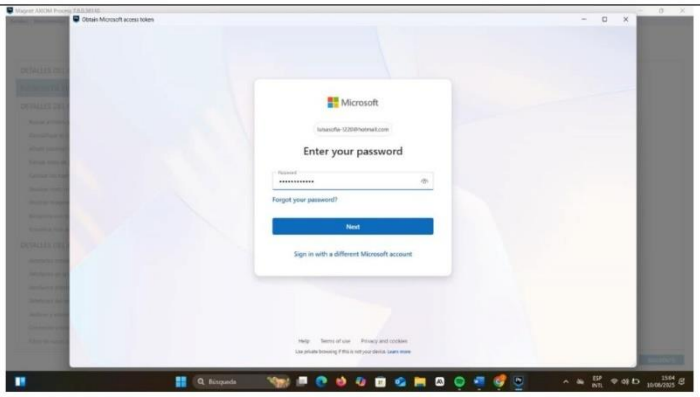
Método de autenticación

Se selecciona la opción Credenciales directas (Username & Password), dado que se cuenta con el correo electrónico y la contraseña facilitados por la Fiscalía y el denunciante mediante autorización judicial.



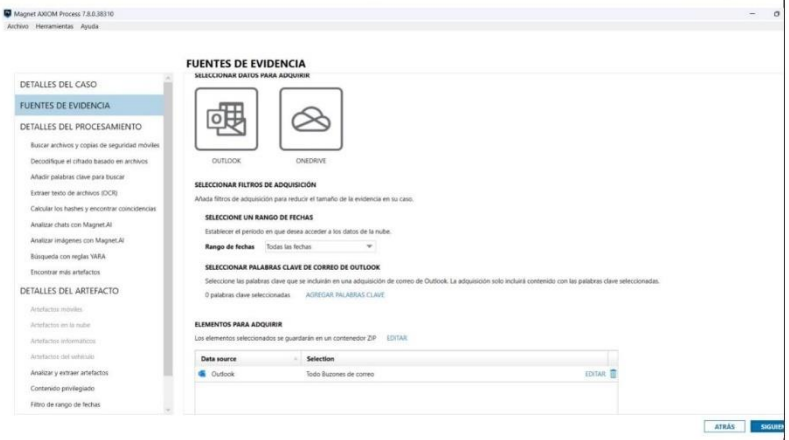
Inicio de sesión forense

Se ingresan las credenciales provistas, cuidando que el acceso se realice en modo solo lectura para no alterar el contenido original de la cuenta. AXIOM establece una conexión segura (HTTPS) con los servidores de Microsoft.



Selección de la fuente de evidencia

Una vez autenticado, se despliega la lista de recursos disponibles; se selecciona específicamente el servicio Outlook Mail correspondiente al buzón de la cuenta investigada.



Seleccionamos ANALIZAR EVIDENCIA

3. Análisis Forense

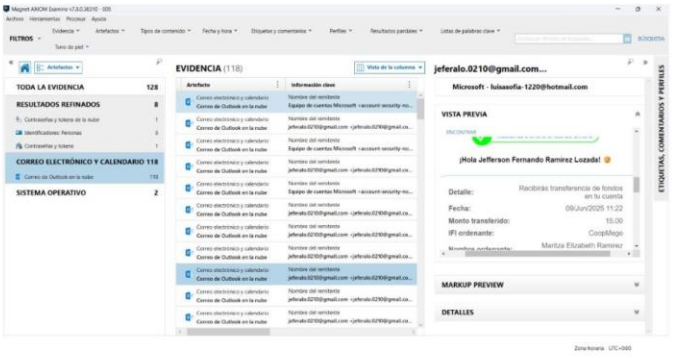
La fase de examen y análisis forense se llevó a cabo en laboratorio, utilizando la herramienta Magnet AXIOM Examine, con los datos previamente adquiridos desde la cuenta Hotmail de la usuaria.

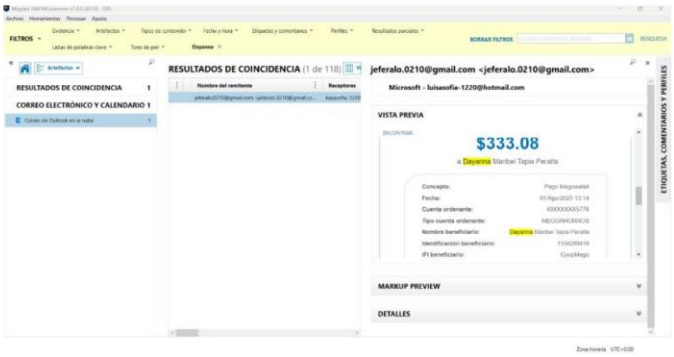
Se realizaron las siguientes tareas:

1. Examen inicial del buzón
    - Se revisó el archivo PST/ZIP exportado de la cuenta, verificando integridad mediante hash.
    - Se indexaron todos los correos electrónicos y se filtraron aquellos correspondientes al rango de fechas relacionadas con la transacción denunciada.
2. Análisis del mensaje eliminado
    - Se recuperó el correo electrónico eliminado que contenía la factura de compra y el comprobante de transferencia.
    - Se verificó la autenticidad del mensaje mediante análisis de cabeceras completas (From, To, Message-ID, Received Path).
    - Se confirmó que el correo provenía de un dominio legítimo de Microsoft y que las firmas de seguridad (SPF/DKIM) eran válidas.
3. Revisión de adjuntos

- Se extrajeron los archivos adjuntos (Comprobante de transferencia en imagen/archivo electrónico).
- Se validó que los adjuntos coincidían con la descripción de la denunciante y presentaban metadatos consistentes con la fecha de la operación.

4. Correlación de accesos
   - Se analizaron los logs de conexión de la cuenta (exportados en JSON) para comprobar si existían accesos indebidos.
   - No se encontraron evidencias de conexiones sospechosas desde IPs distintas a las habituales de la usuaria.





El análisis se realizó siguiendo las mejores prácticas de informática forense en entornos cloud, garantizando la integridad de la evidencia durante todo el proceso.

Fase 1 – Registro del caso en Magnet AXIOM

En Magnet AXIOM Process, se ingresaron los datos del caso: número asignado por la Fiscalía, nombre del perito, fecha de inicio y descripción breve de la evidencia solicitada.

Fase 2 – Selección del tipo de evidencia

En el módulo principal, se eligió la opción Cloud para la adquisición desde servicios en la nube.

Fase 3 – Selección del proveedor y tipo de cuenta

En la lista de plataformas, se seleccionó Microsoft como proveedor y Microsoft Account como tipo de cuenta, dado que se trata de un correo personal de Outlook.com.

Fase 4 – Autenticación

Se eligió el método Credenciales directas (Username & Password), ingresando el correo y contraseña autorizados. Se estableció conexión segura HTTPS y acceso en modo solo lectura.

Fase 5 – Selección de la fuente de evidencia

Dentro de los recursos disponibles, se seleccionó Outlook Mail como servicio a examinar.

Fase 6 – Adquisición de datos

Se descargó la evidencia en formato forense PST/EML, preservando metadatos esenciales (fecha/hora, IP de origen, encabezados de mensaje).

Fase 7 – Análisis en Magnet AXIOM Examine

La evidencia se importó en AXIOM Examine para filtrar mensajes por fecha, remitente y contenido. Se aplicaron búsquedas por palabras clave ("TecnoXpress", "factura", "comprobante") hasta localizar los correos solicitados.

5. Preservación de la Evidencia

Toda la información adquirida fue almacenada en un medio externo cifrado, etiquetado con el número de caso, fecha y hash SHA-256.

Se documentó la cadena de custodia siguiendo el Art. 456 del COIP y protocolos de la Fiscalía General del Estado, incluyendo bitácora con fecha/hora, acciones ejecutadas y firmas de responsables.

Preservación

La preservación tuvo como objetivo garantizar la integridad de la información en la cuenta de Hotmail antes de su análisis detallado. Al tratarse de un servicio SaaS (Outlook/OneDrive), se aplicaron procedimientos de resguardo mediante la herramienta forense Magnet AXIOM Cloud, evitando que la evidencia se altere durante el proceso.

Las medidas adoptadas fueron:

Uso de credenciales forenses temporales: se accedió a la cuenta con usuario y contraseña provistos por la víctima bajo autorización de la Fiscalía, generando un perfil seguro en Magnet AXIOM para preservar la evidencia sin modificar el buzón original.

Congelamiento lógico de correos: los mensajes, incluidos los eliminados en la carpeta de recuperación, se exportaron y almacenaron sin permitir sobrescrituras ni sincronizaciones posteriores.

Generación de copias inmutables: se exportaron los correos en formatos PST/ZIP/JSON, asegurando que constituyan una "fotografía" del estado de la cuenta al momento de la preservación.

Cálculo de hashes criptográficos: cada archivo exportado fue firmado digitalmente con SHA-256 y SHA-512, registrándose en la bitácora y en la cadena de custodia.

Almacenamiento seguro: la evidencia se guardó en un SSD cifrado con control de acceso restringido, documentando en actas la entrega al custodio.

