UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Gestión de evidencias electrónicas. Aplicación de los documentos normativos españoles

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Vidagany Viel, Gema

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2023/2024

RESUMEN

Este trabajo se centra en abordar la falta de una guía integral que cubra el proceso completo de gestión de evidencias electrónicas de manera coherente y unificada. Actualmente, las pautas y procedimientos se encuentran dispersos entre diferentes normas y estándares, lo que genera dificultades para los profesionales que participan en auditorías, investigaciones forenses o procesos legales que dependen de las evidencias digitales. La fragmentación de estas directrices complica la verificación del cumplimiento normativo y la correcta gestión de dichas evidencias, especialmente en lo que respecta a su captación, análisis y preservación.

Para resolver este problema, la metodología del trabajo se basa en un estudio exhaustivo del marco normativo y legal español, con un enfoque particular en las normas UNE aplicables a las evidencias electrónicas. Este análisis busca sintetizar y estructurar las diferentes normativas para ofrecer una guía clara y práctica. El objetivo es proporcionar un recurso útil que sirva como apoyo a los profesionales, permitiéndoles verificar el cumplimiento de las normas y garantizar que las evidencias digitales sean manejadas de acuerdo con los estándares establecidos. La guía cubrirá específicamente las fases de captación, análisis y preservación de evidencias, ayudando a asegurar que los procesos seguidos en investigaciones y auditorías sean correctos y que los resultados obtenidos sean válidos y admisibles en cualquier procedimiento judicial o pericial.

Palabras clave: evidencia electrónica, evidencia digital, normativa, captación, análisis, preservación, cadena de custodia, guía.

RESUM

Aquest treball se centra a abordar la falta d'una guia integral que tracte la gestió d'evidències electròniques de manera coherent i unificada. Actualment, les pautes i procediments es troben dispersos entre diferents normes i estàndards, cosa que genera dificultats per als professionals que participen en auditories, investigacions forenses o processos legals que depenen de l'evidència digital. La fragmentació d'aquestes directrius complica la verificació del compliment normatiu i la correcta gestió d'aquestes l'evidències, especialment pel que fa a la seua captació, anàlisi i preservació.

Per a resoldre aquest problema, la metodologia del treball es basa en un estudi exhaustiu del marc normatiu i legal espanyol, amb un enfocament particular en les normes UNE aplicables a les evidències electròniques. Aquesta anàlisi busca sintetitzar i estructurar les diferents normatives per a oferir una guia clara i pràctica. L'objectiu és proporcionar un recurs útil que servisca de suport als professionals, permetent-los verificar el compliment de les normes i garantir que les evidències digitals siguen gestionades d'acord amb els estàndards establerts. La guia cobrirà específicament les fases de captació, anàlisi i preservació d'evidències, ajudant a assegurar que els processos seguits en investigacions i auditories siguen correctes i que els resultats obtinguts siguen vàlids i admissibles en qualsevol procediment judicial o pericial.

Paraules clau: evidència electrònica, evidència digital, normativa, captació, anàlisi, preservació, cadena de custòdia, guia.

ABSTRACT

This work focuses on addressing the lack of a comprehensive guide that deals with the management of electronic evidence in a coherent and unified manner. Currently, the guidelines and procedures are scattered across different standards, which creates challenges for professionals involved in audits, forensic investigations, or legal proceedings that rely on digital evidence. The fragmentation of these directives complicates the verification of regulatory compliance and the proper handling of said evidence, particularly in relation to its collection, analysis, and preservation.

To solve this problem, the methodology of this work is based on an exhaustive study of the Spanish legal and regulatory framework, with a particular focus on the UNE standards applicable to electronic evidence. This analysis seeks to synthesize and structure the various regulations in order to offer a clear and practical guide. The aim is to provide a useful resource that supports professionals by allowing them to verify compliance with standards and ensure that digital evidence is handled in accordance with established protocols. The guide will specifically cover the phases of collection, analysis, and preservation of evidence, helping to ensure that the processes followed in investigations and audits are correct and that the results obtained are valid and admissible in any judicial or forensic proceeding.

Keywords : electronic evidence, digital evidence, regulations, acquisition, analysis, preservation, custody chain, guidelines.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

A medida que el mundo se digitaliza, la habilidad para gestionar las evidencias electrónicas se vuelve esencial para mantener la confianza y la transparencia en múltiples contextos. A lo largo de las últimas décadas, los dispositivos electrónicos han adquirido mayor relevancia en nuestra vida cotidiana, facilitando y haciendo más cómodas nuestras actividades diarias. Este creciente protagonismo, viene ligado a la creación de información digital, la cual podemos considerar en algunos casos como evidencia electrónica. Estas evidencias pueden usarse tanto en procedimientos judiciales como en el día a día de cualquier empresa, por lo que se debe saber cómo gestionarlas.

Pero ¿qué es realmente una evidencia? Según la Real Academia Española (RAE) una evidencia se define como la «certeza clara y manifiesta de la que no se puede dudar» o bien, como la «prueba determinante en un proceso». En el caso de las evidencias electrónicas ambas definiciones podrían resultar válidas, ya que una evidencia es cualquier dato o información que puede servir para confirmar o negar el acaecimiento de un hecho. Estas son recogidas en la escena de interés y son susceptibles de ser analizadas con una metodología forense.

Si esta definición la aplicamos al mundo digital, podemos entender una evidencia electrónica como: información o datos, guardados o transmitidos de forma binaria en la que nos podemos apoyar como evidencia. Es decir, cualquier información en forma electrónica que sea identificable y susceptible de ser tratada de forma diferenciada. Para que sea relevante en la investigación, esta ha de pasar por un proceso de análisis, además de ser generada, tratada y almacenada de tal forma que se asegure su valor probatorio, es decir, su integridad y confiabilidad.

1.1. Motivación

A pesar del crecimiento del campo de la informática forense, la conciencia sobre la necesidad de la existencia de sistemas de gestión de evidencias electrónicas está aún en una fase incipiente. Existen muchos aspectos técnicos y metodológicos relacionados con la recolección, preservación y análisis de las e-evidencias que no están plenamente comprendidos o estandarizados. Aunque sí que es verdad que existen diversos estándares, ya sean nacionales o internacionales que tratan esta materia, las pautas suele estar dispersas entre ellos y, a su vez, suelen ser bastante generales. Esta falta de centralización de la información necesaria y su poca precisión, representa un desafío significativo para los profesionales, quienes necesitan herramientas y directrices claras para realizar su trabajo de manera efectiva.

El desarrollo de una guía integral es esencial para comenzar a abordar estas deficiencias. Una guía que compile y resuma las mejores prácticas, procedimientos y principios para la gestión de evidencias electrónicas proporcionaría una base sólida para los profesionales del campo. Este tipo de recurso no solo ayudaría a estandarizar las prácticas en la industria, sino que también facilitaría la capacitación de nuevos profesionales al ofrecerles una referencia clara y accesible. Aún más cuanto tenemos en cuenta que las evidencias electrónicas conforman un papel crucial en la resolución de casos y la investigación de delitos cibernéticos. Sin embargo, el conocimiento sobre su manejo sigue siendo limitado. En el mercado laboral actual, la importancia de estas evidencias

NOTA: En el Anexo B se puede encontrar un glosario conformado de las abreviaciones encontradas a lo largo del trabajo y de las definiciones de las palabras técnicas utilizadas para una mejor compresión por parte del lector.

a menudo no recibe la atención que merece, lo que subraya la necesidad de una guía comprensible y accesible que pueda servir como referencia para los profesionales del sector.

En cuanto a mi motivación personal para abordar el tema de la gestión de las evidencias electrónicas, esta surge de un profundo interés en el área de la gestión informática. Sin embargo, la gestión de evidencias electrónicas es un aspecto que aún no he explorado en profundidad, y que, sorprendentemente, he advertido que también es poco conocido entre mis compañeros de grado. Este vacío en nuestro conocimiento colectivo me impulsa a investigar y profundizar en un área que es crucial y a menudo subestimada. La oportunidad de explorar y entender un tema tan especializado y relevante, que ofrece tanto desafíos como oportunidades, no solo me motiva en mi búsqueda para adquirir nuevas habilidades, sino también a contribuir con mi estudio en un área que está en constante evolución.

1.2. Objetivos

El objetivo principal de este trabajo crear una guía clara y concisa que sirva de apoyo para los profesionales de la informática forense, peritos y auditores en cuanto a la gestión de evidencias electrónicas. Esta guía abarcará las diferentes fases del proceso de gestión de evidencias electrónicas, centrándose en las etapas de identificación, captación, análisis, preservación y presentación. Además se podrá utilizar para verificar que estos procesos han sido realizados correctamente y conforme a la normativa española vigente en el momento de redacción de este trabajo. Por lo que se debe estudiar dicha normativa para asegurarse de que los pasos a seguir están alineados con ella.

La guía debe proporcionar un esquema detallado que facilite a los profesionales de la informática forense la gestión adecuada de las evidencias digitales, asegurando que el contenido sea accesible y práctico, para que los usuarios puedan seguir los procedimientos sin ambigüedades. Que estos procesos sean realizados correctamente es necesario para mantener y garantizar la integridad y confiabilidad de las evidencias digitales o e-evidencias.

Por último, esta guía busca ayudar a dar respuesta a los problemas causados por incidentes informáticos o infracciones legales en diversas empresas y organizaciones, ya que la captación de evidencias digitales fiables y robustas contribuye a determinar correctamente los hechos, permitiendo discernir si su causa es intencionada o negligente. Con esta información, se puede identificar adecuadamente los instrumentos usados, las acciones realizadas, los fines de los actores y otros parámetros relacionados con dichas conductas problemáticas.

1.3. Impacto esperado

La creación de una guía para la gestión de evidencias electrónicas traerá consigo numerosas ventajas y mejoras en los procesos que se llevan a cabo en este ámbito. En primer lugar, ofrecerá un marco claro y estructurado para la captación, análisis y preservación de evidencias digitales, asegurando que todos los profesionales involucrados sigan un procedimiento uniforme y

estandarizado. Esto no solo reducirá los errores, sino que también incrementará la eficiencia y la precisión en la manipulación de datos sensibles, elementos clave en investigaciones forenses.

Para los peritos, auditores y empleados responsables de estas labores, la guía será una herramienta invaluable. Permitirá que realicen su trabajo de forma más sencilla, asegurando que cada paso del proceso esté bien documentado y sea verificable, reduciendo la posibilidad de que algún detalle se pase por alto. Al seguir una metodología establecida, estos profesionales podrán estar seguros de que cumplen con la normativa y estándares establecidos, lo que es fundamental cuando se trata de presentar evidencias en procedimientos legales. Además, facilitará la validación de su trabajo por parte de terceros, como jueces y abogados, quienes confiarán más en la integridad de las evidencias presentadas.

Además, esta guía puede ayudar a mitigar problemas contemporáneos, como la falta de estandarización en la gestión de evidencias electrónicas, lo que en ocasiones puede comprometer casos judiciales o investigaciones corporativas. En una época en la que los ciberataques y las filtraciones de información son cada vez más frecuentes, contar con una metodología clara y válida para el tratamiento de evidencias digitales ofrece un nivel de protección adicional tanto para las organizaciones como para las instituciones de justicia.

1.4. Metodología

La metodología empleada para crear la guía de gestión de evidencias electrónicas conforme a la normativa española vigente se ha basado en un enfoque sistemático y normativo. En primer lugar, se realizó un estudio exhaustivo de las leyes y regulaciones españolas relacionadas con la gestión de evidencias digitales, tales como la Ley de Enjuiciamiento Civil y el Reglamento General de Protección de Datos (RGPD). Se realiza el estudio de estas leyes ya que las evidencias electrónicas pueden ser utilizadas como pruebas en juicio y su tratamiento puede poner peligro la privacidad de personas ajenas a la investigación.

Luego, se estudió la normativa nacional y los estándares vigentes actualmente en España, especialmente los que tienen como temática las evidencias electrónicas y la gestión de procesos informáticos. Además se consultaron estándares internacionales, como son los estándares ISO, para un mejor conocimiento acerca de los pasos de este proceso de gestión. Posteriormente, se revisaron protocolos y buenas prácticas recomendadas por organismos forenses, asegurando que cada etapa del proceso estuviese en línea con los requisitos legales. A través de la consulta de manuales técnicos y otras guía de organizaciones expertas en la materia como INTERPOL, se estructuró una guía clara y accesible que detalla los procedimientos esenciales, ofreciendo a los usuarios un recurso práctico y legalmente sólido para la correcta gestión de las evidencias electrónicas.

Basándonos en la información estudiada, la guía está estructurada en capítulos que corresponden a las cinco fases del proceso de gestión de evidencias electrónicas: identificación, captación, análisis, preservación y presentación. En la mayoría de las fases, las instrucciones se dividen en pautas generales y pautas adicionales, reflejando la necesidad de cumplir con ciertos pasos obligatorios mientras que otros pueden variar según las circunstancias específicas y el tipo de

dispositivo involucrado. Esta diferenciación es especialmente relevante en la fase de captación, donde las instrucciones se subdividen en directrices para dispositivos apagados y dispositivos encendidos. Dentro de cada categoría, se detallan pautas generales y adicionales para asegurar que el manejo de cada tipo de dispositivo se realice de manera adecuada y efectiva, atendiendo a las particularidades de cada situación.

1.5. Estructura

Este trabajo se desarrolla a lo largo de siete capítulos descritos a continuación:

- **Capítulo 1: Introducción**

El primer capítulo de este trabajo aborda los aspectos fundamentales que motivan la investigación sobre la gestión de evidencias electrónicas. Se definen los objetivos principales del trabajo, que incluyen la creación de una guía estructurada que permita facilitar la labor de los profesionales. También se anticipa el impacto esperado y se expone la metodología aplicada durante el proceso de investigación, lo que incluye revisiones documentales, análisis normativo y desarrollo de propuestas.

- **Capítulo 2: Estado del arte**

En este capítulo, se realiza una revisión exhaustiva de los tipos de evidencias electrónicas existentes, sus clasificaciones y cómo se emplean en diferentes ámbitos. Además, se hace un análisis de las normativas vigentes, lo que resulta esencial para comprender el marco legal que rodea la gestión de estas evidencias.

- **Capítulo 3: Análisis del problema**

El tercer capítulo se enfoca en el análisis de los desafíos que plantea la gestión de evidencias electrónicas, desde un punto de vista tanto legal como ético. Se discuten los obstáculos que los profesionales enfrentan al tratar con datos digitales y cómo las leyes actuales pueden generar ambigüedades o dificultades en su implementación. A partir de este análisis, se proponen varias posibles soluciones, como la creación de una guía unificada que facilite la comprensión y aplicación de las normativas vigentes. Se elige la solución que será desarrollada a lo largo del trabajo y se define el plan de acción y un posible presupuesto para creación de la guía.

- **Capítulo 4: Competencias básicas del personal**

En este capítulo, se describen las competencias que deben poseer los profesionales de la informática forense involucrados en la gestión de evidencias electrónicas. Se hace hincapié en la necesidad de contar con conocimientos técnicos profundos y habilidades prácticas para que los expertos deben ser capaces de identificar, captar, analizar y preservar evidencias digitales sin comprometer su integridad.

- **Capítulo 5: Fases del proceso de gestión de evidencias electrónicas**

Ofrece una visión detallada de la estructura y los aspectos clave de la guía para gestionar evidencias digitales. El capítulo está organizado en cinco fases esenciales: identificación, captación, análisis, preservación y presentación de evidencias electrónicas.

- **Capítulo 6: Conclusiones**

En el sexto capítulo, se reflexiona sobre los objetivos inicialmente planteados y se verifica en qué medida han sido alcanzados. Asimismo, se establece una relación entre el trabajo realizado y los estudios previos en el área. Las conclusiones también resaltan los aprendizajes adquiridos a lo largo del proceso y la importancia de una constante actualización en este campo en evolución.

- **Capítulo 7: Trabajos futuros**

Finalmente, en el último capítulo se exploran las posibles mejoras y expansiones que podrían realizarse en futuros trabajos. Este capítulo concluye proponiendo líneas de investigación adicionales que pueden contribuir al continuo perfeccionamiento de los procedimientos relacionados con la preservación y tratamiento de evidencias digitales.

Al final del trabajo podemos encontrarnos con el apartado de referencias bibliográficas y con los diferentes anexos:

- **Referencias bibliográficas**

Contiene las referencias bibliográficas utilizadas a lo largo del trabajo. Estas fuentes incluyen libros, artículos científicos, normativas y guías especializadas que han proporcionado el sustento teórico y legal para desarrollar los diferentes capítulos. La correcta citación de estas referencias asegura la veracidad y validez del contenido expuesto.

- **Anexo A. Guía completa**

Este anexo presenta la guía desarrollada a partir del trabajo de investigación. Explicando cada una de las fases del proceso de gestión de evidencias electrónicas. La guía ofrece una serie de pasos básicos que los profesionales pueden seguir para asegurar que las evidencias electrónicas sean gestionadas correctamente en cada una de las fases del proceso: identificación, captación, análisis, preservación y presentación. Se describen de forma clara los procedimientos recomendados para minimizar riesgos de pérdida o alteración de la información, y se proponen mejores prácticas que cumplen con las normativas vigentes. La guía también aborda aspectos técnicos que deben considerarse para garantizar que las evidencias sean admisibles en procedimientos judiciales.

- **Anexo B. Glosario y abreviaturas**

En este anexo se presenta el glosario de términos y las abreviaturas utilizadas a lo largo del trabajo, proporcionando definiciones claras y explicaciones para facilitar la comprensión de los conceptos y términos técnicos empleados en el documento.

- **Anexo C. Plantilla de identificación de evidencias electrónicas**

En este anexo encontramos una plantilla que puede servir para documentar las evidencias electrónicas a lo largo del proceso de identificación.

- **Anexo D. Funcionalidades mínimas de las herramientas hardware y software**

En este anexo se encuentra un listado de las funcionalidades mínimas que deben poseer las herramientas utilizadas para la captación y análisis de las e-evidencias.

- **Anexo E. Relación del trabajo con los objetivos de desarrollo sostenible de la agenda 2030**

Este anexo contiene una tabla y una pequeña explicación acerca de la relación del presente trabajo con los objetivos de desarrollo sostenible de la agenda 2030.

1.6. Convenciones

A lo largo del presente trabajo se han utilizado convenciones específicas para facilitar la comprensión y organización del contenido. Las citas textuales han sido marcadas claramente utilizando las comillas españolas («»), permitiendo diferenciar fácilmente los fragmentos tomados de otras fuentes. Por otro lado, todas las palabras o frases en inglés o en latín han sido presentadas en cursiva, con el objetivo de destacar términos técnicos que son relevantes para el análisis y discusión del tema.

En cuanto a las convenciones de los diagramas de flujo usados, los iconos redondos se utilizan para indicar el principio o fin del proceso o el principio de una rama de actividades adicionales que puede estar de cierta forma conectada con las demás actividades generales. En cuanto a los iconos triangulares, estos muestran que se debe tomar una decisión. Es decir, depende de las circunstancias tomaremos un camino u otro a partir de ese punto. Por último, los iconos rectangulares muestran los pasos a realizar, en otras palabras, dan información y conforman las pautas a seguir.

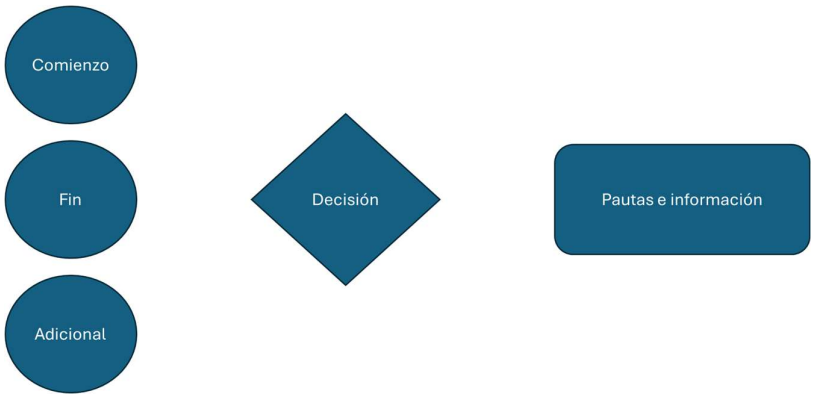

Figura 1. Convenciones de los diagramas de flujo.

Fuente: Elaboración propia.

2. ESTADO DEL ARTE

A día de hoy, prácticamente toda entidad, empresa u organización utiliza la tecnología informática y depende de ella para documentar, transmitir, almacenar y recuperar información digital, por lo que la integridad y seguridad de estos datos son de máxima prioridad para todas ellas.

2.1. Tipos de evidencias electrónicas

Cuando hablamos de evidencias electrónicas, estas vienen acompañadas de una investigación, ya sea jurídica o parte de una auditoria. Estas investigaciones se dividen en diferentes fases, siendo la primera de ellas la identificación de las potenciales evidencias electrónicas para más adelante recolectarlas y analizarlas. No obstante, para poder identificarlas primero tenemos que saber con qué tipos de evidencia electrónica nos podemos encontrar.

No obstante, hay diferentes formas de clasificar las evidencias electrónicas y, por ende, distintas maneras de tratarlas dependiendo del tipo de clasificación que elijamos. Si identificamos una evidencia con un tipo concreto, la tendremos que captar y analizar tratándola como tal. Por lo tanto, hay que ser consciente de la metodología que utilizamos para identificarlas. Las formas más comunes de clasificación las que toman como características principales su origen y naturaleza y las que se basan en su volatilidad, aunque podríamos enumerar muchas más.

2.1.1. Por origen y naturaleza

La clasificación de las evidencias electrónicas por su origen y naturaleza es fundamental para comprender su contexto, manejo y análisis adecuado. Las evidencias electrónicas pueden derivarse de múltiples fuentes, cada una con características distintivas que afectan a cómo deben ser tratadas y evaluadas. Aunque las fuentes pueden distinguirse según los casos, todas tienen una cosa en común: constituyen la base para proceder al análisis de los datos.

En un estudio llevado a cabo por la Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI) sobre las evidencias electrónicas se describen varios tipos de evidencias que pueden ser recolectadas y utilizadas en procedimientos judiciales y administrativos (Figura 2).

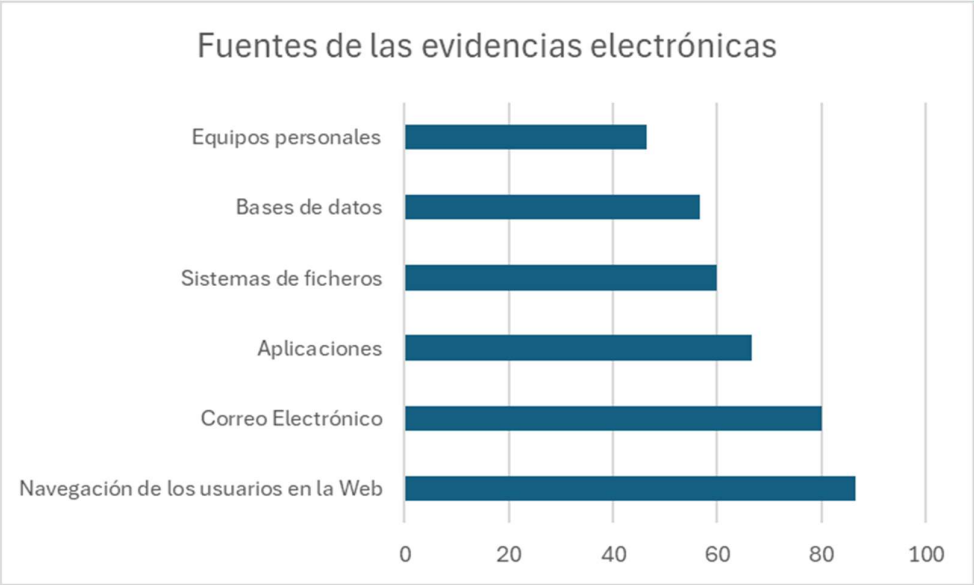

Figura 2. Porcentaje de casos en los que encontraos evidencias electrónicas procedentes de las principales fuentes.

Fuente: Elaboración propia a partir de datos del estudio de AUTELSI.

2.1.1.1. Navegación de los usuarios en la Web

El estudio destaca las seis fuentes donde es más frecuente hallar evidencias electrónicas. Entre estas, se sitúa en primer lugar, la navegación de los usuarios en la web, ya que como consecuencia de esta navegación se crean evidencias en un 86,6% de los casos estudiados. Las evidencias procedentes de esta fuente pueden ser el historial de navegación, las *cookies*, registros de actividad en internet, estadísticas del tráfico red y otros datos del uso de los navegadores por parte de los usuarios. Estas nos pueden proporcionar información sobre el comportamiento en línea de un individuo o entidad.

2.1.1.2. Correo Electrónico

Los correos electrónicos son una fuente común de evidencia, incluyendo tanto el contenido del mensaje como los archivos adjuntos, que pueden contener información crítica y reveladora. En este estudio se revela que en el 80% de los casos, las evidencias electrónicas tienen como origen estos correos. Al ser una forma común de comunicación digital pueden contener información crítica como acuerdos, discusiones, instrucciones, y otras formas de correspondencia relevante para la investigación.

2.1.1.3. Aplicaciones

Las aplicaciones juegan un papel crucial en la generación y almacenamiento de datos electrónicos que pueden servir como evidencias en procesos legales y administrativos. Según el estudio en un 66,6% de casos los datos recogidos en estas aplicaciones sirven como evidencias electrónicas.

Por ejemplo, aplicaciones empresariales como los sistemas de gestión de relaciones con clientes (CRM) y los de planificación de recursos empresariales (ERP) son fundamentales en cualquier negocio u organización. Estas aplicaciones registran transacciones, interacciones con clientes, movimientos de inventario, y otros procesos empresariales críticos. Los registros de estas actividades pueden ser esenciales para demostrar el cumplimiento de contratos, la veracidad de transacciones financieras, o la conducta empresarial.

Otras aplicaciones como Microsoft Teams, Slack o WhatsApp son utilizadas extensamente para la comunicación interna y externa. Las conversaciones y los mensajes pueden contener información relevante sobre acuerdos, decisiones, y acciones tomadas, y pueden ser presentadas como evidencias en litigios o investigaciones.

Además, herramientas como Trello, Asana y Jira registran el progreso de proyectos, asignación de tareas, y comunicaciones relacionadas. Estos registros pueden ayudar a establecer líneas de tiempo, responsabilidades, y el cumplimiento de plazos y entregables, los cuales también se pueden usar como evidencias en auditorías.

Asimismo, *software* como QuickBooks, SAP, y las aplicaciones bancarias registran movimientos financieros, pagos, y recibos. Estos datos son cruciales para auditorías, investigaciones de fraude, y litigios financieros.

2.1.1.4. Sistemas de ficheros

Los sistemas de ficheros son una fuente de información de la cual proceden una parte significativa de las evidencias electrónicas. De hecho, según el estudio de AUTELSI, en un 60% de los casos podemos encontrar evidencias electrónicas con este origen. Esto sugiere que los documentos y archivos almacenados en sistemas de ficheros (como documentos de Word, PDFs y hojas de cálculo, entre otros) son fundamentales como evidencia en procesos legales y auditorías.

2.1.1.5. Bases de datos

Las bases de datos también son una fuente crucial de evidencia electrónica, en el 56,6% de los escenarios estudiados formaban parte del origen de las evidencias. Lo cual indica, que los datos estructurados y transaccionales almacenados en sistemas de gestión de bases de datos son comunes en procedimientos legales. Algunos ejemplos de evidencias provenientes de estas

fuentes podrían ser: registros financieros, historiales de clientes y registros de empleados, entre otros.

2.1.1.6. Equipos personales

Aunque en menor proporción que las anteriores fuentes mencionadas, los equipos personales también pueden ser considerados como fuentes significativas de evidencias electrónicas, ya que podemos obtener evidencias originarias de estos en un 46,6% de los casos estudiados. Prueba de ello puede ser el uso de computadoras personales o dispositivos móviles para almacenar comunicaciones personales relacionadas con el trabajo, correos electrónicos u otros datos relevantes para una investigación.

2.1.1.7. Otras fuentes

Las anteriores eran las seis principales fuentes de información de donde pueden provenir ciertos tipos de evidencias digitales. No obstante una lista parcial de fuentes de evidencia digital también incluye sistemas operativos, medios de almacenamiento (CDs, unidades extraíbles/flash, nube, etc.), módulos de memoria, discos duros (HDD), supercomputadoras, servidores, archivos de registros de eventos, redes cliente-servidor distribuidas, caché de aplicaciones, computadoras portátiles, teléfonos inteligentes, cámaras digitales, LANs, WANs, etc. Cada una de estas fuentes proporciona un camino particular para extraer una gran cantidad de evidencia que puede respaldar todo el proceso forense bajo estricta cadena de custodia.

A su vez, cada uno de estos tipos de evidencias electrónicas tiene sus propias características y requerimientos de manejo para asegurar su integridad y validez en un contexto legal. Es crucial seguir procedimientos adecuados para la recolección, preservación, y presentación de estas evidencias para garantizar que sean admisibles y útiles en un tribunal o cualquier otra instancia legal.

2.1.2. Por volatilidad

Otra forma de clasificar las evidencias electrónicas, y quizás la más importante, es según su volatilidad. Con volatilidad nos referimos a la estabilidad de la evidencia y su persistencia en el tiempo. Esta clasificación es crucial para determinar los métodos y la urgencia con que deben ser recolectadas y preservadas las evidencias electrónicas, garantizando así su integridad y utilidad en análisis posteriores.

A estos efectos, definimos tres tipos de categorías en las que podemos clasificar a las evidencias electrónicas según su volatilidad. En primer lugar tenemos las evidencias estáticas. Estas no cambian. Son evidencias que están almacenadas y que podemos consultar de manera recurrente. Sin embargo, hay peligro de que sean alteradas por el uso normal de las mismas. Por

ejemplo, si accidentalmente modificamos un fichero, ahora nosotros somos el usuario que ha realizado la última modificación. Ya no podemos saber quién fue el usuario que modificó el documento antes de que nosotros lo hiciésemos accidentalmente. Estas son las evidencias que obtenemos de la información no volátil. En segundo lugar tenemos las evidencias dinámicas. Estas son evidencias que podemos hallar en alojamientos temporales, que están procesadas o en espera de ser procesadas. El problema es que sus características hacen que en un breve espacio de tiempo puedan desaparecer, es decir es información volátil. Por último tenemos las evidencias encaminadas. Son evidencias que se están moviendo por la red como, por ejemplo, un paquete de información que puede ser en un momento dado capturado o almacenado.

En los apartados 2.1.2.1. y 2.1.2.2. ahondamos en qué se considera información volátil y no volátil respectivamente.

2.1.2.1. Información volátil

Tomamos como información volátil los datos que son especialmente propensos a cambiar y pueden ser modificados fácilmente. También se incluyen los datos que cambian a medida que cambia el estado del sistema. Estos cambios de estado se pueden efectuar al apagar o reiniciar el dispositivo o al pasar a través de un campo magnético.

Dicho esto, las evidencias volátiles son aquellas que se pierden cuando un dispositivo cambia su estado. Esta información también puede ser afectada por el nivel de humedad, el tiempo o incluso por los cambios a dispositivos cercanos. Ejemplos de evidencias volátiles incluyen los datos almacenados en la memoria RAM, en la caché o las direcciones IP dinámicas, entre otros. Esta característica implica que las evidencias volátiles deben ser capturadas rápidamente y con técnicas especializadas antes de que se desvanezcan.

2.1.2.2. Información no volátil

Las evidencias electrónicas no volátiles son aquellas que permanecen almacenadas de manera persistente en un dispositivo, independientemente de si el dispositivo se apaga o reinicia. Este tipo de evidencia es crucial en investigaciones forenses y auditorías, ya que proporciona datos que pueden ser recuperados y analizados en cualquier momento posterior al evento de interés.

Entre este tipo de evidencias encontramos los archivos guardados en discos duros, unidades de estado sólido (SSD), dispositivos de almacenamiento extraíbles como unidades USB. Además, los registros de sistemas, bases de datos y documentos digitales también forman parte de esta categoría.

La durabilidad de las evidencias no volátiles implica que, una vez almacenadas, estas mantienen su integridad hasta que sean deliberadamente modificadas o eliminadas, lo que las convierte en una fuente confiable de información para reconstruir eventos y validar la integridad de sistemas y datos.

2.1.3. Otras clasificaciones

Las metodologías de clasificación explicadas en los puntos 2.1.1 y 2.1.2 son las más relevantes pero eso no implica que no existan otros métodos que en ciertos escenarios puedan ser de mayor ayuda. Aunque menos populares, también podemos clasificar las evidencias electrónicas según su estructura, su medio de almacenamiento o incluso el tipo de contenido que las forma.

Si decidimos clasificar las evidencias atendiendo a su estructura las estaremos clasificando como evidencias estructuradas, desestructuradas y semiestructuradas. Las evidencias estructuradas son datos organizados en formatos específicos y bien definidos, como hojas de cálculo y otro tipo de bases de datos, que permiten una fácil búsqueda y manipulación. Por otro lado, las evidencias no estructuradas carecen de una organización predefinida, y se encuentran en formas más libres como correos electrónicos y documentos de texto, lo que puede hacer su análisis más complejo y laborioso. Entre estos extremos se encuentran las evidencias semiestructuradas, que poseen algún nivel de organización aunque no tan riguroso como las estructuradas. Ejemplos de estas son los archivos JSON y HTML, que tienen una estructura definida pero flexible, permitiendo almacenar datos en un formato que es tanto legible por humanos como procesable por máquinas.

Por otro lado, la clasificación de las evidencias electrónicas según su medio de almacenamiento es esencial para entender cómo y dónde se guarda la información, lo cual tiene implicaciones significativas para su acceso y seguridad. Las evidencias almacenadas localmente se encuentran en dispositivos físicos como computadoras y dispositivos móviles, lo que permite un control directo sobre los datos, pero también plantea riesgos en caso de pérdida o daño del dispositivo. En contraste, las evidencias almacenadas de manera remota se ubican en servidores externos o en la nube, ofreciendo ventajas como la accesibilidad desde múltiples ubicaciones y una mayor protección contra pérdidas físicas, aunque también pueden suscitar preocupaciones acerca de la protección de la privacidad y la seguridad digital. Por último, las evidencias almacenadas en un sistema híbrido combinan ambos métodos, guardando datos tanto en medios locales como remotos, lo que proporciona un equilibrio entre accesibilidad y seguridad, y permite una mayor flexibilidad en la gestión de la información. Esta clasificación en virtud del medio de almacenamiento ayuda a determinar las estrategias de manipulación y preservación más adecuadas para las evidencias electrónicas.

Otra de las posibles clasificaciones y la última en la que indagaremos es la que distingue las evidencias electrónicas según su tipo de contenido, pudiendo diferenciarse entre evidencias textuales, multimedia o transaccionales. Las primeras comprenden información en forma de texto, tales como correos electrónicos y documentos, que pueden contener detalles precisos y comunicados importantes. Las evidencias multimedia incluyen archivos de audio, video e imágenes, ofreciendo una representación visual o auditiva que puede ser vital para la comprensión completa de un evento o situación. Finalmente, las evidencias transaccionales consisten en registros de transacciones financieras y *logs* de sistemas, proporcionando un rastro detallado de actividades y operaciones que es esencial para auditorías, investigaciones financieras y análisis de comportamiento.

2.2. Usos de las evidencias electrónicas

En el apartado 2.1 se han visto las diferentes formas de clasificar las evidencias electrónicas, pero ¿para qué las necesitamos? ¿Con qué fin las usamos? Estas son las preguntas que vamos a responder en este apartado. Comprender el propósito y la utilidad de las evidencias electrónicas es fundamental para apreciar su importancia en diversos contextos.

En el ámbito legal, las evidencias electrónicas son cruciales para la resolución de disputas y la administración de justicia, ya que proporcionan pruebas contundentes y verificables. Mientras, en el entorno empresarial las evidencias electrónicas son esenciales para la gestión de la información, la auditoría y el cumplimiento normativo, permitiendo a las empresas y organizaciones operar con transparencia y responsabilidad. Además, si hablamos de ciberseguridad, estas evidencias ayudan a identificar y mitigar amenazas, protegiendo la integridad de los sistemas y datos.

2.2.1. El ámbito judicial

Las evidencias electrónicas pueden tener varios contextos de uso, siendo el más popular su uso en el ámbito judicial. En este caso, la evidencias se recopilan específicamente para su uso en procedimientos legales, abarcando registros de llamadas, mensajes en redes sociales y otros datos pertinentes a casos legales. Estas evidencias son fundamentales para la resolución de disputas, la comprobación de hechos y la administración de justicia.

Las evidencias digitales tienen un impacto comparable al de las huellas dactilares en el sentido de que pueden cambiar el rumbo de la investigación. Habitualmente, estas evidencias están escondidas, además de que son sumamente susceptibles a cambios, dado a la facilidad con que puede efectuarse su alteración o borrado. No obstante, este tipo de información es admisible en procesos legales, ya que posibilitan la recuperación de archivos relacionados, como documentos ofimáticos y conversaciones. (LIFe, 2022)

A pesar de que la evidencia digital parece ser útil solamente para investigaciones de delitos cibernéticos, en realidad, pueden usarse en cualquier tipo de caso. Las fuentes de evidencia digital abarcan una amplia gama de delitos, incluyendo acoso, piratería, robos, asesinatos, violaciones, prostitución, maltrato, estafas y vulneración de la propiedad, entre otros. Incluso cuando estos crímenes e infracciones no se cometen directamente a través de las nuevas tecnologías, las evidencias electrónicas se pueden utilizar antes o después del acto delictivo, dejando así un rastro visible para los investigadores. (LIFe 2022)

Estos datos llamados evidencias pueden inculpar a los ciberdelincuentes y ayudar a identificar a las víctimas. De hecho, según el SEC, los delitos informáticos aumentaron entre 2019 y 2023. Así, se puede observar que, en 2023, el número total de hechos conocidos es de 472.125, un 26% más con respecto a 2022. De todos estos incidentes, el 90,5% corresponde a fraudes informáticos (estafas), mientras que el 3,7% restante está formado por amenazas y coacciones. (SEC, 2023)

La cibercriminalidad está ganando importancia a medida que aumenta, año tras año, el número de hechos conocidos y su peso proporcional en la delincuencia en general. Esto se puede observar

en la Figura 3, que muestra como estos hechos han pasado de formar el 9,9% de los delitos en España en el año 2019, a un 19,2% en el año 2023. (SEC, 2023)

2019	9,9%
2020	16,3%
2021	15,6%
2022	16,1%
2023	19,2%

Figura 3. Porcentaje que representa la cibercriminalidad sobre el total de infracciones penales.

Fuente: SEC, 2023.

Adecuadamente captadas y autenticadas, las e-evidencias son esenciales para la acusación o la defensa en cualquier tribunal, ayudando a esclarecer los hechos ocurridos. Como consecuencia, los peritos informáticos cuentan con instrumentos útiles para demostrar la veracidad de las evidencias electrónicas comparando las copias realizadas en el proceso de captación con las evidencias electrónicas originales. Dicha comparación contribuye a que los procesos de captación y preservación de las evidencias sean confiables, demostrando su proveniencia. (LIFe, 2022)

Cada vez es más común presentar pruebas electrónicas ante los tribunales y sea cual sea la jurisdicción. Además, ha crecido significativamente la diversidad de fuentes de evidencia introducidas durante los procesos judiciales. Grabaciones de videovigilancia, correos electrónicos, comentarios en redes sociales, mensajes instantáneos, capturas de pantalla de teléfonos móviles o extractos bancarios son algunos ejemplos del extenso repertorio que continúa aumentando según se desarrollan nuevas y más avanzadas tecnologías. (ICAM)

En un contexto en el que la delincuencia converge con la tecnología, las e-evidencias se han convertido en una herramienta esencial para asegurar la efectividad de los procesos jurídicos actuales. Por ello, es fundamental tener en cuenta que las evidencias digitales deben cumplir con ciertos requisitos para ser aceptadas en cualquier proceso legal. Estos requisitos hacen posible que las e-evidencias sean válidas en los juzgados (Sheetz, 2013):

1. Admisibilidad. - Las evidencias deben acatar las leyes y normativas actuales.

2. Autenticidad - Las evidencias deben ser reales y se deben poder relacionar con el incidente de forma relevante.

3. Integridad. – Con tal que las evidencias sea válidas, estas deben estar completas. Las evidencias deben ser suficientes, crear una representación completa del incidente y tener la capacidad de demostrar las operaciones realizadas en el dispositivo.

4. Fiabilidad. – La veracidad y autenticidad de las evidencias recolectadas y analizadas, no deben ser cuestionable. Las evidencias digitales son confiables si provienen de cualquier

dispositivo que no haya estado expuesto a amenazas. Además, se debe asegurar que dicho dispositivo funciona correctamente.

5. Credibilidad. – El jurado debe estar convencido de la integridad de la evidencia y poder entenderla claramente.

La evaluación de las evidencias electrónicas en un juicio implica establecer la credibilidad que le corresponde según el sistema legal decretado. En España hay dos sistemas legales para valorar este tipo de evidencias (ICAM):

- Sistema de prueba tasado o legal: la legislación establece de antemano el nivel de utilidad que el magistrado debe asignar a una evidencia digital específica para resolver el incidente.

- Sistema de prueba libre: el juez evaluará las evidencias electrónicas mediante una valoración libre y conforme a las reglas del criterio racional. Por norma general, si hablamos de evidencias electrónicas este sistema será el que se aplicará, tal como se puede concluir de los artículos 348 y 384.3 de la Ley de Enjuiciamiento Civil, que determinan que «el Tribunal valorará los instrumentos a que se refiere el apartado primero de este artículo conforme a las reglas de sana crítica aplicables a aquéllos según su naturaleza».

La ley vigente no exige al magistrado o al tribunal a considerar como cierta la información presentada que conforma la evidencia digital, salvo en el caso de que la evidencia estuviese formada por documentos públicos electrónicos. Las e-evidencias servirán simplemente para demostrar el hecho en cuestión, sin embargo su validez será determinada por el juez de acuerdo con las reglas de la sana crítica. (ICAM)

Para la valoración de la prueba electrónica el juez no debe tener razón para dudar de su integridad ni de la autenticidad de su origen. Es decir, el magistrado debe estar convencido de que los datos que forman la evidencia electrónica no han sido modificados y de que su supuesto autor es realmente su autor.

En caso de que surjan dudas sobre la credibilidad de alguna de estas características mencionadas, es extremadamente probable que el magistrado rechace la validez de la evidencia digital en el juicio. Dentro de los criterios para garantizar la legitimidad de una prueba electrónica, además de su captación de forma legal y el cumplimiento de la cadena de custodia, es esencial demostrar la autenticidad e integridad de la prueba mediante un peritaje informático.

En este contexto judicial, la postura de las partes implicadas y de sus respectivos abogados resulta crucial. El magistrado deberá considerar la opinión de todas las partes respecto a la evidencia electrónica presentada, particularmente si otra parte cuestiona su autenticidad.

Si no se duda de la validez de dicha evidencias electrónica, es muy probable que el juez la considere como auténtica y precisa, evaluándola junto con las demás pruebas. Sin embargo, si se presenta una impugnación, el juez prestará atención tanto a las argumentaciones que justifican el rechazo como a los medios de prueba y dictámenes periciales presentados para demostrar su validez.

En la práctica jurídica, la parte que busca validar la prueba debe respaldarla con todos los medios probatorios disponibles. Esto se hace con tal de fortalecer la e-evidencia presentada, normalmente mediante un perito informático que corrobore su autoría y que no ha sido manipulada. En caso de impugnación, es crucial realizar un peritaje que verifique el auténtico origen de la evidencia, identifique a los actores y asegure la integridad de los datos.

En manos de un perito informático competente, las evidencias electrónicas pasan por dos procesos esenciales con el fin asegurar su confiabilidad, integridad y validez. Primero, durante la captación de las evidencias se deben utilizar técnicas que aseguren su integridad. De este modo, los peritos deben documentar y justificar cada una de las acciones realizadas sobre las evidencias, ordenadas por su grado de volatilidad y dando prioridad a las evidencias más volátiles. Por ejemplo, priorizando la adquisición de registros y datos en la memoria caché, continuando con la recopilación de los documentos y archivos guardados en el dispositivo digital. Este tema se verá en más detalle en el punto 4. (LIFe, 2022)

Por otra parte, los peritos informáticos deben prestar atención en especial a la preservación de las evidencias electrónicas, asegurándose de respetar la cadena de custodia y almacenamiento de dichas evidencias. De esta forma se evitan acciones que puedan dañar su integridad, como, por ejemplo, apagar un dispositivo sin razón alguna. (LIFe, 2022)

2.2.2. El ámbito empresarial

Otro ámbito en el que usamos las evidencias electrónicas es en el ámbito empresarial, es decir dentro de empresas y organizaciones. En este caso las evidencias abarcan datos generados y utilizados por estas, por sus empleados o por sus clientes, incluyendo registros financieros, correos electrónicos corporativos y datos de clientes. Estas evidencias son esenciales para la gestión eficiente de las operaciones, la toma de decisiones informadas y la conformidad con regulaciones.