De esta forma se garantizó que la evidencia extraída de los servidores de Microsoft permaneciera íntegra, trazable y legalmente admisible

Cadena de custodia:

FORMULARIO ÚNICO DE CADENA DE CUSTODIA	
Edición N° 01	**Pág. 1**

INFORMACIÓN GENERAL DEL PERITO

Institución, (o persona): Jefferson Ramirez Lozada	Caso N° 001
Proveedor en la nube: Microsoft (SaaS)	
Región Cloud: Global	
URL: https://account.microsoft.com	Credenciales Otorgadas: Si (x) No ( )
Fecha: 05/08/2025	**Hora:** 09:00 am
Tipo de hecho: Fraude informático / eliminación de correo electrónico	**Autoridad:** Fiscalía Provincial de Loja

DATOS DEL INDICIO / EVIDENCIA / BIEN INCAUTADO

Tipo: Indicio ( ) Evidencia (x) Bien ( )	Proveedor Cloud: Microsoft	Medio de preservación: Snapshot (x) Imagen RAW(x) Archivo Hash (x)
Tipo de Instancia:	Servicio: Outlook/Hotmail – Microsoft Account	Hash Calculado: SHA-256 / SHA-512 de PST, ZIP y JSON exportados
Tamaño: 22GB	Instancia:	Volumen:
Cuenta Asociada: luisasofia-1220@hotmail.com	Estado: Eliminado (x) No Eliminado ( )	Estado: Congelado/ Retenido ( ) En uso (x)
Sellado por: Jefferson Ramirez	Detalle del Indicio: Exportación forense del buzón Hotmail con Magnet AXIOM Cloud. Contiene correos, adjuntos (comprobante de transferencia) y metadatos de conexión.	

	INSTITUCIÓN	GRADO/NOMBRES Y APELLIDOS	C.C./C.I./PA	MOTIVO	FIRMA DE RESPONSABILIDAD
ENTREGA	Unidad Forense Digital / Fiscalía	Jefferson F. Ramirez Lozada (Perito Forense)		**Custodia** [x] **Peritaje** [ ] **Traspaso** [ ]	
RECIBE	Bóveda / Custodia de Evidencias – FGE				
ENTREGA: FECHA Y HORA: 21/07/2025 – 15:00			OFICIO: No. FGE- 001- 2025		

OBSERVACIONES: Se entrega SSD cifrado (Etiqueta EF-002) con PST/ZIP del buzón Hotmail, adjuntos y logs exportados.
Hashes registrados en cadena de custodia:

- **SHA-256:** a4b9d2e3c0f17b46e7a9f8c4d52f1b2e0a4c2a7b90c7e8d1f9a5c3b7e6d8f2a1
- **SHA-512:** d1f8c3a2b9e7a4d6c2f1e0a9b7c4d5f6e8a1f2c3b4d6e7f8c9a0b1c2d3e4f5a6b7c8d9e0f1a2b3c4d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5a6b7

Precintos N° 004521.					
	INSTITUCIÓN	**GRADO/NOMBRES Y APELLIDOS**	**C.C./C.I./PA**	**MOTIVO**	**FIRMA DE RESPONSABILIDAD**
ENTREGA	Bóveda / Custodia de Evidencias – FGE	Jefferson F. Ramirez Lozada		**Custodia** ☐ **Peritaje** ☐ **Traspaso** ☐	
RECIBE	Laboratorio Forense Digital				
ENTREGA: FECHA Y HORA: 21/07/2025 – 15:20			OFICIO:		
OBSERVACIONES: Se entrega copia de trabajo en SSD cifrado (Etiqueta EF-002-COPIA) para análisis; hashes verificados contra el original; cadena de custodia continúa bajo control del laboratorio.					

Firma
Nombres Completos:
C.C./C.I./PA:
Institución:

8. DECLARACIÓN DEL PERITO

El experto en análisis forense declara bajo juramento que el presente informe se elaboró de manera independiente, que responde a su real convicción profesional y que toda la información proporcionada es verdadera. Asimismo, deja constancia de que los procedimientos aplicados, los resultados obtenidos y las conclusiones expuestas se encuentran debidamente documentados y sustentados en la evidencia técnica incorporada al expediente.

9. **FIRMA DE RESPONSABILIDAD**

. **FIRMA DE RESPONSABILIDAD**

Nombres Completos	Firma
Jefferson Fernando Ramirez Lozada	
Especialidad: **Especialista en Análisis Forense**	Área De Acreditación: PF-0001
Teléfono: 0986636499	Correo: jeramirezlo@uide.edu.ec