En un contexto donde prácticamente toda organización y empresa, pública o privada, depende de sistemas digitales para sus procesos y actividades de negocio, es fundamental asegurar la disponibilidad de evidencias digitales lícitas. Esto permite salvaguardar adecuadamente los intereses empresariales y demostrar el cumplimiento de sus obligaciones.

La informática forense también facilita la investigación de incidentes de ciberataques corporativos que involucran ataques de virus y *ransomware*, denegación de servicio, secuestro de sesiones de sitios web y muchas otras formas de delitos cibernéticos. La aplicación de la informática forense en la investigación de ciberataques se centra en la reconstrucción sistemática de los incidentes mediante la recopilación de posibles pruebas de numerosas fuentes internas y externas, incluyendo una revisión de las configuraciones de las computadoras, la evaluación de topologías de red, el escrutinio de credenciales de inicio de sesión, la auditoría de archivos de registro anteriores, la confirmación del estado del software antivirus, la revisión de la efectividad de los Sistemas de Detección y Prevención de Intrusiones (IDS e IPS), la colusión interna, las violaciones de ingeniería social, etc. Además, ayuda a descubrir la causa raíz y los impactos de

los incidentes que involucran datos electrónicos recuperados de activos digitales locales o remotos.

Teniendo esto en cuenta, para algunas empresas un problema puede ser una fuga o robo de información que ponga en duda su servicio y reputación, afectando su cotización, como ocurrió con Facebook en el año 2018. Sin embargo, para otras empresas, un incidente puede ser la falta de servicio de un proveedor que afecta la operativa, el envío de un correo electrónico con información crítica por parte de un empleado, un comentario inapropiado o noticias falsas en las redes sociales, la recepción de un mensaje anónimo en el canal de denuncias, o un pleito relacionado con casos de competencia desleal o propiedad intelectual, entre otros.

Para dar una solución adecuada a un problema o incidente, es esencial contar con un plan de acción que sirva de guía para tomar los pasos necesarios que mitiguen su impacto y permitan resolverlo en un tiempo razonable. Aquí es donde los servicios forenses entran en juego. Habitualmente, los departamentos de sistemas de las empresas no poseen los conocimientos ni las herramientas necesarias para tratar los datos desde una perspectiva técnico-forense, es decir, manejando estos datos como evidencias electrónicas. No sería la primera vez que, en un intento de contener el incidente, los propios técnicos de la empresa terminan haciendo que la información no sirva como evidencia o prueba del caso.

A pesar de esto, según el estudio de AUTELSI mencionado en el punto 2.1.1. , solo un 20% de las empresas y organizaciones encuestadas efectúan un cifrado sobre las evidencias obtenidas y solamente el 25% utiliza medios para protegerlas, como pueden ser la firma digital o el almacenamiento en dispositivos seguros. Citando al presidente del grupo de regulación de AUTELSI y encargado de presentar los resultados del estudio, Óscar López, «Mantener los registros de las evidencias sin un mecanismo que permita garantizar que cualquier modificación ulterior será detectada, puede derivar en el posterior cuestionamiento de las evidencias proporcionadas».

Un elemento clave para obtener información son los registros o *logs* de actividad. Sorprendentemente solamente un 6.6% de los encuestados en el estudio afirman contar con mecanismos para proteger y, por lo tanto, preservar las evidencias electrónicas. Desde AUTELSI se señala que, aunque la mayor parte de las empresas son, en cierta medida, capaces de adquirir evidencias digitales de sus dispositivos, pocas cuentan con la capacidad de proteger su integridad. Por lo que queda claro que es necesario mejorar los mecanismos de protección. Además, es significativo que solo el 53.3% de los encuestados haya respondido afirmativamente a la pregunta de si consideran los aspectos relacionados con la gestión de e-evidencias en sus procedimientos y políticas, sin embargo el 9.5% de ellos no vea necesario el uso de tal sistema de gestión.

Existen casos en los que la alteración de la fecha de un archivo (algo común en los procesos de recuperación de ficheros) impide que el análisis técnico-forense pueda confirmar que dicho archivo no ha sido modificado posteriormente, generando dudas sobre su integridad o incluso su autenticidad. En resumen, el éxito en la resolución de un problema o incidente dependerá de que la empresa cuente con una estrategia que identifique a los actores (internos y externos) y los recursos (herramientas y metodología) necesarios para su contención y resolución. Es crucial que la información a analizar esté previamente identificada y sea accesible de manera oportuna, es

decir que esté bien protegida y preservada, lo que permitirá a la empresa abordar una solución de manera ágil y adecuada.

Con la evolución de las tecnologías digitales, las organizaciones se han visto obligadas a cambiar la forma en que planifican, desarrollan y ejecutan sus estrategias de tecnología de la información. Esto se debe a que las tecnologías digitales modernas no solo presentan nuevas oportunidades para las organizaciones empresariales, sino también un conjunto diferente de problemas y desafíos que necesitan ser resueltos. Con el aumento de las amenazas de delitos cibernéticos, por ejemplo, que se ha acelerado con la aparición de nuevas tecnologías digitales, muchas organizaciones, así como las agencias que aplican de la ley a nivel mundial, están implementando medidas proactivas como una forma de aumentar su capacidad para responder a incidentes de seguridad y crear un entorno preparado para la informática forense.

Durante la pandemia de COVID-19, hubo un cambio de mentalidad en el sector empresarial entorno a la necesidad de servicios forenses. Según un estudio de IMARC Group, una empresa experta en investigación y análisis de mercado, el repentino brote de la pandemia llevó a un aumento de la implementación de la informática forense en organizaciones y empresas de diferentes partes del mundo. Principalmente este se aplica para la investigación rápida y precisa de fraudes financieros y estafas durante el trabajo, que durante esta época en muchos sectores se realizaba a remoto, haciendo uso de los dispositivos electrónicos disponibles en las casas de los trabajadores. En consonancia con esto, la creciente disponibilidad de conexiones a internet fáciles de acceder, junto con la proliferación de diversas aplicaciones y dispositivos basados en redes, como servicios de correo electrónico, computadoras, tecnologías en la nube, banca por internet y teléfonos inteligentes, están favoreciendo el crecimiento de este mercado de la informática forense.

Estos incidentes en la industria BFSI (Banca, Servicios Financieros y Seguros) a nivel mundial además de varios avances tecnológicos, como la integración de la inteligencia artificial (IA) con la informática forense para observar con precisión las similitudes en la comunicación y detectar elementos que puedan ser usados como evidencias en fotos y videos, están impulsando su crecimiento en el mercado. Adicionalmente, la creciente demanda de productos para recuperar archivos eliminados de dispositivos digitales y obtener datos encriptados debido al aumento de casos de fraude y robo de identidad y otros factores, como las mejoras significativas en la infraestructura de tecnología de la información (TI) y la implementación de diversas iniciativas gubernamentales para promover soluciones de seguridad avanzadas que protejan datos sensibles, están creando una perspectiva positiva para este mercado.

Según este mismo estudio, en el año 2023, el mercado mundial de la informática forense se estimó en 6.400 millones de dólares y se espera que este presente una tasa compuesta anual (CAGR) del 8,7% durante el periodo de 2024 a 2032, es decir, que se espera que en el año 2032 el mercado crezca un 8.7% en respecto a 2023, con una valoración de 13.700 millones de dólares. El estudio se hizo cogiendo como referencia los cambios que tuvo el mercado forense digital durante los años 2018 al 2023.

En los Estados Unidos, varias grandes corporaciones y empresas ya han establecido unidades de informática forense independientes dentro de sus organizaciones para investigar y analizar datos digitales relacionados con delitos informáticos. Otras integran este servicio en

departamentos de tecnología de la información ya existentes con tal de solucionar incidentes emergentes. Algunas más optan por establecer acuerdos contractuales con firmas consultoras externas o individuos para proporcionar estos servicios tan necesarios. (Barbara, 2005)

Por otro lado, un informe de Mordor Intelligence, una firma especializada en análisis de mercado, proyecta que en Europa el sector de la informática forense aumentará para alcanzar una tasa compuesta anual (CAGR) del 10,9% entre 2023 y 2028. Este mercado en Europa se encuentra solo parcialmente consolidado, ya que las empresas en este sector han recurrido a asociaciones, fusiones y adquisiciones con el fin de crear soluciones adecuadas para los usuarios finales. Entre los actores principales del mercado se encuentran LogRhythm Inc., MSAB Inc., IBM Corporation, Nuix y PricewaterhouseCoopers.

La informática forense ha evolucionado desde la investigación de delitos informáticos menores hasta la investigación de incidentes con un impacto significativo. Esta disciplina implica la recuperación y el análisis de datos de dispositivos digitales, que a menudo, aunque no siempre, están vinculados a delitos informáticos. Además, con el creciente impactos de los dispositivos electrónicos en Europa, el mercado de la informática forense está en constante evolución.

Por otra parte, otros campos de la informática forense, como los relacionados con teléfonos móviles y dispositivos portátiles, están emergiendo rápidamente en el ámbito de la preservación digital, aunque tradicionalmente el enfoque ha estado en computadoras de escritorio, portátiles y medios asociados como discos duros, disquetes y discos ópticos. El mercado de los teléfonos inteligentes también ha estado creciendo progresivamente en términos de proveedores, modelos y tamaño. Adicionalmente, tecnologías como la computación en la nube y el Internet de las Cosas (IoT) están teniendo un impacto significativo en la industria de las tecnologías de la información, configurando el futuro del entorno digital.

El progresivo aumento en la popularidad de la computación en la nube ha sido impulsado por la innovación tecnológica de las empresas, destacando las políticas de BYOD (Bring Your Own Device) en diversos sectores. La expansión de las soluciones en la nube, que permiten acceder a información y archivos desde prácticamente cualquier lugar, ha facilitado una colaboración más eficiente entre equipos ubicados en distintas zonas. Sin embargo, este incremento en la cantidad de dispositivos conectados en las empresas también ha elevado las posibilidades de intrusión por parte de los hackers.

Los especialistas en informática forense trabajan para mejorar la seguridad corporativa al ofrecer asesoramiento a los ejecutivos sobre las actualizaciones de sistemas y al proporcionar formación al personal en temas de ciberseguridad. Dado que las brechas de datos pueden llevar al robo de información o dinero, perjudicando la reputación y las finanzas de la empresa, estas recurren a expertos forenses para asegurar la protección adecuada de sus activos.

Además, durante la pandemia global de 2020, la necesidad de soluciones para el trabajo remoto creció a medida que las empresas adoptaron el trabajo desde casa en lugar de las prácticas laborales tradicionales. La incorporación de más dispositivos personales, que a menudo no están suficientemente protegidos, a la red corporativa incrementa el riesgo de comprometer la seguridad de la red. Por lo tanto, estos cambios deben ser evaluados con cautela en el contexto de la ciberseguridad empresarial.

Las técnicas de informática forense aún se consideran herramientas especializadas para la policía. De manera similar, hasta hace unas décadas, la seguridad informática y de redes se percibía como una utilidad de defensa para establecimientos militares. Pero ahora, la seguridad informática y de redes se ha convertido en un producto básico para todos los sistemas empresariales y las PC domésticas. Las empresas de hoy sienten la necesidad de mecanismos de monitoreo eficientes para protegerse de las amenazas comerciales emergentes, como el análisis de la competencia y la esteganálisis. Las compañías en Estados Unidos han adoptado ampliamente la tecnología de informática forense; sin embargo, las empresas europeas, en particular las pequeñas y medianas empresas (PYMES), aún no han aprovechado el potencial de esta tecnología.

La iniciativa de la Comisión Europea de Sistemas Empresariales de Internet del Futuro (FInES) presenta una nueva era prometedora para la innovación empresarial. Sin embargo, las soluciones y prácticas de seguridad empresarial existentes generalmente se concentran en las medidas de prevención de incidentes, es decir, la prevención de ataques, sin un enfoque considerable para los escenarios posteriores a los accidentes.

En octubre de 2022, la Oficina Europea de Lucha contra el Fraude (OLAF) organizó su vigesimotercera sesión de capacitación para forenses y analistas digitales. Este taller, dirigido a personal de organismos nacionales de aplicación de la ley, abordó temas como ciberdelitos, informática forense y análisis en la lucha contra el fraude. Los estudiantes, gracias a la formación en inteligencia de fuentes abiertas, Linux y forense móvil, están mejor preparados para gestionar tareas de análisis y forense en campos como el análisis de fraudes monetarios, intercambio de datos en línea, transacciones con criptomonedas, investigaciones financieras y colaboración con OLAF. (Mordor Intelligence, 2024)

La informática forense apoya la resolución técnica de problemas operativos de computación, proporcionando a los administradores de sistemas las herramientas para realizar el restablecimiento de contraseñas, la revisión de CCTV, la recuperación de archivos de *back-end*, la auditoría de informes de acceso biométrico, la recuperación de daños accidentales del sistema, la respuesta a incidentes, etc.

Independientemente del área de aplicación, la informática forense sigue un procedimiento estándar universal que consiste en la recolección de datos, el examen, el análisis y la elaboración de informes bajo una estricta cadena de custodia. El producto final de la informática forense suele ser una evidencia documentada de manera sistemática, derivada de fuentes digitales, para abordar disputas, investigaciones y otros problemas que involucran dispositivos de almacenamiento, sistemas de comunicación de datos, aplicaciones de *software* y recursos en línea.

2.3. Normativa vigente actual

En este apartado, se hablará sobre la normativa en vigor en España relacionada con la gestión de evidencias electrónicas. Este marco normativo es esencial para garantizar que la obtención, análisis, conservación y presentación de dichas evidencias se realice adecuadamente, satisfaciendo los requisitos legales. Se explicarán las principales normas que orientan este

proceso, asegurando que las evidencias digitales sean aceptadas y válidas, al mismo tiempo que se protege la integridad de los datos durante todo su ciclo de vida. Además, es importante dejar claro que ninguna de estas normas y estándares es de cumplimiento obligatorio, es decir, son fundamentalmente guías de buenas prácticas.

2.3.1. UNE 17505:2013

La norma UNE 17505:2013, titulada formalmente como «Sistema de Gestión de Evidencias Electrónicas (SGEE)» está conformada por 3 partes. Esta establece los requisitos necesarios para asegurar el tratamiento de información personal en el ámbito de las TIC. Esta norma se focaliza en avalar que el procesamiento la información personal se efectúe de forma segura y conforme a la normativa de protección de datos vigente, protegiendo los derechos de los individuos y su privacidad.

En la primera parte de la norma, UNE 71505-1:2013, se describen el «vocabulario y principios generales». Es decir, se proporcionan definiciones de términos y conceptos para asegurar la uniformidad y consistencia entre las tres partes que la componen. Además, proporciona una visión general del proceso de gestión de evidencias digitales.

Específicamente, la norma UNE 71505-1:2013 establece los principios y directrices fundamentales para la gestión segura de información personal en las organizaciones. Enfatiza la importancia de la legalidad, transparencia, delimitación de los objetivos y precisión en el procesamiento de la información. Además, define las responsabilidades organizativas, la necesidad de implementar medidas para garantizar la seguridad adecuadas y asegurar el cumplimiento con la normativa vigente, como el RGPD. También introduce la gestión de riesgos como un elemento clave para mantener la protección de la información personal.

Durante la segunda parte de la norma, UNE 71505-2:2013, se describen una serie de «buenas prácticas en la gestión de las evidencias electrónicas». Esta define los controles y procedimientos aplicables para garantizar la seguridad de las evidencias digitales. En mayor detalle, se enfoca en los procedimientos específicos para la implementación de las directrices y principios descritos en la primera parte. Esta sección detalla las medidas que las organizaciones deben adoptar para asegurar la protección efectiva de la información personal. Esto incluye la gestión de riesgos, la adopción de controles de seguridad como la autenticación o el cifrado, y la creación de políticas internas que garanticen el cumplimiento continuo de la normativa. También se aborda la importancia de las auditorías, la formación del personal y la revisión periódica de las prácticas de seguridad para adaptarse a cambios en las amenazas y en la normativa aplicable.

En la norma UNE 71505-3:2013, la última de las tres partes, «formatos y mecanismos técnicos», se pretende establecer un formato estandarizado que posibilite el intercambio de evidencias digitales entre entidades. Además, se determinan qué mecanismos se aplicarán para conservar su confiabilidad. Más específicamente, se enfoca en los requisitos técnicos que deben implementarse con el fin de proteger la integridad de los datos almacenados y procesados en sistemas informáticos. Esta sección aborda los requisitos para proteger los datos y sistemas frente a amenazas como accesos no autorizados, alteraciones, pérdida de datos y otros riesgos de

seguridad. Se enfoca en la implementación de controles técnicos, como el uso de cifrado, autenticación, gestión de accesos, y copias de seguridad, para asegurar que la información permanezca confidencial, íntegra y disponible durante todo su ciclo de vida. Además, se destaca la importancia de documentar todos los accesos y las acciones para garantizar la trazabilidad y la posibilidad de auditorías.

2.3.2. UNE 17506:2013

La norma UNE 71506:2013 formalmente conocida como «Metodología para el análisis forense de las evidencias electrónicas» define los procesos para la captación, análisis, preservación, documentación, y presentación de e-evidencias, integrando también los métodos descritos en la norma UNE 71505.

En esta se establecen directrices y requisitos para asegurar la que el almacenamiento de información en sistemas de información y comunicaciones es seguro. Su objetivo es proteger los datos almacenados en dispositivos y medios digitales contra accesos no autorizados, alteraciones, pérdidas y otras amenazas de seguridad. La norma abarca medidas de protección como el cifrado de datos, autenticación de usuarios y gestión de accesos con el fin de garantizar la integridad, confidencialidad y disponibilidad de los datos. Además, establece pautas para la administración del ciclo de vida de las e-evidencias, desde su generación hasta su eliminación segura, e incluye consideraciones sobre la seguridad física y ambiental de los dispositivos de almacenamiento. También hace énfasis en la trazabilidad y la auditoría, resaltando la importancia de llevar un control minucioso, mediante registros detallados de todas las acciones realizadas vinculadas al almacenamiento de datos para garantizar el cumplimiento de las medidas instauradas. En conjunto, la UNE 71506:2013 proporciona un marco integral para asegurar la protección de la información almacenados a lo largo de su ciclo de vida.

2.3.3. UNE-EN ISO/IEC 27037:2016

Esta norma ratificada en diciembre de 2016 por AENOR y oficialmente conocida como «Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas» recopila los estándares actuales que establecen los procedimientos para la identificación, recopilación, adquisición y preservación de las pruebas digitales. Su objetivo es garantizar que las pruebas electrónicas sean gestionadas de manera efectiva y adecuada desde su identificación hasta su análisis final, manteniendo su integridad y validez en todo momento. La norma establece directrices para identificar las evidencias relevantes, preservarlas adecuadamente para evitar alteraciones, adquirir los datos de manera que se minimice el riesgo de modificación, y analizarlas meticulosamente para obtener conclusiones precisas. Además, enfatiza la importancia de documentar exhaustivamente todas las acciones realizadas durante el proceso, asegurando una cadena de custodia sólida y una presentación adecuada de las evidencias en contextos legales. En esencia, garantiza que la gestión de las evidencias electrónicas se realice

con el máximo profesionalismo y cuidado, facilitando su uso en investigaciones y procedimientos judiciales.

2.3.4. UNE-EN ISO/IEC 27042:2016

La norma conocida y ratificada como UNE-EN ISO/IEC 27042:2016 «Directrices para el análisis y la interpretación de las evidencias electrónicas» proporciona directrices esenciales para el análisis y la interpretación de las pruebas digitales en el ámbito de la informática forense. Establece una metodología rigurosa para el análisis de datos digitales, incluyendo la selección adecuada de herramientas y procesos para asegurar una evaluación exhaustiva y confiable. Además, contiene pautas sobre la interpretación de los datos analizados, subrayando la importancia de contextualizar estos hallazgos dentro del entorno de la investigación para garantizar conclusiones precisas y pertinentes. También especifica los requisitos para la documentación y reporte del proceso de análisis, asegurando que sea claro, detallado y accesible para las partes interesadas, como equipos legales o judiciales. Finalmente, la norma destaca la necesidad de validar y verificar los resultados para asegurar su exactitud y fiabilidad, incluyendo la posible replicación de análisis y la revisión por terceros.

2.3.5. RFC 3227

Los RFC (*Request for Comments*) son documentos que reúnen recomendaciones de expertos en un área específica, con el propósito de crear directrices para implementar procesos, desarrollar estándares o establecer protocolos. En este caso el RFC 3227, titulado «Directrices para la recopilación de evidencias y su almacenamiento», tal y como dice su nombre ofrece directrices detalladas para la captación y el almacenamiento de e-evidencias, asegurando su integridad y validez.

Este documento destaca la importancia de una preparación adecuada antes de comenzar la recolección, incluyendo el uso de herramientas aprobadas y la capacitación del personal. Durante la recolección, se debe seguir un procedimiento meticuloso para evitar la alteración de la información, documentando cada paso del proceso para permitir la revisión y validación posterior. La documentación completa es esencial para que las evidencias puedan ser utilizadas efectivamente en procedimientos legales, registrando toda la información relevante sobre la recolección y el contexto en el que se encontró la evidencia. El almacenamiento adecuado asegura que las evidencias se mantengan seguras y accesibles, protegiéndolas de daños o alteraciones.

Por último, el RFC 3227 subraya la importancia de mantener una cadena de custodia rigurosa para garantizar que la evidencia no sea contaminada ni manipulada, registrando detalladamente su movimiento y manipulación.

2.3.6. Otras normas relevantes

Aparte de las normas y estándares previamente mencionados, es importante tener en cuenta otros marcos regulatorios y directrices que también desempeñan un papel crucial en el proceso de gestión de evidencias electrónicas. Por lo que también son relevantes las normas descritas a continuación.

2.3.6.1. UNE-EN ISO/IEC 27040:2016

Esta norma es formalmente conocida como «UNE-EN ISO/IEC 27040:2016. Seguridad en el almacenamiento (ISO/IEC 27040:2015) (Ratificada por AENOR en diciembre de 2016.)». Se trata de un manual técnico detallado sobre cómo las empresas pueden establecer un nivel adecuado de reducción de riesgos usando un enfoque bueno y consistente para planificar, diseñar, documentar e implementar la seguridad del almacenamiento de información.

Proteger el almacenamiento implica proteger donde almacenan los datos y la información transferida. La protección del almacenamiento abarca la seguridad medios y dispositivos, actividades de gestión ligadas a los medios y dispositivos, servicios y aplicaciones, y la seguridad relevante para los usuarios finales a lo largo de la vida útil de dichos sistemas y medios, así como después de su uso.

Esto es relevante ya que mecanismos de seguridad, como la encriptación, pueden impactar en la capacidad para realizar una investigación al introducir mecanismos de ofuscación. Estos deben ser considerados antes y en el periodo de una investigación. También pueden resultar de importancia para asegurar que el almacenamiento del material probatorio durante y en el tiempo después de una investigación esté adecuadamente preparado y asegurado.

2.3.6.2. UNE-EN ISO/IEC 27041:2016

Ratificada por AENOR en diciembre de 2016, la norma UNE-EN ISO/IEC 27041:2016 (ISO/IEC 27041:2015) titulada «Directrices para garantizar la idoneidad y adecuación del método de investigación de incidentes» proporciona orientación sobre cómo asegurar que las técnicas y procedimientos cumplen con las necesidades de la investigación y han sido probados de manera apropiada. Es decir, se centra en ofrecer un marco para evaluar y validar la idoneidad de las técnicas empleadas durante las diversas fases que constituyen el proceso de gestión de evidencias electrónicas, garantizando que las pruebas digitales sean manejadas de manera confiable y que los resultados obtenidos sean consistentes y admisibles.

2.3.6.3. ISO/IEC 27035

El estándar ISO/IEC 27035 «*Information security incident management*» proporciona a las organizaciones un enfoque planificado y estructurado para gestionar incidentes de seguridad. Este está compuesto por tres partes:

- ISO/IEC 27035-1:2023. Parte 1: Principios y procesos. Esta parte describe los conceptos básicos y las fases que conforman la gestión de incidentes de seguridad en las tecnologías de la información. Además, combina estos conceptos con principios en un enfoque estructurado para la detección, documentación, evaluación, respuesta y aplicación de lecciones aprendidas.

- ISO/IEC 27035-2:2023. Parte 2: Directrices para planificar y preparar la respuesta al incidente. En esta parte se presentan los pasos necesarios para planificar y prepararse para la respuesta a incidentes. Estos incluyen establecer la política y el plan de gestión de incidentes, el establecimiento del equipo de respuesta a incidentes, y las sesiones de concienciación y capacitación, se basan en la fase de planificación y preparación del modelo presentado en ISO/IEC 27035-1. En esta parte también se cubre la fase de «Lecciones Aprendidas» del modelo.

- ISO/IEC 27035-3:2020 Parte 3: Directrices para las operaciones de respuesta a incidentes TIC. Esta parte incluye las actividades prácticas de respuesta a incidentes en toda la organización y las responsabilidades del personal. Se pone un enfoque particular en las tareas del equipo de respuesta, incluyendo la monitorización, detección y análisis de los datos recopilados o de los eventos de seguridad.

2.3.6.4. ISO/IEC 27050:2016

El estándar internacional ISO/IEC 27050 titulado «*Electronic discovery*» establece directrices y requisitos para trabajar con evidencias digitales. Este se divide en cuatro partes que cubren los aspectos fundamentales del proceso de *e-Discovery*, un término que hace referencia a la identificación, preservación, captación, análisis, y producción de información almacenada electrónicamente (ESI) para ser utilizada como evidencia en procesos legales o de auditoría.

Es de importancia tanto para el personal técnico como el personal no técnico involucrado en algunas o todas las actividades del descubrimiento electrónico, dado que este a menudo impulsa las investigaciones, así como las actividades de adquisición y tratamiento de pruebas.

2.4. Crítica al estado del arte

El desarrollo de una guía de gestión de evidencias electrónicas se justifica por la existencia de fallos, ineficacias y lagunas en la normativa y guías actualmente disponibles. Aunque existen diversas normas UNE que abordan la gestión de evidencias electrónicas, las pautas y directrices

se encuentran dispersas entre varias de ellas, lo que puede generar confusión entre los profesionales que deben seguir estos procedimientos. La falta de cohesión entre las normas puede llevar a que se pasen por alto pasos críticos o se produzcan inconsistencias en la forma en que se gestionan las evidencias. Esto pone en riesgo la integridad de las pruebas, lo cual es fundamental para garantizar que puedan ser utilizadas de manera efectiva en procesos judiciales. Además, la falta de una guía unificada que cubra los aspectos básicos del manejo de evidencia digital puede hacer que los profesionales con conocimientos menos avanzados se enfrenten a barreras innecesarias.

En cuanto a trabajos previos de fin de grado (TFG) relacionados con la gestión de evidencias electrónicas, se ha detectado que algunos se centran más en la descripción teórica del problema de los delitos informáticos que en la creación de herramientas prácticas para la recolección y gestión de la evidencia. Por ejemplo, el TFG creado por Jordi Magraner en el curso 2014-2015 documenta las dificultades para identificar, esclarecer e imputar delitos informáticos, analizando las características de los medios telemáticos para la comisión de estos delitos y el marco legal asociado. Se describe la informática forense en lo que respecta a la evidencia digital y el perfil del perito informático, pero aunque se proponen herramientas de apoyo, no se centra en guías prácticas aplicables por profesionales informáticos en general.

Otro TFG, el creado por Héctor Ruiz en el curso 2022-2023, tiene como objetivo la creación de una guía que permita a los profesionales informáticos crear informes de gestión tras la detección de delitos informáticos. Aunque esta propuesta es útil, sigue enfocada principalmente en la elaboración de informes, dejando de lado la fase concreta del manejo y preservación de la evidencia digital que se lleva a cabo en el campo, durante la investigación.

Por otro lado, guías internacionales como las elaboradas por INTERPOL, como sus «*Guidelines for Digital Forensics First Responders*» y «*Global Guidelines for Digital Forensics Laboratories*», están orientadas hacia la actuación policial, con un enfoque restringido a los cuerpos de seguridad y laboratorios forenses especializados. Aunque estas guías son sumamente valiosas, no son de fácil acceso o aplicación para profesionales de TI no vinculados directamente con cuerpos de seguridad o laboratorios forenses. No obstante, sirven de apoyo para la creación de la guía en el presente trabajo.

2.5. Propuesta

La propuesta de este trabajo se centra en la creación de una guía completa y accesible que detalle los pasos básicos necesarios para llevar a cabo la identificación, captación, análisis, preservación y presentación de evidencias digitales. A diferencia de otras guías existentes, que suelen estar dirigidas principalmente a cuerpos policiales o especialistas forenses altamente capacitados, esta guía está diseñada para que cualquier profesional de la informática con un conocimiento básico sobre evidencias electrónicas pueda utilizarla. Esto facilita la gestión de las partes más cruciales del proceso sin requerir una formación especializada en ciberseguridad o criminalística. A pesar de que ya existen guías y TFGs relacionados con la gestión de evidencias electrónicas, la mayoría se centran en el estudio de cibercrímenes o en la redacción de informes, pero no abordan el proceso concreto de manejo de evidencias. La guía desarrollada en este

proyecto cubre esos aspectos fundamentales y prácticos, proporcionando una herramienta única y necesaria que puede ser utilizada tanto en el ámbito profesional como en el académico.

3. ANÁLISIS DEL PROBLEMA

Si un profesional de la informática con un conocimiento básico sobre evidencias electrónicas debe, en algún momento de su carrera, participar en alguna fase del proceso de gestión de evidencias electrónicas y, a su vez, quiere asegurarse de que completa todos los pasos acorde a la normativa actual, puede encontrarse con alguno de los siguientes problemas:

- **Estandarización de procedimientos**

Como se ha visto en el punto 2.3., en el ámbito normativo español existen varias normas que tratan especialmente sobre las evidencias electrónicas. El principal problema es que no todas ellas contienen todos los pasos necesarios. De hecho en la mayoría de ellas solamente se tratan aspectos parciales del proceso. Por otra parte, algunas al ser estándares ISO ratificados por AENOR, no están traducidas al castellano, lo que puede crear confusión en cuanto al entendimiento de algunos término técnicos. Este tipo de confusiones podría resultar en prácticas ineficaces, invalidar el valor probatorio de las evidencia o incluso llevar a la pérdida de información crucial. Esto también puede llevar a inconsistencias en la forma en que las evidencias son tratadas.

- **Cumplimiento de normativas legales**

Debido a la dispersión de los aspectos fundamentales del proceso de gestión de evidencias digitales entre las diferentes normas, algunos de estos pueden incluso llegar a omitirse. Si añadimos esto al hecho de que la gestión de evidencias electrónicas está sujeta a una serie de normativas legales y estándares que deben cumplirse para que las evidencias sean admitidas en procedimientos judiciales, el incumplimiento de estas puede invalidar la evidencia y perjudicar la prosecución de algunos casos.

- **Pérdida o alteración de datos**

Los datos digitales son susceptibles a ser alterados o perdidos debido a errores humanos, fallos técnicos o problemas de seguridad. Sin una guía adecuada, los profesionales pueden enfrentar dificultades para proteger adecuadamente la integridad de la evidencia.

- **Capacitación y desarrollo profesional**

La falta de capacitación específica en la gestión de evidencias electrónicas puede llevar a una falta de competencia en el manejo de herramientas forenses, técnicas de análisis y procedimientos adecuados, afectando la eficacia del análisis forense.

- **Falta de comunicación y documentación**

La gestión de evidencia electrónica a menudo implica múltiples partes interesadas y etapas del proceso. La falta de documentación clara y comunicación efectiva puede llevar a malentendidos, errores y dificultades para presentar evidencia en contextos legales.

- **Adaptación a nuevas tecnologías y desafíos**

La tecnología está en constante evolución, lo que presenta nuevos desafíos y herramientas en el campo de la informática forense. Los profesionales pueden tener dificultades para mantenerse al día con estos cambios sin una guía actualizada.

3.1. Análisis del marco legal y ético

El cumplimiento de la Ley de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD) es crucial en la gestión de evidencias electrónicas porque garantiza que el tratamiento de datos personales se realice de manera legal, ética y segura, protegiendo los derechos fundamentales de los individuos involucrados. En investigaciones forenses, se manejan datos sensibles que, si no son tratados correctamente, pueden resultar en violaciones de la privacidad, vulneración de derechos o comprometer la validez de las evidencias. La Ley asegura que se mantenga la confidencialidad, integridad y legalidad en el ciclo de vida de las evidencias, evitando sanciones y asegurando la legitimidad del proceso judicial.

Aspectos clave a destacar son:

- Asegurarse de que la guía respete principios como la legalidad, minimización de datos y limitación de propósito (Art. 5 LOPDGDD). La captación y el tratamiento de los datos deben alinearse con estos principios.

- Se deben establecer procedimientos para garantizar los derechos de acceso, rectificación, cancelación y oposición (Art. 15-18 LOPDGDD). Se deben definir mecanismos para permitir a los interesados ejercer estos derechos sobre sus datos. No obstante, también pueden haber restricciones de dichos derechos dependiendo de las circunstancias de la investigación, como también se indica en la ley.

- La guía debe contemplar medidas técnicas y organizativas adecuadas para la seguridad del tratamiento de datos (Art. 32 LOPDGDD), protegiendo la información de accesos no autorizados y alteraciones.

Otra ley aplicable es la Ley de Enjuiciamiento Criminal (LECrim) en España, y la normativa específica sobre informática forense. Estos se centran en la admisibilidad de las pruebas y en los procedimientos legales a cumplir. Por lo que la guía creada debe seguir las directrices para el tratamiento y captación de evidencias para asegurar que sean admisibles en procedimientos judiciales. Esto incluye la preservación de la cadena de custodia y la documentación adecuada de la evidencia. Además se debe cumplir con los procedimientos legales para la obtención de datos, como la obtención de órdenes judiciales si es necesario para acceder a ciertas evidencias.

La gestión de evidencias electrónicas está bastante ligada con la ciberseguridad, por lo que también podemos hablar de Ley de Seguridad Nacional y Ley de Protección de Infraestructuras Críticas en España. Estas tratan la protección contra amenazas, en nuestro caso contra las amenazas a la integridad y seguridad de las evidencias. Por esto la guía debe incluir medidas para proteger la evidencia digital contra amenazas cibernéticas y garantizar su integridad durante el proceso de recolección y análisis acorde con estas leyes.

En cuanto al marco internacional, nos centramos en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Este es una versión un poco más general de la LOPDGDD española, aunque un aspecto fundamental de este reglamento es que trata las transferencias de información a nivel internacional. Pues si la evidencia se transfiere a través de fronteras, la guía debe contemplar las normativas sobre transferencias internacionales de datos para asegurar el cumplimiento con el RGPD.

El marco ético en la gestión de evidencias electrónicas establece los principios y valores fundamentales que guían el comportamiento profesional en este ámbito. Dada la naturaleza sensible de los datos involucrados, es crucial garantizar la integridad, confidencialidad y respeto por los derechos de las personas implicadas. Este marco promueve la transparencia, la imparcialidad y el cumplimiento de las normativas legales, asegurando que los profesionales actúen con responsabilidad, discreción y honestidad, además de mantener altos estándares de profesionalidad y respeto por la privacidad y la dignidad humana durante todo el proceso de manejo y análisis de las evidencias.

En los siguientes puntos se hablara sobre cómo el desarrollo de una guía de gestión de evidencias electrónicas requiere una consideración exhaustiva del marco legal y ético. Legalmente, debe alinearse con la LOPDGDD, la legislación sobre informática forense, y normativas internacionales de protección de datos. Éticamente, debe garantizar la confidencialidad, integridad, y responsabilidad en el manejo de datos. Incorporar estos aspectos asegura que la guía no solo cumpla con las exigencias legales, sino que también promueva prácticas éticas que protejan la privacidad y los derechos de los individuos, y mantengan la integridad del proceso forense.

3.1.1. Análisis de protección de datos

En el ámbito internacional encontramos el Reglamento General de Protección de Datos (RGPD). Este regula el tratamiento de datos personales dentro de la Unión Europea y su transferencia hacia otros países. Cuando las evidencias digitales contienen datos personales, como información de usuarios o registros de actividades, por lo que los responsables deben asegurarse de que se cumplan las normativas del RGPD. Esto incluye obtener el consentimiento adecuado para el tratamiento de los datos o garantizar que las transferencias internacionales se realicen solo con países que ofrezcan un nivel adecuado de protección.

Sin embargo, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) es el marco legal que regula el tratamiento de datos personales en España, en consonancia con el anteriormente mencionado RGPD de la UE. Una guía de apoyo para la gestión de evidencias electrónicas tiene el potencial de influir significativamente en la protección de datos personales, especialmente cuando se maneja información sensible en investigaciones forenses. Por esto se deben tener en cuenta las disposiciones de esta ley para garantizar el tratamiento adecuado de los datos personales y salvaguardar los derechos de los individuos. A continuación, se detalla cómo la creación de una guía afectaría a la protección de datos, aplicando directamente la normativa de la LOPDGDD.

- **Principio de Transparencia y Derecho de Información (Artículos 13 y 14 de la LOPDGDD)**

Durante el proceso de gestión de evidencias electrónicas se debe especificar cómo el profesional debe cumplir con el deber de informar a los interesados sobre el tratamiento de sus datos personales, incluso en el contexto de una investigación forense. Aunque en algunos casos la investigación puede implicar la restricción de este derecho (por razones de seguridad, confidencialidad o integridad de la investigación).

Por ejemplo, se debe asegurar que cualquier recogida de datos personales en el proceso de investigación cumpla con el deber de informar, cuando proceda, o se contemple la posibilidad de excepciones legales, como ocurre en el tratamiento de datos para la prevención, investigación o enjuiciamiento de infracciones penales (art. 23 del RGPD y art. 22 de la LOPDGDD).

Tal y como dice el artículo 13 de esta ley, «El responsable del tratamiento, en el momento de la obtención de los datos personales, facilitará al interesado la siguiente información: [...] la existencia del tratamiento de datos personales, la identidad del responsable, los fines del tratamiento y las bases jurídicas para dicho tratamiento.»

- **Legitimación del Tratamiento (Artículo 6 de la LOPDGDD)**

El artículo 6 de la LOPDGDD trata sobre las bases que legitiman el tratamiento, como en los casos de investigaciones penales o la preservación de evidencias en juicios, donde los responsables pueden justificar el acceso a datos personales sin necesidad de consentimiento. «El tratamiento será lícito cuando sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.». Por lo que los profesionales deben comprender las bases legales que permiten la captación y análisis de datos.

- **Minimización de Datos y Proporcionalidad (Artículo 4 de la LOPDGDD)**

El principio de minimización de datos (art. 5 del RGPD y art. 4 de la LOPDGDD) implica que solo se recojan y procesen los datos estrictamente necesarios para el fin de la investigación. En el artículo 4 se dice claramente que «Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.». La guía tiene que establecer procedimientos claros para que los profesionales recojan únicamente los datos relevantes y necesarios para la investigación forense, evitando la recopilación de información irrelevante o excesiva. Esto no solo ayuda a cumplir con las disposiciones del artículo 4 de la LOPDGDD, sino que también reduce el riesgo de vulneraciones de la privacidad de los afectados.

- **Cadena de Custodia y Protección de Datos (Artículos 32 y 34 de la LOPDGDD)**

El artículo 32, reforzado por el art. 34 de la LOPDGDD, exige que se implementen medidas técnicas y organizativas adecuadas para garantizar la seguridad del tratamiento, incluyendo la

protección contra el acceso no autorizado, la alteración o la destrucción de datos personales. La guía debe incluir protocolos que garanticen la cadena de custodia de las evidencias electrónicas, asegurando que los datos personales se manejen de manera segura y que se mantenga su integridad durante todo el proceso. Por ejemplo, la guía podría incluir el uso de medidas como el cifrado u otras técnicas de seguridad para proteger los datos mientras se procesan y almacenan, asegurando el cumplimiento de las obligaciones de seguridad establecidas por la ley.

El mantenimiento de la cadena de custodia es esencial para asegurar la integridad y autenticidad de las evidencias electrónicas. Según los artículos 32 y 34 de la LOPDGDD, «El responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluidas, entre otras: [...] cifrado de datos personales; y medios para garantizar la confidencialidad, integridad y disponibilidad continuas de los sistemas y servicios.». Esto incluye proteger los datos personales contra accesos no autorizados, alteración, destrucción o pérdida.

- **Derechos de los Interesados (Artículos 13 a 18 de la LOPDGDD)**

Los derechos de los interesados recogidos en los artículos 13 al 18 de la LOPDGDD, como el derecho de acceso, rectificación, supresión, y oposición, deben ser considerados en la guía, aunque se reconoce que en ciertos contextos forenses, algunos de estos derechos pueden ser limitados por razones justificadas. La LOPDGDD, en su artículo 23, permite limitaciones a estos derechos siempre y cuando estén justificadas y sean proporcionales.

En los casos donde el ejercicio de estos derechos no interfiera con la investigación, los profesionales deben estar preparados para responder a solicitudes de acceso o rectificación de datos, respetando los plazos y procedimientos establecidos por la ley.

- **Transferencias Internacionales de Datos (Artículo 40 de la LOPDGDD)**

En el contexto de investigaciones que implican colaboración internacional o recolección de evidencias de servidores ubicados fuera de la Unión Europea, la transferencia internacional de datos puede ser un desafío. Por esta razón, los requisitos legales para la transferencia de datos a terceros países fuera de la UE los podemos encontrar en el artículo 40 de la LOPDGDD, que establece que «Las transferencias de datos personales a un tercer país u organización internacional solo se realizarán si el tercer país u organización internacional garantiza un nivel de protección adecuado.». Este artículo es una ampliación del artículo 44 del RGPD, que establece reglas estrictas sobre las transferencias de datos fuera del Espacio Económico Europeo, lo que puede implicar procedimientos adicionales de seguridad y autorización.

El profesional forense debe estar informado de las condiciones bajo las cuales los datos pueden ser transferidos legalmente y cómo documentar adecuadamente estas transferencias para mantener la legalidad de la investigación.

- **Ética y Buenas Prácticas (Artículo 89 de la LOPDGDD)**

La gestión de evidencias electrónicas no solo tiene un componente técnico y legal, sino también un profundo compromiso ético. El artículo 89 de la LOPDGDD establece que cualquier tratamiento de datos personales con fines de investigación debe observar principios éticos, como la honestidad, la transparencia, la responsabilidad y la proporcionalidad. Es decir, «El tratamiento de datos personales con fines de archivo en interés público, investigación científica o histórica o fines estadísticos estará sujeto a garantías adecuadas, de conformidad con el Reglamento (UE) 2016/679 [...] para proteger los derechos y libertades del interesado.». Además, se debe destacar la importancia de aplicar siempre las mejores prácticas en el manejo de los datos personales para minimizar cualquier riesgo de violación de los derechos fundamentales de las personas afectadas.

3.1.2. Otros aspectos legales

Las evidencias digitales deben cumplir con ciertos requisitos para ser aceptadas en un tribunal. Esto incluye asegurar que la recolección de la evidencia siga un procedimiento legal adecuado y que se preserve la integridad de los datos. Por ejemplo, la Ley de Enjuiciamiento Criminal (LECrim) de España establece que las pruebas deben ser obtenidas de manera lícita y sin vulnerar derechos fundamentales. Cualquier manipulación indebida o falta de cadena de custodia puede hacer que la evidencia sea inadmisible en juicio. En algunos casos, la obtención de datos digitales, como la información almacenada en dispositivos o redes, puede requerir órdenes judiciales. Las leyes de enjuiciamiento criminal y otras normativas específicas establecen los procedimientos a seguir para obtener datos almacenados o en tránsito, como correos electrónicos, registros de actividad de internet, o datos almacenados en la nube. En este sentido, la ley garantiza que cualquier adquisición de datos que implique la intervención en la privacidad de un individuo cumple con los requisitos de proporcionalidad y necesidad.

La Ley de Enjuiciamiento Civil regula las pericias en relación con la prueba tradicional en el Libro II, Capítulo V. Asimismo, en la Sección VIII del Capítulo VI, titulada «De la reproducción de la palabra, el sonido y la imagen y de los instrumentos que permiten archivar y conocer datos relevantes para el proceso», se incluyen los «nuevos medios de prueba». Finalmente, aunque no se mencione específicamente la prueba electrónica, se observa en el texto de la LEC una aplicación analógica de las normativas que regulan la prueba clásica.

También resulta aplicable la Ley 34/2002 de Servicios de la Sociedad de la Información, junto con la Ley 6/2020 que regula ciertos aspectos de los servicios electrónicos de confianza. Esta última, en su artículo 3, establece que «los documentos electrónicos públicos, administrativos y privados poseen el valor y eficacia jurídica correspondientes a su naturaleza, de acuerdo con la legislación aplicable». De esta manera, se reconoce la validez de los soportes electrónicos y se admite su uso como pruebas documentales en los procesos legales.

Por otro lado, la Ley 25/2007 sobre la conservación de datos relacionados con las comunicaciones electrónicas y las redes públicas de comunicaciones, establece en su artículo 3 los datos que deben ser preservados por los operadores de servicios de comunicaciones

electrónicas. Estos datos son esenciales para poder rastrear e identificar tanto el origen como el destino de una comunicación.

La regulación sobre ciberseguridad establece las normativas y estándares para la protección de las infraestructuras digitales y la gestión de incidentes de seguridad. Estas regulaciones son fundamentales en la gestión de evidencias electrónicas, ya que la preservación, análisis y adquisición de estas evidencias está estrechamente vinculada a la seguridad de los sistemas digitales.

La Ley de Protección de Infraestructuras Críticas establece las medidas necesarias para proteger las infraestructuras críticas del país, incluidas las TIC. La regulación impone medidas estrictas para la seguridad y protección de los sistemas que manejan datos sensibles, como en el sector de energía, telecomunicaciones, y sistemas financieros. La gestión de evidencias electrónicas dentro de este contexto debe respetar los protocolos de ciberseguridad establecidos para evitar accesos no autorizados o la alteración de datos críticos.

También en el ámbito de la ciberseguridad, la Ley de Seguridad Nacional establece un marco para coordinar las acciones necesarias para la protección frente a amenazas que afecten la seguridad de los sistemas nacionales, incluyendo incidentes cibernéticos. Esta fomenta una estrategia conjunta en la prevención, respuesta y recuperación de ataques cibernéticos, lo cual es crucial en el manejo de evidencias electrónicas relacionadas con cibercrimen o ataques a infraestructuras críticas.

Las normas españolas, como las mencionadas en el punto 2.3. establece directrices sobre cómo gestionar y proteger los sistemas informáticos y, a su vez, las evidencias electrónicas. Además, la Directiva NIS (*Network and Information Systems Directive*) de la UE exige que los operadores de servicios esenciales y proveedores de servicios digitales cumplan con requisitos específicos de ciberseguridad, por lo que la evidencia digital debe ser gestionada dentro de este marco para proteger la integridad y seguridad de los sistemas afectados.

Las investigaciones que involucran evidencia electrónica también pueden tener un alcance internacional, lo que exige un marco normativo que permita la cooperación entre jurisdicciones y regule la transferencia transfronteriza de datos.

El Convenio de Budapest sobre Cibercriminalidad es el principal instrumento a nivel mundial para abordar los delitos cibernéticos y regula la cooperación internacional en la investigación y enjuiciamiento de delitos digitales. Proporciona un marco legal para la cooperación transfronteriza y el intercambio de evidencias electrónicas entre países signatarios. La guía de gestión de evidencias electrónicas debe cumplir con los requisitos del Convenio de Budapest, asegurando que cualquier evidencia obtenida en una jurisdicción sea manejada y transferida de manera que cumpla con las leyes tanto locales como internacionales.

3.1.3. Ética

La ética juega un papel fundamental en la gestión de evidencias electrónicas, ya que las acciones realizadas por los profesionales en este campo pueden tener consecuencias directas en

los derechos individuales, la privacidad, la justicia y la confianza en las instituciones. Al crear una guía para la gestión de evidencias electrónicas, se deben tener en cuenta varios principios éticos que aseguren que las investigaciones y el manejo de la evidencia se realicen de manera responsable y con respeto a los derechos humanos.

Uno de los principios éticos clave en la gestión de evidencias electrónicas es la integridad. Esto implica que los profesionales deben actuar con honestidad y transparencia en todas las etapas del proceso forense, desde la recolección de la evidencia hasta su presentación en un tribunal. La manipulación, alteración o destrucción intencionada de estas va en contra de este principio y puede afectar gravemente la justicia. Además, los profesionales deben asegurarse de que las evidencias digitales que se recolecten sean fieles al original, preservando su integridad para evitar alteraciones que puedan falsear los hechos investigados. Esto incluye una correcta cadena de custodia y la aplicación de técnicas forenses que garanticen que la información no se corrompa. Asimismo, el personal encargado debe asumir la responsabilidad de sus acciones en todo momento. Si se comete un error, debe informarse a las autoridades competentes y tomar medidas correctivas, en lugar de intentar encubrirlo.

La imparcialidad también es esencial en las investigaciones forenses digitales. Los profesionales deben mantenerse objetivos y libres de prejuicios durante todo el proceso de manejo de la evidencia. Cualquier sesgo personal, presión externa o conflicto de intereses puede comprometer la investigación y perjudicar la justicia. Por lo que es crucial que el investigador mantenga una postura neutral, sin favorecer ninguna parte en particular, asegurando que las conclusiones se basen únicamente en la evidencia disponible, no en opiniones o intereses externos. Además, se deben evitar los conflictos de interés. Los profesionales deben estar atentos a cualquier situación que pueda comprometer su capacidad para realizar su trabajo de manera imparcial. Si surge un conflicto de intereses, deben abstenerse de participar en la investigación o notificar a sus superiores para que tomen las medidas adecuadas.

La gestión de evidencias electrónicas puede involucrar datos sensibles y privados, como información personal, financiera o confidencial de individuos u organizaciones. Por ello, la confidencialidad es un principio ético esencial que debe ser respetado en todo momento. Los profesionales deben manejar la evidencia de manera que respete la privacidad de los individuos no involucrados en el caso. Por ejemplo, al revisar los dispositivos electrónicos, deben centrarse en la información relevante para la investigación y evitar la exposición innecesaria de otros datos personales. Asimismo, los profesionales forenses solo deben compartir información sobre la evidencia digital con personas autorizadas. Cualquier divulgación indebida puede dañar la investigación, afectar la privacidad de las personas involucradas y tener implicaciones legales.

Otro de los principios éticos claves en la gestión de evidencias electrónicas es el principio de justicia, que dicta que las acciones de los profesionales deben estar orientadas a promover la equidad y el cumplimiento de la ley. Este principio implica que la evidencia digital debe ser gestionada de una manera que permita su uso en el proceso judicial de manera justa para todas las partes involucradas. Esto quiere decir que todas las partes en una investigación o proceso judicial deben tener un acceso justo a la evidencia. Lo que significa que los profesionales no deben suprimir, ocultar o manipular ninguna evidencia, ya que esta podría ser relevante para la defensa o la acusación. Por otra parte, los profesionales deben estar atentos a proteger los derechos fundamentales de todas las personas afectadas por la investigación. Esto incluye evitar

actuaciones que puedan afectar la presunción de inocencia, así como garantizar que la evidencia recolectada se maneje conforme a los procedimientos legales establecidos.

El profesionalismo exige que los expertos forenses se mantengan actualizados sobre los desarrollos en su campo y actúen con la máxima competencia y ética profesional en todo momento. La gestión de evidencias electrónicas requiere una serie de habilidades técnicas complejas, pero también un alto grado de autodisciplina y compromiso. Dado que las tecnologías evolucionan rápidamente, los profesionales deben comprometerse con una formación continua y mantenerse al día con las nuevas técnicas, herramientas y normativas legales. No hacerlo podría poner en riesgo la validez de la evidencia recolectada. Asimismo, los expertos deben actuar con la máxima diligencia al recolectar, analizar y preservar la evidencia electrónica, asegurándose de que su trabajo resista el escrutinio en un entorno judicial, ya que la falta de cuidado o precisión puede resultar en la pérdida de alguna evidencia crítica, lo que puede comprometer el caso.

Por último, la transparencia en el proceso es crucial para garantizar que todas las acciones realizadas durante la gestión de evidencias electrónicas puedan ser auditadas y verificadas. La transparencia permite a las partes implicadas en un caso revisar y validar el trabajo realizado. Esto no solo fortalece la credibilidad de los profesionales, sino que también protege la integridad del proceso judicial. Por lo que es fundamental que cada paso en la gestión de las evidencias electrónicas esté documentado de manera clara y detallada. Esto incluye registrar los métodos utilizados, las herramientas aplicadas y cualquier intervención realizada sobre la evidencia. Los profesionales deben estar preparados para justificar las decisiones que toman durante la recolección, preservación y análisis de la evidencia. Cada intervención sobre la evidencia debe tener una razón válida y estar alineada con los principios éticos y las normativas legales.

3.2. Análisis de riesgos

El análisis de riesgos aplicado a la gestión de evidencias electrónicas es un proceso fundamental que permite identificar, evaluar y mitigar posibles amenazas que puedan comprometer la integridad, confidencialidad y disponibilidad de las evidencias durante su recolección, almacenamiento, análisis y presentación en un proceso legal. Dado que las evidencias electrónicas son extremadamente sensibles y pueden verse afectadas por una variedad de riesgos, como la alteración de los datos, accesos no autorizados o la degradación por factores ambientales, es crucial implementar un enfoque sistemático para prever y minimizar estos riesgos.

Este análisis incluye la identificación de los posibles puntos de fallo en cada fase del proceso de manejo de evidencias. Además, implica evaluar las vulnerabilidades de los sistemas y herramientas utilizadas, así como las amenazas externas, como ciberataques o fallos en la cadena de custodia. Con una evaluación adecuada de riesgos, los profesionales pueden diseñar estrategias efectivas para proteger la evidencia electrónica, asegurando que sea admisible en un juicio y manteniendo su valor probatorio.

3.2.1. Evaluación de riesgos

El encargado de recolectar las evidencias electrónicas debe tener cuidado al usar una herramienta específica para recolectar o adquirir posibles evidencias digitales. No calcular los riesgos antes de actuar puede llevar a la pérdida de algunas o todas las evidencias digitales potenciales debido a la tecnología aplicada durante la recolección o adquisición. Por esa razón, cuando estamos realizando la identificación de las evidencias se deben evaluar los riesgos que pueden surgir en la recolección para reducir los potenciales daños.

La evaluación de riesgos implica la evaluación sistemática de los riesgos y el impacto potencial que estos pueden tener en la investigación de evidencias digitales. Podemos usar, por ejemplo, el siguiente formulario, que puede servir como plantilla, de los aspectos a considerar durante la evaluación de riesgos para evidencias digitales.

NOTA: En la Figura 4 se encuentran los aspectos básicos a considerar, pero se podrían añadir más.

Evaluación de Riesgos		
Identificador de Evidencia		
Nivel de volatilidad	◯ Volátil	
	◯ No volátil	
Nivel de relevancia	1 2 3 4 5 6 7 8 9 10 ◯ ◯ ◯ ◯ ◯ ◯ ◯ ◯ ◯ ◯ Muy relevante — Poco relevante	
Método de Captación		
Justificación		
Equipamiento especial necesario		
Existe acceso remoto a la evidencia?	◯ Sí	Dispositivos:
	◯ No	
Solución si el dispositivo se daña		
Indicios de que los datos están comprometidos		

Indicios de que el dispositivo está configurado para destruir, deteriorar u ofuscar datos	

Figura 4. Plantilla para la evaluación de riesgos.

Fuente: Elaboración propia.

3.2.2. Usar cuidado razonable

Cuando estamos tratado con e-evidencias es imprescindible prevenir cualquier acción, intencionada o accidental, que pueda alterarlas. Por ejemplo, la exposición a campos magnéticos puede dañar la e-evidencia contenida en medios de almacenamiento magnético. El personal responsable no debe manipular los dispositivos electrónicos, por ejemplo para efectuar un volcado de memoria de un sistema activo, si no posee las competencias necesarias y emplea procedimientos confiables y validados.

Existen algunas circunstancias en las que es impráctico realizar la adquisición de una evidencia electrónica. El responsable debe considerar las siguientes circunstancias, pero también debe tener en cuenta que no solamente se limita a estos casos:

- Si no hay derecho legal o autorización para la adquisición del dispositivo digital.
- Si existe una obligación de utilizar otros métodos (por ejemplo, para evitar interrumpir un negocio).
- Si se quiere determinar cómo algún implicado opera durante la explotación indebida de un sistema.
- Cuando se trata de un sistema crítico el cual no puede estar inactivo en ningún momento.
- Cuando el dispositivo digital tiene un tamaño físico demasiado grande, como es el caso de un sistema RAID o de un servidor en un centro de datos.
- Si es un sistema crítico para la seguridad que pondría en peligro vidas si se detiene.
- Si es un dispositivo digital que también da servicio a partes inocentes.

3.3. Identificación y análisis de soluciones posibles

En la gestión de evidencias electrónicas, los problemas identificados giran en torno a la falta de claridad y coherencia en la aplicación de las normativas existentes. Para abordar estos desafíos, se presentan dos soluciones posibles, cada una con sus respectivas ventajas y desventajas.

3.3.1. Mantener el enfoque actual

Esta solución implica continuar utilizando las diferentes normativas vigentes, aplicables a la gestión de evidencias electrónicas, pero sin unificar estas regulaciones en un único documento o guía. En este enfoque, los profesionales deberán seguir consultando las diferentes normas UNE, buscando cual es la más adecuada para cada caso e incluso para cada fase del proceso de gestión de evidencias digitales. Cada una de estas normas regula aspectos específicos, como la cadena de custodia de la evidencia, la protección de datos y la validez de pruebas digitales.

La principal ventaja de este enfoque es que no hay que invertir más tiempo ni dinero en crear una solución acorde a la normativa, ya que estamos hablando de las normas en sí. Al manejar múltiples normativas, los profesionales pueden adaptar su enfoque según la especificidad del caso, el tipo de evidencia o incluso la fase del proceso de gestión de evidencias electrónicas que se vaya a abordar. Además, permite una mayor especialización en áreas concretas del manejo de evidencias, lo que puede ser útil en situaciones complejas que requieren un enfoque particular para ciertos aspectos como ciberseguridad o protección de datos. Al operar dentro de leyes ya establecidas, este enfoque también garantiza que el profesional cumpla con el marco legal vigente, evitando el riesgo de saltarse regulaciones actualizadas.

Sin embargo, este enfoque presenta varias desventajas. La mayor de ellas es la fragmentación de la información. Tener que recurrir a múltiples marcos normativos puede generar confusión, aumentar las posibilidades de omisiones de información y llevar a errores que comprometan la integridad y, por lo tanto, la validez de la evidencia. También existe el riesgo de dificultades en la interpretación, ya que no siempre está claro cómo las diferentes normativas se aplican en conjunto, especialmente en situaciones nuevas o complejas. Esto puede llevar a mayores costos de tiempo y esfuerzo, ya que los profesionales deberán invertir más en investigar y comprender las normativas aplicables a cada caso.

3.3.2. Crear una guía unificada para la gestión de evidencias electrónicas

La segunda solución consiste en desarrollar una guía integral que unifique todas las normativas relevantes en un único documento. Esta guía proporcionaría un conjunto de procedimientos estandarizados y alineados con las leyes actuales, cubriendo todas las etapas de la gestión de evidencias electrónicas, desde su identificación y recolección hasta su preservación y presentación ante un tribunal. El objetivo de esta guía sería ofrecer un recurso claro y accesible

que permita a los profesionales seguir un conjunto coherente de pasos, garantizando así el cumplimiento normativo y protegiendo la validez de las pruebas.

Una de las principales ventajas de esta solución es la claridad y coherencia que aportaría al proceso de gestión de evidencias. Al tener todos los procedimientos básicos reunidos en una única guía, los profesionales tendrían menos probabilidades de cometer errores o de saltarse pasos cruciales. También permitiría una estandarización de los procedimientos, lo que garantizaría un enfoque más uniforme en todas las situaciones y facilitaría la capacitación de nuevos profesionales. Además, esto podría reducir el tiempo y esfuerzo invertido en la búsqueda de normativas y su interpretación, ya que toda la información relevante estaría centralizada en un solo documento.

Por otro lado, una guía unificada podría ser vista como demasiado básica o general, limitando la capacidad de los profesionales para adaptarse a situaciones específicas que no encajen perfectamente dentro de los procedimientos estandarizados. Además, dicha guía requeriría una actualización constante para asegurarse de que siempre esté alineada con las leyes más recientes, lo que podría convertirse en un proceso costoso y complicado. Si la guía no se mantiene actualizada, podría incluso perder su utilidad, generando problemas de cumplimiento y exponiendo a los profesionales a riesgos legales. Finalmente, el costo inicial de desarrollar esta guía sería elevado, ya que se deberían estudiar las leyes aplicables antes de proceder a su creación para así asegurarse de que realmente cumple con la normativa establecida.

3.4. Solución propuesta

Ambas soluciones presentan ventajas y desventajas. Mientras que mantener las normativas dispersas permite estar actualizado en todo momento, también aumenta el riesgo de confusión y errores en la aplicación. Por otro lado, una guía unificada aportaría claridad y estandarización, pero podría requerir de actualizaciones constantes. Sin embargo y a pesar de su mayor coste inicial, esta segunda opción es la más óptima ya que una sola guía que recoja los procedimientos básicos para la captación, preservación y análisis de evidencias electrónicas sería de gran ayuda para los profesionales.

La guía proporciona un marco claro para cumplir con los requisitos legales pertinentes. Incluye directrices sobre cómo mantener la cadena de custodia, gestionar la evidencia de acuerdo con las leyes y regulaciones vigentes, y cómo documentar adecuadamente cada paso del proceso. Esto asegura que la evidencia digital sea manejada de manera que mantenga su validez en procedimientos judiciales.

Esta también detalla las mejores prácticas para proteger la evidencia digital durante su recolección, preservación y análisis. Incluye instrucciones sobre el uso de herramientas adecuadas, técnicas de preservación y medidas de seguridad para proteger la evidencia contra daños físicos, alteraciones y pérdidas. Esto minimiza el riesgo de comprometer la integridad de los datos.

Además puede servir como una herramienta de formación y referencia para los profesionales al proporcionar información sobre el uso de *software* y *hardware* forense, técnicas de análisis y

métodos de recolección de evidencia. Esto facilita la capacitación continua y el desarrollo de habilidades entre los profesionales, asegurando que estén actualizados con las mejores prácticas y tecnologías emergentes.

Por último, la guía ofrece directrices sobre cómo documentar de manera efectiva cada paso del proceso de gestión de evidencias electrónicas. Esto incluye la creación de informes claros, la gestión de registros y la comunicación de hallazgos de manera comprensible. Una documentación y comunicación bien estructuradas facilitan la colaboración entre equipos y la presentación efectiva de la evidencia en procedimientos judiciales.

3.5. Plan de trabajo

El plan de trabajo se diseñó con una duración total de 280 horas, distribuidas en 35 jornadas de ocho horas cada una. Desde un principio, el objetivo fue organizar las tareas de manera eficiente para cumplir con los plazos establecidos. El proyecto se dividió en una serie de actividades clave: la búsqueda de información actualizada sobre evidencias electrónicas, el estudio de las leyes relacionadas, el análisis de la normativa vigente, la investigación de guías especializadas y el estudio de estas, para finalmente proceder con la redacción de la guía final. Paralelamente, se planificó la redacción de la memoria del TFG, que sería desarrollada en conjunto con las demás tareas.

TAREA	Comienzo planeado	Duración planeada	Comienzo	Duración
Búscar información actual sobre evidencias electrónicas	1	4	1	4
Estudiar las leyes relacionadas	4	6	4	5
Estudiar la normativa vigente	4	7	7	8
Búscar guías especilizadas	10	2	14	2
Estudiar las guías especializadas	12	7	15	7
Redacción de la guía	19	15	21	17
Redacción de la memoria	4	32	6	35

Figura 5. Actividades planificadas y su duración real.

Fuente: Elaboración propia.

Durante la fase inicial del proyecto, las dos primeras tareas, que consistían en la búsqueda de información actual y el estudio de las leyes relacionadas con las evidencias electrónicas, se completaron según lo planificado, sin desviaciones en el cronograma. Sin embargo, a medida que se avanzaba en el análisis de la normativa vigente, surgieron complicaciones que provocaron un retraso. La razón principal de este retraso fue la gran cantidad de normas que podían estar vinculadas, de una forma u otra, con la gestión de evidencias electrónicas. Este factor no se había

considerado completamente durante la planificación inicial, lo que generó una acumulación de trabajo en esta etapa.

El retraso experimentado en la fase de estudio de la normativa se arrastró hacia las etapas finales del proyecto, afectando la redacción de la guía y de la memoria del TFG. Ambas actividades resultaron ser considerablemente más intensivas en cuanto a tiempo y recursos, lo que exacerbó el desajuste en el cronograma. La redacción de la guía final, en particular, requirió una mayor atención al detalle y revisión, lo que consumió más horas de las previstas.

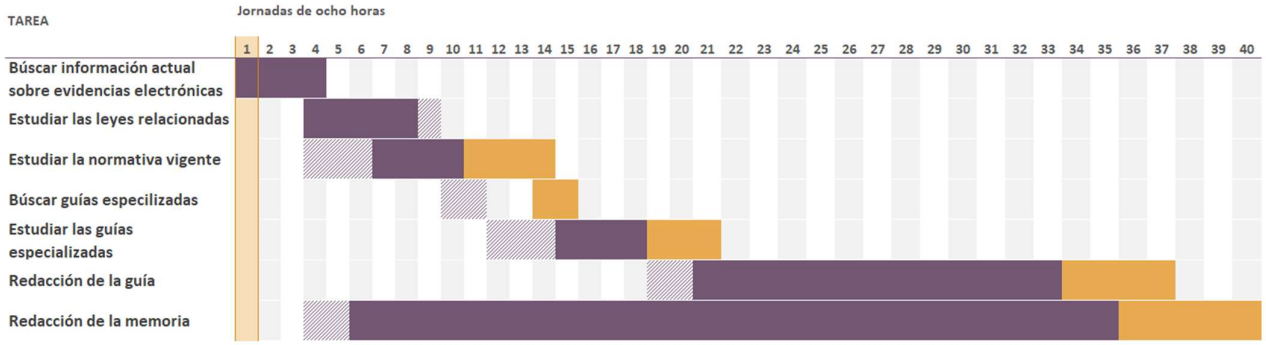

Figura 6. Diagrama de Gantt de las tareas realizadas a lo largo del TFG.

Fuente: Elaboración propia.

Finalmente, aunque el proyecto aumentó en 40 horas sobre la duración planeada, gran parte de este tiempo adicional ya estaba previsto como margen de contingencia para cubrir posibles retrasos. De estas 40 horas adicionales, la mitad formaba parte de las horas de seguridad reservadas en la planificación original, lo que permitió que el trabajo se completara de manera satisfactoria, aunque con un ligero ajuste en la carga horaria final. Este enfoque proactivo permitió mantener el control sobre el proyecto, a pesar de los desafíos encontrados durante el proceso.

3.6. Presupuesto

Al estimar los costos asociados con el trabajo realizado para la creación de una guía sobre gestión de evidencias electrónicas, es esencial tomar en cuenta diversos factores, incluyendo el tiempo invertido, los recursos necesarios y los gastos relacionados con las herramientas y normativas utilizadas. El salario mínimo en España es de 8,87 euros por hora, pero se recomienda que, para un trabajo especializado como este, el pago mínimo sea de 10 euros por hora. Basándonos en esta cifra, y considerando que se han dedicado 320 horas al proyecto, esto supondría un coste total de 3200 euros en términos de tiempo de trabajo.

Además del coste asociado a las horas trabajadas, también es importante considerar el precio de las normas UNE e ISO necesarias para la realización del proyecto. Estas normas, esenciales para garantizar el cumplimiento de los estándares y la calidad del trabajo, tienen un coste que ronda los 70 euros por norma. En este caso, tomando como referencia el apartado 2.3. del

documento, se estima que como mínimo se han consultado entre 5 y 7 normas o estándares esenciales, lo que genera un coste adicional de aproximadamente 500 euros.

Otro aspecto clave para el desarrollo de la guía es la adquisición de una computadora portátil adecuada, junto con una licencia de *software* de Microsoft Word, que es fundamental para crear y editar el documento. El coste estimado de este equipo, junto con el software necesario, sería de 500 euros. Este gasto se suma al presupuesto total del proyecto.

Teniendo en cuenta todos estos elementos, el presupuesto estimado para la creación de la guía ascendería a unos 4200 euros aproximadamente. Este cálculo incluye tanto el coste del trabajo como el de las herramientas y recursos necesarios para asegurar que la guía esté elaborada conforme a los estándares de calidad y a las normativas aplicables en el ámbito de las evidencias electrónicas. Este presupuesto también refleja la inversión necesaria en tecnología y acceso a información normativa crítica, garantizando que el trabajo final sea fiable y acorde a las mejores prácticas.

4. COMPETENCIAS BÁSICAS DEL PERSONAL

Es fundamental que el personal encargado de participar en cualquier fase del proceso de gestión de evidencias electrónicas cuente con las capacidades y conocimientos necesarios para llevar a cabo su labor de manera precisa y conforme a las normativas legales. Esto se debe a que una manipulación incorrecta de las evidencias digitales puede comprometer su integridad, su validez jurídica o incluso llevar a la pérdida de información clave para la investigación. Además, las diferentes etapas del proceso, como son la identificación, preservación, captación y análisis de las evidencias, requieren habilidades técnicas específicas y un profundo entendimiento de los protocolos de seguridad y de la cadena de custodia, por lo que solo personal debidamente capacitado podrá garantizar el éxito del proceso y la protección de la e-evidencia a lo largo de todo su ciclo de vida.

En primer lugar se ha diferenciar claramente el significado entre conocimientos y competencias, refiriéndose el primero a la asimilación de información a través de cualquier acción formativa, y el segundo a la habilidad demostrada para aplicar ese conocimiento en la resolución de tareas y problemas específicos. Además, se debe tener en cuenta que, para realizar algunas actividades de las distintas fases, se requiere que el personal encargado de realizar dichas tareas posea cierta maestría para asegurar que se van a realizar correctamente.

Las siguientes recomendaciones de las competencias básicas que debería poseer el personal se amplían en la Guía «*CEN/Guide 14 Common policy guidance for addressing standardisation on qualification of professions and personnel*».

4.1. Competencias para la identificación

Durante la primera fase de gestión de las evidencias electrónicas, se requiere poder identificar correctamente dichas evidencias, lo que implica no solo la capacidad de caracterizar los dispositivos y componentes involucrados, sino también la capacidad de comprender la información que pueda ser relevante para la investigación. Esto incluye un conocimiento profundo de las leyes relacionadas con el manejo de evidencias digitales y delitos informáticos, garantizando que las pruebas se traten de acuerdo con los marcos legales establecidos. Además, el personal debe ser capaz de identificar las herramientas adecuadas para la recolección y adquisición de datos, así como de evaluar los riesgos asociados con cada dispositivo y su manipulación.

El personal debe poseer un sólido conocimiento en TI y administración de varios tipos de dispositivos, tanto de TI como de redes. Esto incluye estar familiarizado con los procedimientos de investigación en la escena del crimen, ser capaz de determinar el estado de los dispositivos y valorar la información que estos contienen como evidencia potencial. Asimismo, deben conocer los dispositivos y la información relacionada con la informática forense, especialmente en un entorno de redes, donde la interacción entre los dispositivos puede ser compleja y crítica para la investigación.

El desarrollo de la habilidad necesaria incluye el manejo de registros y configuraciones del sistema y de aplicaciones. Esto abarca la identificación de registros clave, como correos electrónicos, registros web, registros de acceso, archivos de contraseñas y configuraciones del sistema. Además, el personal debe entender cómo estos registros pueden estar interrelacionados con las funcionalidades y dependencias del dispositivo, así como evaluar el impacto sobre la evidencia volátil y no volátil. Tener la capacidad de interpretar la configuración del sistema y sus aplicaciones es vital para asegurar la integridad de la evidencia y para descubrir pistas críticas durante una investigación.

Finalmente, la maestría en este campo involucra un análisis especializado y la interpretación avanzada de registros para la detección de intrusiones y la identificación de sistemas afectados. En algunas jurisdicciones, se requiere la confirmación de la evidencia antes de proceder con su recolección, lo que resalta la necesidad de conocimientos especializados. La maestría también implica la capacidad de identificar las contraseñas necesarias para acceder a los dispositivos, comprender diagramas de red y mecanismos de control de acceso, y vincular direcciones IP y MAC para confirmar la identidad de los dispositivos en una red. Esta combinación de habilidades técnicas y analíticas permite al personal gestionar de manera efectiva las complejidades de las evidencias digitales en entornos forenses.

4.2. Competencias para la captación

En cuanto a las competencia requeridas para la captación de evidencias digitales, estas se separan entre las competencias necesarias para realizar su recolección y las necesarias para abordar su adquisición.

4.2.1. Competencias para la recolección

En la recolección de evidencias digitales, se debe garantizar que estas se obtengan de manera segura y eficiente, protegiéndolas de cualquier alteración o amenaza externa. Uno de los aspectos fundamentales es conocer los requisitos de herramientas apropiadas, que permiten la recolección y el empaquetado correcto de la evidencia digital, asegurando que esta permanezca íntegra durante el transporte y almacenamiento. Además, el personal debe estar preparado para implementar medidas de protección contra amenazas ambientales, como variaciones de temperatura, humedad o interferencias electromagnéticas, que podrían comprometer la validez de los datos. Otra área clave abarca la garantía de la información, lo que significa que la evidencia debe ser recolectada, almacenada y transportada de tal manera que su autenticidad y confiabilidad no sean cuestionadas.

En cuanto a las conocimientos necesarios, el personal debe poseer un robusto conocimiento sobre la seguridad general en la recolección de datos. Esto incluye familiarizarse con los principios y el diseño de herramientas básicas utilizadas en la recolección de evidencia digital. Además, es crucial determinar el mejor método de recolección para preservar la mayor cantidad posible de información relevante al incidente investigado. Esto requiere una comprensión del tipo

de evidencia que se necesita preservar y la selección adecuada de técnicas y herramientas que minimicen el riesgo de pérdida o alteración de datos valiosos.

La habilidad para formular y ejecutar el proceso de recolección de evidencia digital es una competencia clave. El personal debe ser capaz de recolectar la evidencia de manera precisa y documentarla adecuadamente, siguiendo los procedimientos establecidos para la cadena de custodia, lo que asegura que la evidencia pueda ser rastreada desde el momento de su recolección hasta su presentación en un tribunal. Además, debe haber un enfoque en el control de calidad durante todo el proceso para garantizar que la recolección de evidencia se realice correctamente. En algunas situaciones, también será necesario entrevistar a los sospechosos para obtener información adicional que pueda ser crucial para el análisis digital.

Por último, la maestría en la recolección de evidencia digital implica la capacidad de optimizar este proceso. Esto significa que el personal no solo debe realizar la recolección de manera eficiente, sino también documentar cualquier evidencia que no pueda ser adquirida debido a restricciones tecnológicas o legales. Esta competencia incluye la recolección de contraseñas, claves y otras formas de seguridad digital que serán necesarias para realizar análisis más avanzados en el laboratorio. La maestría también requiere habilidades especializadas para comprender y gestionar situaciones complejas, asegurando que toda la evidencia recolectada sea viable para su uso en investigaciones más profundas y procedimientos judiciales.

4.2.2. Competencias para la adquisición

La adquisición de evidencia digital es una fase crítica dentro de la gestión de evidencia electrónicas que requiere un conjunto especializado de habilidades clave para asegurar la integridad y legalidad de los datos obtenidos. Uno de los aspectos más importantes es la aplicación precisa de los requisitos de adquisición, lo que implica seguir un procedimiento lógico que garantice la repetibilidad, auditabilidad y reproducibilidad de los datos recolectados. Esto significa que la evidencia adquirida debe ser obtenida de manera que pueda ser replicada por otros profesionales y sometida a un escrutinio legal, permitiendo su defensa en un tribunal de justicia. Las habilidades clave también incluyen la capacidad para manejar adquisiciones tanto en sistemas que están encendidos como en sistemas apagados, cada uno con sus propios desafíos técnicos y legales. Además, la forénsica de redes es una parte esencial, ya que involucra la adquisición de datos que circulan a través de sistemas conectados en red, requiriendo una comprensión avanzada de las comunicaciones y protocolos de red.

En términos de conocimiento, es crucial que los profesionales comprendan la naturaleza de la información que se puede obtener de los dispositivos digitales. Esto incluye datos almacenados en bases de datos, documentos generados por el sistema, datos generados por el usuario y, de particular importancia, datos volátiles, que son aquellos que se pierden si el dispositivo se apaga. La conciencia sobre las estructuras de archivos en sistemas Unix y Windows, así como en diversos dispositivos, es fundamental para poder navegar y extraer información de manera efectiva. Además, los especialistas deben estar atentos al impacto que sus acciones podrían tener sobre los datos volátiles, asegurando que se preserven adecuadamente durante la adquisición.

La habilidad para ejecutar el proceso de adquisición es igualmente esencial. Los profesionales deben saber cómo determinar los requisitos de almacenamiento necesarios para manejar grandes volúmenes de datos y ser capaces de realizar adquisiciones parciales o completas de medios de almacenamiento digital. Esto incluye la adquisición de imágenes, que permite copiar el contenido de un dispositivo sin alterarlo, manteniendo la integridad de la evidencia. El personal debe estar preparado para realizar adquisiciones tanto en sistemas encendidos como apagados, lo que implica diferentes técnicas y consideraciones. Además, deben generar valores *hash*, que son secuencias de caracteres que verifican la integridad de los datos adquiridos y aseguran que estos no hayan sido manipulados.

La maestría en adquisición de evidencia digital implica una mayor comprensión y habilidad en la realización de adquisiciones complejas. Esto incluye la adquisición de medios de almacenamiento digital en configuraciones avanzadas como RAID y bases de datos, así como en dispositivos y equipos miniaturizados que presentan desafíos adicionales debido a su tamaño y arquitectura. Además, quienes dominan estas habilidades entienden las dependencias y el impacto de los diferentes métodos de adquisición, asegurándose de que el método elegido no comprometa la validez de la evidencia. Este nivel de competencia permite al personal enfrentar situaciones complicadas y llevar a cabo la adquisición de manera que los datos recolectados sean consistentes, completos y útiles para futuras investigaciones y procedimientos judiciales.

4.3. Competencias para el análisis

En el ámbito del análisis forense digital, la integridad y autenticidad de las evidencias electrónicas son cruciales y dependen en gran medida de la labor meticulosa y profesional de los especialistas encargados. Para garantizar la validez de las evidencias, se deben seguir estrictas pautas que aseguren un proceso riguroso de cualificación para aquellos que realizarán tareas en este campo. Este proceso incluye la evaluación de características personales y profesionales clave en los candidatos. La honestidad y la discreción son fundamentales para asegurar que la información sensible sea manejada adecuadamente y que los hallazgos no se vean comprometidos. Además, los profesionales deben adherirse a un código de práctica profesional, que garantice el cumplimiento de los estándares éticos y técnicos. La capacidad de mantener un espíritu crítico e independiente es esencial para evaluar las pruebas sin prejuicios, mientras que una mente abierta es necesaria para considerar diversas opiniones y enfoques. La perseverancia y la autodisciplina aseguran que el profesional pueda enfrentar y superar los desafíos que surjan durante el análisis. Finalmente, la capacidad de aprendizaje y adaptación es vital en un campo que evoluciona rápidamente con nuevas tecnologías y métodos.

En términos de conocimiento, es imperativo que los profesionales del análisis forense digital estén bien informados sobre la legislación vigente que regula la relevancia digital de las evidencias y cómo deben ser tratadas a lo largo de su ciclo de vida para mantener su validez. El conocimiento de *software* y *hardware* forense actual es esencial para emplear las herramientas adecuadas en cada fase del análisis. Además, deben poseer habilidades en la identificación de la información forense, así como una comprensión profunda de los sistemas de ficheros utilizados en diversos entornos digitales. El conocimiento acerca de los métodos de extracción de contraseñas y los elementos de Internet que pueden ser almacenados en sistemas también es

crucial. Igualmente, se requiere familiaridad con las técnicas y herramientas empleadas en el fraude informático y con los métodos utilizados por intrusos informáticos, para poder anticipar y mitigar posibles amenazas durante el análisis.

Las habilidades necesarias para un analista forense digital se desarrollan mediante un entrenamiento adecuado en el manejo de evidencia digital y una experiencia previa relevante en las tareas específicas que desempeñará. Esta experiencia garantiza que el profesional pueda aplicar su conocimiento de manera efectiva en las diferentes fases del análisis forense. La formación continua es igualmente importante, ya que el campo de la informática forense está en constante evolución. La actualización periódica en nuevas técnicas, herramientas y mejores prácticas asegura que los analistas mantengan su competencia y capacidad de respuesta ante los desafíos emergentes.

Finalmente, el análisis forense digital implica tener una capacidad excepcional para observar, analizar y extraer conclusiones basadas en el razonamiento lógico. Los profesionales deben ser capaces de describir situaciones y fenómenos complejos en términos comprensibles, lo que facilita la comunicación de hallazgos a personas no especializadas y apoya la presentación efectiva de la evidencia en contextos legales. Esta habilidad es crucial para asegurar que la información técnica se interprete correctamente y se utilice adecuadamente en el proceso judicial, contribuyendo a la resolución efectiva de casos relacionados con delitos informáticos.

4.4. Competencias para la preservación

La preservación de evidencia digital es un componente esencial de la informática forense que garantiza la integridad y autenticidad de los datos desde su recolección hasta su posible uso en tribunales. Las habilidades clave necesarias para la preservación incluyen la capacidad de aplicar y evaluar los requisitos adecuados que aseguren que la evidencia digital permanezca precisa, íntegra y segura. Esta preservación requiere una metodología rigurosa que aborde todos los aspectos, desde el mantenimiento de la cadena de custodia hasta la correcta manipulación de dispositivos informáticos y medios de almacenamiento. La correcta preservación de la evidencia asegura que los datos puedan ser auditados y verificados en cualquier fase del proceso judicial, sin que su validez sea cuestionada.

Los conocimientos necesarios para la preservación de evidencias digitales incluyen entender los requisitos legales y técnicos que rigen la cadena de custodia. Los profesionales deben estar familiarizados con los procedimientos específicos necesarios para garantizar que la evidencia sea rastreable, segura y manejada adecuadamente en todo momento. Esto también implica comprender cómo factores ambientales, como la humedad, la temperatura y posibles golpes, pueden afectar los dispositivos digitales, y aplicar las medidas preventivas adecuadas para mitigar esos riesgos. Además, es importante que el personal entienda las opciones de embalaje y transporte más apropiadas para cada tipo de dispositivo, así como los requisitos de almacenamiento que garantizan la protección de la evidencia contra cualquier tipo de daño o deterioro.

Entre las habilidades necesarias para preservar evidencias electrónicas está saber cómo generar documentos de auditoría que respalden todo el proceso. Esto incluye la capacidad de definir parámetros clave para la documentación de la evidencia, tales como la descripción detallada de los dispositivos, las condiciones de su recolección y las medidas de seguridad aplicadas para garantizar su integridad. Además, los profesionales deben estar capacitados para evaluar las amenazas, vulnerabilidades y controles sobre la evidencia digital, asegurándose de que la información esté protegida frente a posibles alteraciones, accesos no autorizados o cualquier otro tipo de vulnerabilidad.

En cuanto a la maestría, los especialistas en preservación de evidencia digital deben tener la capacidad de aplicar medidas avanzadas para asegurar la integridad de la evidencia, independientemente de su tamaño o complejidad. Esto no solo incluye grandes dispositivos como servidores o unidades de almacenamiento masivo, sino que también dispositivos portátiles miniaturizados, como teléfonos móviles o memorias USB, que presentan desafíos únicos debido a su portabilidad y facilidad de alteración. Además, un experto en esta área debe dominar los procedimientos de documentación detallada, garantizando que cada paso en el proceso de preservación sea minuciosamente registrado, permitiendo así una trazabilidad clara y precisa de la evidencia. Esta habilidad avanzada es crucial para asegurar que la evidencia pueda ser utilizada y defendida en procedimientos legales sin que su autenticidad sea puesta en duda.

5. FASES DEL PROCESO DE GESTIÓN DE EVIDENCIAS ELECTRÓNICAS

La gestión de evidencias electrónicas es un proceso fundamental en el ámbito de las investigaciones digitales y forenses, que asegura que los datos electrónicos puedan ser utilizados de manera efectiva y legal en investigaciones judiciales, auditorías y otros procedimientos. Este proceso se compone de varias fases interrelacionadas que garantizan que la evidencia digital sea manejada, analizada y preservada de forma adecuada, manteniendo su integridad y validez en todo momento. La guía creada como fin de este trabajo cubre las cinco fases fundamentales: identificación, captación, análisis, preservación y presentación. Cada una de estas etapas desempeña un papel crucial en la cadena de custodia de la evidencia digital y están intrínsecamente conectadas entre sí.

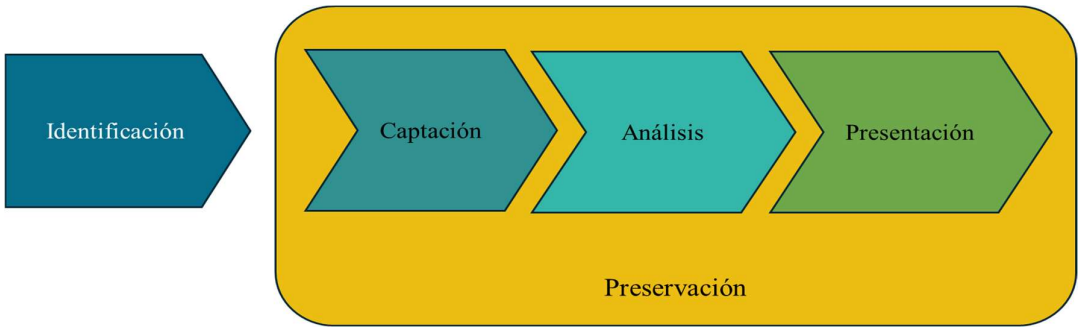

Figura 7. Fases del proceso de gestión de evidencias electrónicas.

Fuente: Elaboración propia.

Identificación: Es la fase inicial donde se detectan y determinan los datos electrónicos que pueden ser relevantes para una investigación. En esta etapa se define qué información es potencialmente valiosa y dónde se encuentra, estableciendo las bases para las etapas siguientes.

Captación: Una vez identificada la evidencia, se procede a su captura o recolección. Esta fase implica la adquisición de la evidencia digital de su entorno original, asegurando que se obtenga de manera precisa y sin alteraciones que puedan comprometer su integridad.

Análisis: Con la evidencia digital en manos, el análisis se enfoca en examinarla y procesarla para extraer información significativa que pueda responder a las preguntas de la investigación. Es una fase técnica que busca interpretar los datos en un contexto forense.

Preservación: Durante todo el proceso, es fundamental mantener la integridad y autenticidad de la evidencia recolectada. La preservación implica proteger la evidencia de cualquier alteración, pérdida o daño desde su captación hasta su presentación.

Presentación: Finalmente, los hallazgos derivados del análisis de la evidencia deben ser presentados de manera clara y comprensible, ya sea en un tribunal o en un informe de

investigación. Esta etapa asegura que los resultados obtenidos sean comunicados de forma efectiva y que la evidencia se mantenga válida y admisible.

5.1. Identificación

La fase de identificación en el proceso de gestión de evidencias electrónicas es la primera etapa crucial en la investigación digital. Consiste en localizar, reconocer y determinar las fuentes potenciales de evidencia digital que pueden ser relevantes para el caso. El objetivo principal de esta fase es identificar de manera exhaustiva toda la información que puede contener datos importantes para la investigación, con el fin de preservarlos adecuadamente para su posterior análisis.

Los aspectos clave de esta fase comienzan con la localización de la evidencia, donde se identifican todos los dispositivos, sistemas, redes y plataformas que puedan almacenar información relevante para la investigación. Esto abarca una amplia gama de equipos y tecnologías, tales como computadoras, teléfonos móviles, tabletas y servidores. Además, incluye fuentes como correos electrónicos, bases de datos, discos duros y dispositivos de almacenamiento externo, así como redes sociales, servicios en la nube, aplicaciones y *software*.

Otro aspecto crucial es la identificación de los actores relevantes. En este paso, se determinan las personas o entidades asociadas con los dispositivos o sistemas previamente identificados. Estos actores pueden incluir empleados, proveedores, administradores de sistemas y cualquier otra parte que tenga relación con los datos o dispositivos involucrados en la investigación.

La determinación del alcance es también fundamental. Aquí se define el tipo de evidencia digital que se va a buscar, lo cual puede abarcar correos electrónicos, archivos, registros de actividad (*logs*), transacciones, entre otros tipos de datos. Asimismo, se especifican los intervalos de tiempo relevantes para la investigación y se considera la naturaleza de los datos, como textos, imágenes, videos o cualquier otro formato digital que sea importante para el caso.

En esta fase, también se determinará el orden de captación y análisis, dando prioridad a las evidencias más volátiles, como datos en la memoria RAM o en sesiones activas que podrían perderse rápidamente. Asimismo, se establecerán las herramientas forenses que se utilizarán a lo largo del proceso, asegurando que sean adecuadas para capturar y analizar la evidencia de manera eficaz y conforme a los requisitos técnicos y legales de la investigación.

También es crucial garantizar el cumplimiento legal y normativo a lo largo de todo el proceso de identificación. Esto implica asegurarse de que se respeten las leyes y regulaciones aplicables, como las normativas sobre privacidad de datos y la obtención de las autorizaciones legales necesarias para acceder a la información. Cumplir con estos requisitos asegura que la evidencia recolectada sea válida y admisible en procedimientos legales o investigaciones.

Para la redacción de los pasos que esta fase en la guía que podemos encontrar en el Anexo A, se hizo uso principalmente de las pautas establecidas en las normas UNE 71505:2013 y UNE-ISO/IEC 27037:2013. La primera de ellas es relevante debido a que, como se ha mencionado en el punto 2.3., esta establece los procedimientos necesarios para asegurar que la evidencia sea

identificada de manera correcta y oportuna. Esto es crucial ya que de esta forma se establece un marco metodológico que ayuda a los investigadores a localizar y reconocer las fuentes de datos relevantes de manera consistente y controlada, minimizando el riesgo de omisiones o alteraciones accidentales. La segunda norma es una adaptación de la norma internacional ISO/IEC 27037 y proporciona directrices específicas sobre cómo proceder en la identificación de evidencias digitales. Define los roles y responsabilidades de los involucrados en el proceso, así como los métodos adecuados para la localización de la evidencia digital, garantizando su integridad desde el inicio del proceso de identificación.

En resumen, la fase de identificación se enfoca en descubrir todas las fuentes potenciales de evidencia digital, de manera sistemática y ordenada, con el fin de garantizar que toda la información relevante sea preservada y utilizada adecuadamente en la investigación.

5.2. Captación

En el ámbito de la gestión de evidencias electrónicas, las normas y directrices varían en su enfoque sobre los procesos de recolección y adquisición de datos. Mientras que algunas normas distinguen claramente entre la recolección y la adquisición, otras consideran la recolección como una parte integral del proceso de preservación. Esta variabilidad puede generar confusión y complicar la implementación de prácticas estandarizadas. En la guía que hemos desarrollado, hemos optado por hacer una distinción clara entre estas fases, tratando la recolección y la adquisición como procesos separados. En particular, hemos definido la fase de captación de manera que refleje esta separación, facilitando así una comprensión más precisa y la aplicación efectiva de cada etapa en la gestión de evidencias electrónicas. Esta distinción pretende proporcionar un enfoque más estructurado y coherente, que permita a los profesionales seguir procedimientos claros y específicos en la captura y manejo de datos digitales.

Existen varias normas UNE que están directamente relacionadas con los procesos de recolección y adquisición de evidencias electrónicas, ya que ambas fases son cruciales para asegurar la integridad, validez y legalidad de la evidencia digital. Al igual que en la fase de identificación las normas UNE 71505:2013 y UNE-ISO/IEC 27037:2013 son las más destacadas. Además estas normas proporcionan la diferenciación entre recolección y adquisición. La normas UNE 71506:2013 también proporciona ciertas pautas en cuanto a la captación de evidencias pero no diferencia los procesos de recolección y de preservación, centrándose solamente en la adquisición de evidencias electrónicas durante esta fase.

5.2.1. Recolección de evidencias electrónicas

La recolección es la fase en la que se identifican y juntan los dispositivos y medios físicos que contienen potencialmente evidencias electrónicas. En este proceso, se toma control físico de los dispositivos o soportes donde están almacenados los datos relevantes para el caso. La recolección abarca desde la localización del dispositivo hasta su preservación y transporte a un entorno controlado para su análisis.

Las características principales de la recolección de evidencias electrónicas se centran en varios aspectos clave. En primer lugar, esta fase se enfoca en recoger los dispositivos o medios físicos donde reside la evidencia, tales como discos duros, teléfonos móviles, unidades USB, servidores, entre otros. Es esencial que el proceso de recolección se lleve a cabo con una atención meticulosa a la preservación de la cadena de custodia desde el momento en que se toman los dispositivos. Esto asegura que no haya alteraciones en la evidencia durante su traslado y manejo.

Además, la recolección implica una documentación exhaustiva del proceso para garantizar que se mantenga la integridad y autenticidad de los dispositivos que contienen la evidencia. Aunque la evidencia puede estar en su estado original durante esta fase, aún no se ha llevado a cabo ningún proceso de extracción o análisis. Por ejemplo, si se sospecha que una computadora contiene correos electrónicos comprometidos, la recolección implicará trasladar el dispositivo a un laboratorio de análisis digital. En este caso, el dispositivo se almacena y transporta de manera que se preserve su estado y se documente adecuadamente para futuras fases de análisis.

5.2.2. Adquisición de evidencias electrónicas

La adquisición es el proceso de extraer la evidencia digital del dispositivo o medio físico de manera forense, asegurando que los datos sean copiados de forma íntegra y sin alteraciones. El objetivo es crear una copia exacta de los datos (imagen forense) para poder analizarlos sin comprometer la información original.

Las características principales de la adquisición de evidencias electrónicas se centran en la creación y manejo de copias precisas de los datos. En esta fase, se realiza la creación de una copia forense de los datos, que es una réplica bit a bit del contenido del dispositivo original. Este proceso asegura que todos los datos sean duplicados en su totalidad, sin perder ninguna información durante la transferencia.

Para garantizar que la evidencia no se altere durante la extracción, se utilizan herramientas especializadas diseñadas para este propósito. Estas herramientas están calibradas para mantener la integridad de los datos mientras se realiza la copia. Además, la integridad de los datos adquiridos se verifica mediante el uso de sumas de verificación o *hashes*, como MD5 o SHA-1. Estas técnicas aseguran que la copia forense es idéntica al original y que no ha habido ninguna alteración durante el proceso.

Una vez realizada la adquisición, la evidencia puede ser analizada sin riesgo de modificar los datos originales, lo que permite realizar un análisis detallado sin comprometer la integridad del dispositivo original. Por ejemplo, si se recoge una computadora sospechosa de contener correos electrónicos comprometidos, se puede adquirir una imagen forense del disco duro de la máquina. Esta imagen puede luego ser utilizada para analizar los correos electrónicos sin intervenir directamente en el dispositivo original, garantizando así que los datos se mantienen intactos durante todo el proceso de investigación.

5.3. Análisis

El análisis de evidencias electrónicas es una fase crítica en el proceso de gestión de evidencias digitales que implica el examen detallado y sistemático de los datos recolectados o adquiridos con el fin de identificar, extraer, interpretar y documentar la información relevante para una investigación.

El proceso de análisis de evidencias electrónicas comienza con la preparación del entorno de análisis. Es fundamental crear un entorno controlado y seguro para llevar a cabo el análisis de las copias forenses de la evidencia digital, en lugar de trabajar con el dispositivo original. Esto asegura que la evidencia original permanezca inalterada durante el proceso. Para esta tarea, se emplean herramientas especializadas y software forense que permiten realizar un análisis detallado y preciso de los datos.

La siguiente etapa es la revisión inicial de los datos. En esta fase, se realiza una inspección preliminar de los datos para familiarizarse con su estructura y contenido. El objetivo es identificar archivos, registros, correos electrónicos, *logs* y otros tipos de datos que puedan ser relevantes para la investigación. Se aplican filtros y técnicas de búsqueda para enfocar el análisis en la información más pertinente, como fechas, palabras clave o tipos de archivos específicos.

Una vez realizada la revisión inicial, se procede a la extracción de información relevante. En esta etapa, se extrae información que pueda tener valor probatorio o esté directamente relacionada con la investigación. Esto puede incluir archivos eliminados, metadatos sobre la creación, modificación y acceso a archivos, historial de navegación web, registros de chat o mensajería instantánea, y registros de actividad de usuario, entre otros. A menudo, es necesario reconstruir eventos o actividades digitales a partir de los datos analizados, como la cronología de acciones realizadas en un sistema o dispositivo.

El análisis de evidencias electrónicas utiliza diversas técnicas comunes. La recuperación de archivos eliminados implica el uso de técnicas forenses para recuperar archivos que han sido eliminados pero aún pueden estar presentes en el almacenamiento. El análisis de metadatos proporciona información sobre archivos, como fechas de creación y modificación, que puede ofrecer pistas importantes sobre el uso del dispositivo. El análisis de registros y *logs* examina eventos y actividades en sistemas operativos, aplicaciones o dispositivos de red, para identificar accesos o actividades sospechosas. La revisión de correos electrónicos y comunicaciones permite identificar contenido relevante, patrones de comunicación o vínculos entre individuos. Además, el análisis de redes examina datos de tráfico de red, registros de conexión y otros indicadores para identificar intrusiones, conexiones sospechosas o transferencias de datos inusuales.

La importancia del análisis de evidencias electrónicas radica en su capacidad para transformar datos brutos en pruebas procesables que pueden ser utilizadas en investigaciones criminales, civiles o corporativas. Los resultados de esta fase pueden ser determinantes para probar la culpabilidad o inocencia en casos legales, detectar fraudes, robos de información, acoso o delitos cibernéticos, obtener información sobre actividades maliciosas dentro de una organización, y entender cómo se cometieron incidentes de seguridad o violaciones de datos.

El análisis de evidencias electrónicas es una fase crítica que está regida por normas que aseguran la correcta metodología, integridad de la evidencia y procedimientos adecuados para convertir datos digitales en pruebas confiables. Las normas UNE relacionadas con esta fase incluyen aquellas que establecen directrices sobre cómo realizar el análisis de manera forense y con garantías legales. A continuación, se presentan las normas más relevantes:

- UNE 71505:2013 - Metodología para la Identificación, Recolección, Adquisición y Preservación de Evidencias Electrónicas. Aunque esta norma cubre varias etapas del proceso de gestión de evidencias, también se relaciona con el análisis, ya que proporciona un marco metodológico que abarca desde la identificación hasta la preservación de la evidencia. Este marco establece las pautas necesarias para garantizar que la evidencia que se va a analizar sea íntegra y confiable, lo cual es crucial para el éxito del análisis.

- UNE-ISO/IEC 27037:2013 - Directrices para la Identificación, Recolección, Adquisición y Preservación de Evidencias Digitales. Esta norma es una de las más completas en cuanto a la gestión de evidencias electrónicas, y se extiende también al análisis de las mismas. Establece los métodos y procedimientos que se deben utilizar para analizar la evidencia digital de manera forense, asegurando que los datos se procesen de forma que sean aceptables en un contexto legal.

- UNE-ISO/IEC 27042:2016 - Directrices para el Análisis de Evidencias Digitales. Esta norma se centra específicamente en el proceso de análisis de la evidencia digital. Proporciona directrices detalladas para llevar a cabo un análisis forense de manera estructurada y metodológica, asegurando que las técnicas utilizadas sean consistentes, reproducibles y que se mantenga la integridad de la evidencia.

5.4. Presentación

La fase de presentación de evidencias electrónicas es fundamental para garantizar que la evidencia digital relevante sea documentada y presentada de manera efectiva en procedimientos judiciales u otros contextos importantes. En esta fase, se genera una documentación detallada que incluye informes forenses que describen los métodos utilizados, las evidencias encontradas, su interpretación y su relevancia en el caso. Estos informes deben ser claros, completos y comprensibles para las partes interesadas, como abogados y jueces, para asegurar que los hallazgos sean defendibles en un tribunal. Es crucial que los informes demuestren que se mantuvo la integridad de los datos y que los procedimientos forenses se realizaron siguiendo las normas y mejores prácticas establecidas.

Además, la interpretación de la evidencia es un aspecto clave de esta fase. La evidencia extraída debe ser contextualizada en relación con la investigación, lo que puede requerir conocimientos especializados en sistemas operativos, redes, aplicaciones y otros aspectos técnicos. El objetivo es identificar patrones, relaciones y correlaciones en los datos que puedan proporcionar pruebas claras sobre los hechos investigados, como acciones sospechosas, accesos no autorizados o comunicaciones comprometedoras.

Finalmente, en algunos casos, los hallazgos del análisis pueden ser sometidos a una revisión crítica por un equipo o peritos independientes para asegurar que los resultados sean fiables y que se hayan seguido correctamente los protocolos. Esta revisión adicional ayuda a validar la integridad del análisis y a reforzar la credibilidad de la evidencia presentada.

5.5. Preservación

La preservación de evidencias electrónicas es un proceso crítico dentro de la gestión de evidencias digitales que tiene como objetivo mantener la integridad y autenticidad de la información digital desde el momento en que se recolecta o adquiere hasta que se presenta en un tribunal o durante una investigación. Este proceso garantiza que la evidencia no sea alterada, modificada, destruida o contaminada durante su manejo y almacenamiento, asegurando que los datos se mantengan en su estado original. Desde el momento de la recolección, se deben implementar medidas para proteger los datos digitales, como archivos, registros de actividad y correos electrónicos, de manera que permanezcan tal como se encontraron. Este proceso abarca el manejo adecuado de los dispositivos físicos que contienen la evidencia, como discos duros, dispositivos móviles y servidores, y la creación de copias forenses exactas (imágenes bit a bit) que se utilizan para el análisis, dejando el dispositivo original intacto.

Se emplean herramientas forenses certificadas y especializadas para crear imágenes precisas de los dispositivos, garantizando que los datos no se alteren durante la adquisición o el análisis. Estas herramientas también permiten la verificación de la integridad de los datos mediante el uso de códigos *hash* (como MD5 o SHA-256), que generan un valor único basado en los datos y actúan como una «huella digital» de la evidencia, asegurando que no se ha producido ninguna alteración durante la cadena de custodia.

La cadena de custodia es fundamental en la preservación de evidencia, ya que representa el registro detallado del manejo de la evidencia desde su recolección hasta su presentación en un tribunal o durante una investigación. Es crucial documentar todas las transferencias y accesos a la evidencia para demostrar quién tuvo acceso y qué se hizo con ella en cada etapa, evitando cualquier cuestionamiento sobre la integridad de los datos.

Además, la protección física y lógica de los dispositivos que contienen la evidencia es esencial. Los dispositivos deben ser almacenados en entornos seguros con controles de acceso adecuados para evitar manipulaciones no autorizadas. Simultáneamente, se deben implementar medidas de seguridad lógicas, como cifrado y control de acceso, para proteger los datos digitales contra accesos o alteraciones inapropiadas.

Otro aspecto importante de la preservación es la garantía de disponibilidad. Esto implica mantener copias de seguridad adecuadas de la evidencia digital para prevenir la pérdida accidental y asegurar que los datos puedan ser recuperados de manera confiable en el futuro. La documentación completa de cada acción realizada sobre la evidencia, incluyendo accesos, análisis, transferencias y cambios en las condiciones de almacenamiento, es crucial para demostrar que la evidencia no ha sido alterada desde su recolección y es fundamental para su presentación en un tribunal.

La preservación de la evidencia está regulada por normas y estándares que garantizan que los procesos seguidos sean adecuados y aceptables en contextos judiciales:

- UNE-ISO/IEC 27037:2013 - Directrices para la Identificación, Recolección, Adquisición y Preservación de Evidencias Digitales: Esta norma establece directrices detalladas para la preservación de evidencia electrónica, describiendo las mejores prácticas para proteger los datos digitales y garantizar su integridad durante todo el proceso.

- UNE 71505:2013 - Metodología para la Identificación, Recolección, Adquisición y Preservación de Evidencias Electrónicas: Abarca todos los aspectos de la preservación de evidencias digitales y proporciona directrices específicas sobre cómo mantener la evidencia en su estado original.

Como se ha mencionado previamente en el punto 5.2, la preservación y la recolección de evidencias electrónicas se tratan como dos etapas distintas dentro del proceso de gestión de evidencias digitales, aunque están estrechamente relacionadas. Ambas fases son complementarias y esenciales para garantizar que la evidencia electrónica sea válida y confiable en cualquier investigación forense o procedimiento legal.

La recolección de evidencias electrónicas es el proceso de identificación, localización y obtención de datos digitales que puedan ser relevantes para una investigación. Se trata de tomar los datos o dispositivos electrónicos (discos duros, memorias USB, correos electrónicos, archivos, etc.) desde su ubicación original y trasladarlos a un entorno controlado, como una copia forense. Su objetivo principal es asegurar la captura de todos los datos pertinentes sin comprometer su integridad, siguiendo procedimientos estandarizados para evitar alteraciones.

Mientras tanto, la preservación de evidencias electrónicas es el proceso de proteger y mantener la integridad y autenticidad de los datos recolectados desde el momento en que se obtiene la evidencia hasta que se presenta en una investigación o en un tribunal. Su objetivo es garantizar que la evidencia se conserve inalterada, tanto durante el almacenamiento como durante el análisis, para que pueda ser utilizada como prueba fiable y admisible en procesos judiciales o investigaciones.

Por último, mencionar que la recolección ocurre al inicio del proceso de gestión de evidencias electrónicas. Es la primera etapa después de la identificación de la evidencia relevante y se centra en obtener los datos o dispositivos que contienen la evidencia. Por otro lado, la preservación comienza inmediatamente después de la recolección y continúa durante todo el ciclo de vida de la evidencia digital. Abarca desde la captura inicial de la evidencia hasta su almacenamiento seguro, transporte, análisis y eventual presentación en un tribunal.

6. CONCLUSIONES

En definitiva, todos los objetivos planteados en el punto 1.2. este trabajo han sido alcanzados con éxito. El principal objetivo de crear una guía clara y concisa para la gestión de evidencias electrónicas ha sido cumplido. Esta guía está dirigida a profesionales de la informática forense, peritos y auditores, brindándoles una herramienta útil para seguir los pasos adecuados durante la identificación, captación, análisis, preservación y presentación de evidencias electrónicas. Además, la guía asegura que los procedimientos estén alineados con la normativa española vigente, permitiendo verificar que cada fase del proceso se haya realizado correctamente conforme a la ley.

A lo largo del desarrollo de la guía, se tomó una decisión clave sobre cómo dividir las fases del proceso. Si bien algunas normativas unificaban los pasos de recolección y preservación mientras que otras los separaban, se consideró más lógico esta última opción, ya que la preservación puede tener lugar antes o después del análisis, mientras que la recolección debe ocurrir antes. Esta división clara de los pasos garantiza una mejor organización y coherencia en el manejo de las evidencias electrónicas, facilitando su gestión adecuada.

La guía también cumple con el objetivo de proporcionar un esquema detallado y accesible, que permite a los profesionales seguir los procedimientos sin ambigüedades, asegurando la integridad y confiabilidad de las evidencias digitales. Finalmente, la guía puede usarse para contribuir a la solución de problemas derivados de incidentes informáticos o infracciones legales, permitiendo la recolección de evidencias robustas y confiables que ayuden a esclarecer los hechos de manera precisa, ya sea para identificar la causa de un incidente o determinar la responsabilidad de los actores involucrados.

Para finalizar, mencionar que, personalmente, he adquirido diferentes habilidades tanto a nivel profesional como personal. En el ámbito profesional, he ampliado significativamente mis conocimientos en informática forense, legislación relacionada con la gestión de evidencias electrónicas y los procesos detallados de identificación, captación, análisis, preservación y presentación de estas evidencias. Además, he ganado una comprensión más profunda de cómo aplicar normativas vigentes a situaciones reales, lo que refuerza mi capacidad de tomar decisiones fundamentadas en entornos legales y técnicos complejos. En el plano personal, durante este proceso he desarrollado habilidades críticas como la perseverancia, la autodisciplina y la capacidad de adaptarse a nuevos retos, lo que ha incrementado mi confianza para enfrentar futuros desafíos tanto en mi carrera profesional como en mi vida diaria.

6.1. Relación del trabajo desarrollado con los estudios cursados

Este trabajo tiene una estrecha relación con la asignatura de Deontología y Profesionalismo cursada en el grado. Esta asignatura se centra en enseñar a los estudiantes de ingeniería informática los principios éticos y las responsabilidades profesionales que deben guiar su ejercicio profesional.

En términos generales, la asignatura aborda temas como el estudio de los deberes éticos y morales relacionados con la práctica de la ingeniería informática. Esto incluye los códigos de conducta que deben seguir los ingenieros, las normas y principios éticos del sector, y cómo aplicarlos en el día a día profesional. Además explora el impacto de las decisiones técnicas y tecnológicas en la sociedad y el medio ambiente, promoviendo la toma de decisiones responsables en temas como privacidad, muy presente en este trabajo. Asimismo, durante esta asignaturas se estudian las leyes y normativas que regulan la profesión de ingeniero informático, así como las implicaciones legales de su trabajo en áreas como la protección de datos, propiedad intelectual, ciberseguridad y cumplimiento normativo.

Por otra parte, la asignatura de Gestión de Proyectos también está muy ligada a la creación del TFG, ya que tiene como objetivo formar a los estudiantes en las metodologías, técnicas y herramientas necesarias para planificar, gestionar y ejecutar proyectos informáticos de manera eficiente y efectiva. En otras palabras, es la asignatura que nos capacita para poder gestionar bien la creación del TFG.

Por último, muchas de las competencias adquiridas a lo largo del grado han sido de gran valor para la realización del TFG. La aplicación práctica de estas competencias ha sido crucial en todas las fases del proyecto, desde la planificación inicial hasta la elaboración final de la guía:

- La competencia CT1 - Comprensión e integración fue esencial desde el comienzo del TFG. La capacidad para identificar y expresar de manera clara los objetivos generales y específicos del trabajo permitió estructurar la guía correctamente. Esta competencia también garantizó que la guía fuera coherente con los objetivos propuestos, mejorando su utilidad práctica.

- La competencia CT2 - Aplicación y pensamiento práctico se manifestó a través de la recopilación y análisis de información relevante para el trabajo. Buscar fuentes de calidad y referenciarlas adecuadamente permitió construir una base sólida para el desarrollo de la guía.

- La competencia CT3 - Análisis y resolución de problemas se aplicó de forma continua durante el proyecto. El enfoque sistemático para descomponer el problema y trabajar en soluciones viables resultó clave para el éxito del TFG. La justificación de las decisiones tomadas, tanto en la elección de tecnologías como en la metodología empleada, demostró un análisis profundo de las alternativas disponibles y la implementación de procedimientos de validación para garantizar la efectividad de la guía.

- En cuanto a la competencia CT5 - Diseño y proyecto, comprender el alcance total del proyecto y gestionar los límites establecidos fue fundamental, especialmente en lo referente a la restricción de horas dedicadas. Asumir la responsabilidad en la toma de decisiones permitió mantener un enfoque riguroso y estructurado durante el desarrollo del TFG, asegurando que todas las soluciones propuestas fueran evaluadas de manera adecuada en términos de viabilidad y cumplimiento de los requisitos.

- La competencia CT9 - Pensamiento crítico también tuvo un papel relevante en el análisis de la situación actual de la tecnología y las soluciones existentes. El TFG se desarrolló

no solo con el objetivo de cumplir los requerimientos académicos, sino también para aportar valor al ámbito profesional, sintetizando los logros conseguidos y reflexionando sobre su impacto en el aprendizaje del estudiante.

- Finalmente, la competencia CT12 - Planificación y gestión del tiempo fue indispensable para la correcta distribución de las actividades a lo largo del desarrollo del TFG. Elaborar un plan de trabajo eficiente, ajustarse a los plazos establecidos, y entregar los avances de manera oportuna permitió llevar a cabo el proyecto de manera organizada, asegurando la calidad del resultado final.

En resumen, las competencias transversales adquiridas durante el grado han sido herramientas indispensables en la realización del TFG, permitiendo abordar el trabajo de manera integral y asegurar que se cumpliera con los objetivos y requerimientos planteados, tanto a nivel técnico como profesional.

7. TRABAJOS FUTUROS

Una posible ampliación del trabajo presentado sería el desarrollo de una guía auxiliar que ofrezca una explicación más detallada de la fase de análisis de evidencias electrónicas. Esta guía adicional podría proporcionar directrices específicas sobre cómo elegir el tipo de análisis adecuado en función de las características del caso y de la evidencia disponible. Actualmente, la guía principal asume que el responsable del análisis posee conocimientos previos sobre qué técnicas aplicar en cada situación particular, lo cual puede no ser siempre el caso.

La guía auxiliar también podría incluir una sección dedicada a las herramientas forenses específicas recomendadas para cada tipo de análisis. Esta adición no solo detallaría las funcionalidades y aplicaciones de estas herramientas, sino que también ofrecería recomendaciones basadas en la naturaleza de los datos a analizar, como archivos eliminados, metadatos, registros de actividad, entre otros. Proporcionar esta información adicional ayudaría a los profesionales a tomar decisiones informadas sobre qué métodos y herramientas utilizar, optimizando así la eficacia y precisión del análisis forense.

Esta ampliación abordaría el riesgo de malinterpretaciones y errores al elegir técnicas de análisis, asegurando que el proceso se realice de manera más informada y sistemática.

REFERENCIAS BIBLIOGRÁFICAS

AENOR. *UNE-EN ISO/IEC 27040:2016. Seguridad en el almacenamiento (ISO/IEC 27040:2015)*. Ratificada por AENOR en diciembre de 2016. [en línea]. Disponible en: https://www.aenor.com/normas-y-libros/buscador-de-normas/?c=UNE-EN%20ISO/IEC%2027040%3A2016.

AENOR. *UNE-EN ISO/IEC 27041:2016. Directrices para garantizar la idoneidad y adecuación del método de investigación de incidentes (ISO/IEC 27041:2015)*. Ratificada por AENOR en diciembre de 2016. [en línea]. Disponible en: https://www.aenor.com/normas-y-libros/buscador-de-normas/?c=UNE-EN%20ISO/IEC%2027041%3A2016.

Barbara, John J. *Digital evidence accreditation in the corporate and business environment*. Digital Investigation, vol. 2, n.º 2, junio de 2005, pp. 137-146. Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S1742287605000344

CEN/Guide 14. Common Policy Guidance for Addressing Standardisation on Qualification of Professions and Personnel. Brussels: European Committee for Standardization (CEN), 2008.

Computing. *Autelsi presenta su estudio sobre evidencias electrónicas.* [en línea]. 9 nov. 2012. Disponible en: https://www.computing.es/mercado-ti/autelsi-presenta-su-estudio-sobre-evidencias-electronicas/

Convenio sobre Ciberdelincuencia. Convenio del Consejo de Europa sobre Ciberdelincuencia (Convenio de Budapest). Budapest: Consejo de Europa, 2001.

Gobierno de España. *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Boletín Oficial del Estado [en línea]. 6 de diciembre de 2018, nº 294. [Consulta: 28 de agosto de 2024]. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf.

Ilustre Colegio de la Abogacía de Madrid. *Prueba digital: la admisibilidad en juicio de las evidencias electrónicas.* [en línea]. Disponible en: https://masterdigital.icam.es/prueba-digital-la-admisibilidad-en-juicio-de-las-evidencias-electronicas/

IMARC Group. *Digital Forensics Market* [en línea]. Disponible en: https://www.imarcgroup.com/digital-forensics-market

Internet Engineering Task Force (IETF). *Guidelines for Evidence Collection and Archiving*. RFC 3227. [en línea]. February 2002. Disponible en: https://datatracker.ietf.org/doc/rfc3227/.

INTERPOL. *Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence*. Lyon: Interpol, 2019.

INTERPOL. Global Guidelines for Digital Forensics Laboratories. Lyon: International Criminal Police Organization (INTERPOL), 2018.

ISO/IEC 27035:2011. Information security incident management. Geneva: International Organization for Standardization (ISO), 2011.

ISO/IEC 27050:2016. Information technology — Electronic discovery. Geneva: International Organization for Standardization (ISO), 2016.

Laboratorio de Informática Forense europeo. *¿Por qué es importante la evidencia digital y su adecuada gestión?* [en línea]. 22 oct. 2022. Disponible en: https://www.laboratoriodeinformaticaforense.com/por-que-es-importante-la-evidencia-digital-y-su-adecuada-gestion/

Ley 41/2015, de 5 de octubre. Ley de Enjuiciamiento Criminal. Boletín Oficial del Estado (BOE), núm. 238, 6 de octubre de 2015, pp. 76425-76536.

Ley 1/2000, de 7 de enero. Ley de Enjuiciamiento Civil. Boletín Oficial del Estado (BOE), núm. 7, 8 de enero de 2000, pp. 567-593.

Ley 34/2002, de 11 de julio. Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE). Boletín Oficial del Estado (BOE), núm. 166, 12 de julio de 2002, pp. 25360-25379.

Ley 6/2020, de 11 de noviembre. Ley de medidas urgentes en materia de prevención, contención y coordinación para hacer frente a la crisis sanitaria causada por la COVID-19. Boletín Oficial del Estado (BOE), núm. 319, 12 de noviembre de 2020, pp. 101069-101092.

Ley 25/2007, de 18 de octubre. Ley de Protección de Datos de Carácter Personal. Boletín Oficial del Estado (BOE), núm. 250, 19 de octubre de 2007, pp. 44067-44095.

Ley 8/2011, de 28 de abril. Ley de Protección de las Infraestructuras Críticas. Boletín Oficial del Estado (BOE), núm. 103, 29 de abril de 2011, pp. 45244-45259.

Ley 36/2015, de 28 de septiembre. Ley de Seguridad Nacional. Boletín Oficial del Estado (BOE), núm. 236, 29 de septiembre de 2015, pp. 75226-75258.

Magraner Gimeno, Jordi. *Pruebas y evidencias telemáticas*. Trabajo Fin de Grado. Grado en Ingeniería Informática. Valencia: Escola Tècnica Superior d'Enginyeria Informàtica, Universitat Politècnica de València, 2014-2015. Tutor: Juan Vicente Oltra Gutiérrez.

Ministerio del Interior de España. *Informe sobre Cibercriminalidad 2023*. [en línea]. Madrid: Ministerio del Interior, 2023. [Consulta: 28 de agosto de 2024]. Disponible en: https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf.

MORDOR INTELLIGENCE. *Europe Digital Forensics Market - Industry Trends, Share, Size, Growth, Opportunity and Forecast 2024*. [En línea] 2024. Disponible en: https://www.mordorintelligence.com/industry-reports/europe-digital-forensics-market-industry

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Reglamento General de Protección de Datos (RGPD). Diario Oficial de la Unión Europea, L 119, 4 de mayo de 2016. pp. 1-88.

Sheetz, M. *Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers*. New York: John Wiley & Sons, 2013.

UNE 71505-1:2013. *Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales*. Madrid: Asociación Española de Normalización y Certificación (AENOR), 2013.

UNE 71505-2:2013. *Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas*. Madrid: Asociación Española de Normalización y Certificación (AENOR), 2013.

UNE 71505-3:2013. *Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos*. Madrid: Asociación Española de Normalización y Certificación (AENOR), 2013.

UNE 71506:2013. *Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas*. Madrid: Asociación Española de Normalización y Certificación (AENOR), 2013.

UNE-EN ISO/IEC 27037:2016. *Tecnología de la información. Técnicas de seguridad. Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas (ISO/IEC 27037:2012)*. Ratificada por AENOR en diciembre de 2016.

UNE-EN ISO/IEC 27042:2016. *Tecnología de la información. Técnicas de seguridad. Directrices para el análisis y la interpretación de las evidencias electrónicas (ISO/IEC 27042:2015)*. Ratificada por AENOR en diciembre de 2016.

ANEXOS

Anexo A. Guía completa

Las evidencias electrónicas, al igual que todas las evidencias tradicionales, deben ser manipuladas cuidadosamente para que puedan ser válidas. Esto afecta tanto a la integridad física de los dispositivos como a la información o datos contenidos en ellos. Debe tenerse en cuenta que algunos dispositivos electrónicos requieren de procedimientos específicos para su recolección y preservación, ya sea porque son susceptibles a daños físicos o porque pueden sufrir cambios en su contenido durante su manipulación.

El proceso integral de gestión de evidencias electrónicas descrito en este documento tiene como objetivo la generación, manipulación y conservación segura de la información con valor probatorio. Esto se logra mediante la integración de procesos que estén adaptados a las necesidades operativas (procesos de negocio), físicas y técnicas (equipamientos, *software* y *hardware*, es decir, tecnologías) y humanas (personas y comportamientos), tal y como se aprecia en la Figura 8. Este proceso debe realizarse dentro del marco legal, regulatorio y social apropiado. Además este debe permitir crear un entorno seguro para proteger y gestionar los datos con valor probatorio, orientado tanto al cumplimiento de leyes y normas, como a la reducción de los riesgos económicos, legales y reputacionales de la organizaciones.

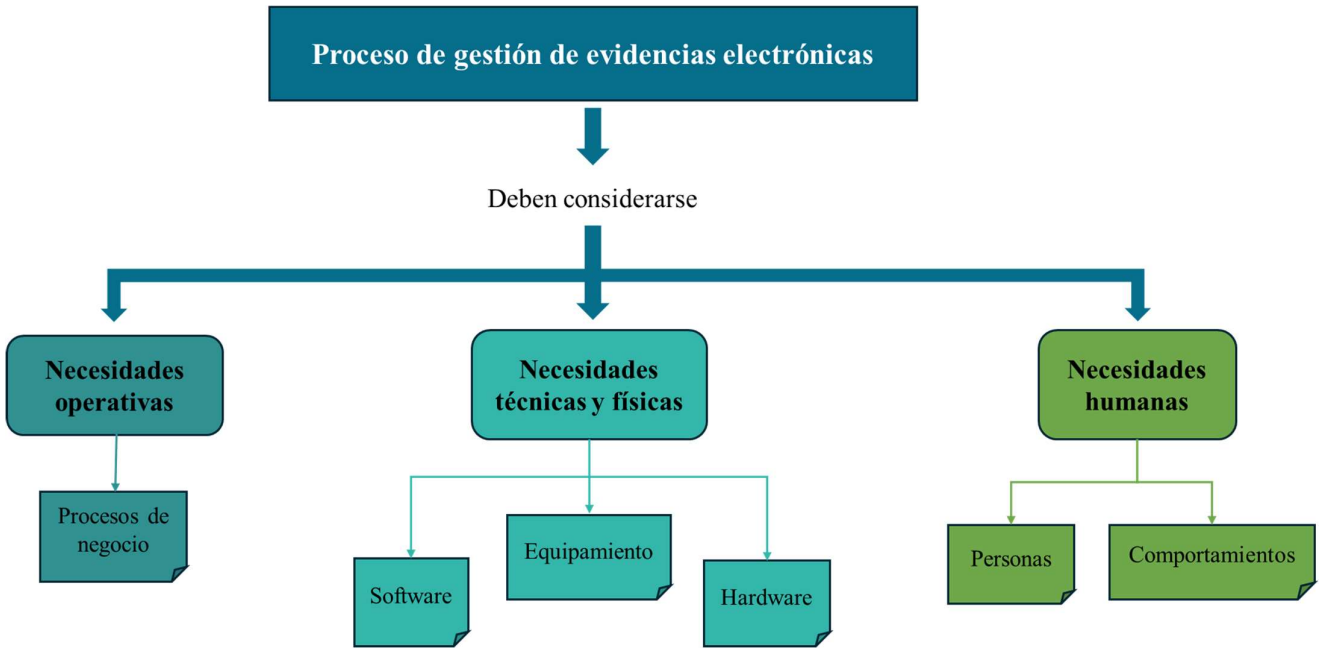

Figura 8. Necesidades a tener en cuenta durante el proceso de gestión de las evidencias electrónicas.

Fuente: Elaboración propia.

Se necesita la realización de un análisis forense detallado de las e-evidencias que confirme la existencia de un incidente, sus causas y consecuencias. Este proceso comienza con la localización de dichas evidencias, que luego serán analizadas siguiendo una metodología forense específica, como la que se presenta en esta guía.

La presente guía está estructurada siguiendo las diferentes fases que componente el proceso de gestión de evidencias electrónicas, como se muestra en la Figura 9.

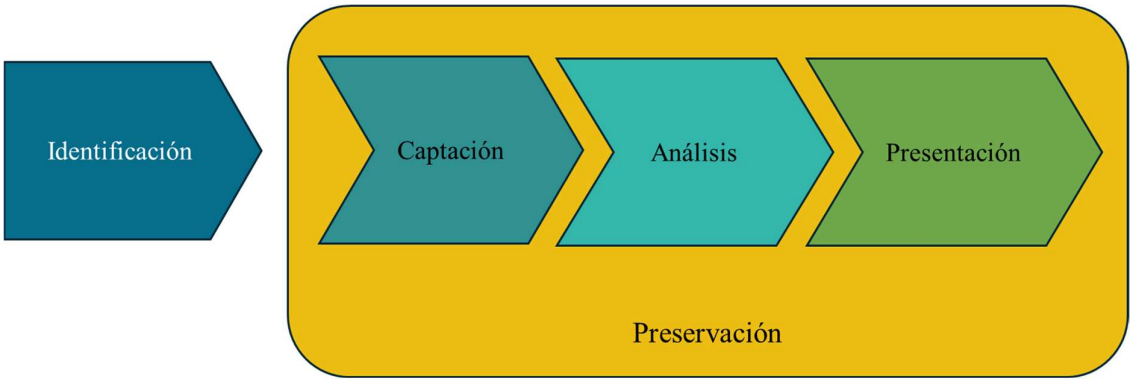

Figura 9. Fases del proceso de gestión de evidencias electrónicas.

Fuente: Elaboración propia.

1. IDENTIFICACIÓN

El proceso de identificación implica la búsqueda, el reconocimiento y la documentación de una potencial evidencia electrónica en la escena de un incidente. Esta fase trata de identificar los dispositivos y medios de almacenamiento digital que puedan almacenar alguna evidencia electrónica que pueda ser relevante al incidente bajo investigación. Dentro de esta fase y una vez identificadas todas las potenciales evidencias, lo más correcto sería priorizar su recolección basándonos en su volatilidad.

La volatilidad de la información debe ser identificada para establecer un orden adecuado de captación, minimizando el daño (pérdida de datos) y, por lo tanto, obteniendo la mejor evidencia posible. Además, durante esta fase del proceso se debe identificar en qué medida es posible que existan evidencias electrónicas ocultas. El personal encargado de llevar a cabo estas tareas debe ser consciente de que no todos los de medios de almacenamiento digital pueden ser fácilmente identificados y localizados; por ejemplo, la computación en la nube, NAS y SAN añaden un componente virtual al proceso de identificación.

Generalmente, en las escenas de incidentes podemos encontrar diferentes tipos de almacenamiento digital, tal y como pueden ser discos duros externos portátiles, unidades flash, CDs, DVDs, discos, cintas magnéticas y tarjetas de memoria. Estos se usan con el fin de almacenar información de los dispositivos electrónicos, y muchas veces son los que contienen las evidencias que buscamos.

Los encargados de identificar las posibles evidencias electrónicas deben realizar una búsqueda sistemática de componentes que puedan contener alguna e-evidencia. Los diferentes tipos de dispositivos electrónicos pueden pasar fácilmente desapercibidos, por ejemplo, debido a su tamaño reducido, disimulados o mezclados entre otros materiales irrelevantes. Además, hay que tener en cuenta que nos podemos encontrar con dos tipos de dispositivo: los dispositivos independientes y los que están conectados a la red.

Se consideran dispositivos digitales independientes aquellos que están desconectados de la red, aunque pueden hallarse vinculados a dispositivos periféricos como son impresoras, escáneres, *webcams*, sistemas GPS o dispositivos RFID. Un dispositivo con una tarjeta de red, pero que, en el momento de su captación, no está conectado a dicha red, debe tratarse como un dispositivo independiente. Si se localiza una computadora con una interfaz de red pero sin ninguna conexión activa, es necesario llevar a cabo acciones para identificar los dispositivos a los que podría haber estado conectada. El personal encargado debe verificar que el dispositivo supuestamente independiente no se haya conectado recientemente a una red. En caso de sospechar de que un dispositivo ha sido desconectado en fechas recientes, se debe tratar como si estuviera conectado a una red para asegurar un manejo adecuado de las otras partes de la red.

Por otra parte, los dispositivos en red, como bien dice su nombre, están conectados a una red ya sea de forma cableada o inalámbrica. Estos pueden ser dispositivos como mainframes, servidores, computadoras de escritorio, puntos de acceso, *switches*, *routers*, dispositivos móviles, PDA, PED, dispositivos Bluetooth, sistemas de CCTV y muchos más. Es importante tener en cuenta que, dado que los dispositivos electrónicos están en red, puede ser complicado localizar la posible evidencia electrónica, ya que los datos pueden estar distribuidos en cualquier parte de la red.

1.1. Priorizar la captación

Puede ser necesario priorizar los elementos según su volatilidad, relevancia o potencial valor probatorio. Los elementos de alta relevancia o valor probatorio potencial son aquellos que probablemente contengan datos directamente relacionados con el incidente bajo investigación.

Sin embargo, la priorización por volatilidad solo es aplicable si las circunstancias específicas del caso en investigación lo requieren. La evidencia digital potencial puede dividirse en dos categorías: volátil y no volátil. Los datos volátiles pueden ser fácilmente destruidos o perdidos para siempre si no se aplica el cuidado necesario. Por ejemplo, retirar la fuente de alimentación de un dispositivo digital puede resultar en la pérdida de datos volátiles.

Por otro lado, los datos no volátiles permanecen en el medio incluso si se retira la fuente de alimentación. Dado que algunos tipos de evidencia electrónica pueden tener una vida útil corta, esta puede ser fácilmente manipulada o dañada. Cuando no está claro si los dispositivos digitales contienen alguna e-evidencia, o qué elementos son más relevantes que otros, puede ser necesario examinarlos antes de la recolección utilizando un proceso para determinar la prioridad. Hay que tener en cuenta que algunos datos volátiles pueden cambiar debido a factores como la ubicación, el tiempo y los cambios en los dispositivos digitales circundantes. Por lo tanto, el responsable se debe asegurar de preservar dichos datos antes de mover el dispositivo.

Durante este proceso se priorizará la adquisición de la evidencia digital potencial más volátil, como por ejemplo, los datos de la memoria RAM, espacio de intercambio, procesos en ejecución, etc. Tras la identificación, el tiempo puede ser un factor limitante, por lo que el responsable debe seguir el orden para la recolección establecido en esta fase y tomar medidas rápidas para recolectar y adquirir los datos volátiles con métodos validados.

No obstante, a parte de la volatilidad de la posible evidencia, debemos tener en cuenta los siguientes aspectos que pueden marcar un orden para realizar el proceso de adquisición:

- La existencia de cifrado de disco completo o volúmenes cifrados donde las contraseñas o claves pueda ser información volátil almacenada en la memoria RAM, tokens externos, tarjetas inteligentes, otros dispositivos o medios.

- La criticidad del sistema.

- Los requisitos legales.

- Otros recursos como, por ejemplo, la capacidad de almacenamiento necesaria, la disponibilidad de personal o las restricciones de tiempo.

1.2. Pautas generales para la identificación de evidencias electrónicas

A continuación se definen un conjunto de directrices generales con miras a la identificación de los dispositivos que posiblemente contengan las evidencias electrónicas que a lo largo de las siguientes etapas se adquirirán y analizarán:

- Documentar el tipo de dispositivo del que se trata, su marca, modelo, número de serie, número de licencia, capacidad y otras marcas identificativas (incluidos los daños físicos).

- Documentar el estado en que se ha encontrado el dispositivo. Hay que tener en cuenta que el estado debe mantenerse sin cambios. Los dispositivos que están apagados, no se deben encender. Los que están encendidos, no se deben apagar. Esto, por simple que parezca, puede prevenir la alteración innecesaria de las evidencias.

- Si un dispositivo debe ser transportado y examinado en una fecha futura indeterminada, puede ser apropiado apagarlo para minimizar el potencial de daño a los datos contenidos en el dispositivo.

- Si hay dispositivos con pantallas que están encendidas, se debe fotografiar o describir aquello que se ver por pantalla (posiciones aproximadas de las ventanas, títulos, contenidos, etc.).

- Los dispositivos con baterías que puedan descargarse debe ser recargado para evitar la pérdida de información. Por lo que también es necesario identificar y recoger posibles cargadores y cables durante esta etapa.

- El responsable también debe considerar usar un detector de señales inalámbricas para detectar e identificar dispositivos que puedan estar ocultos. Puede haber ocasiones en las que un detector de señales inalámbricas no se utilice debido a restricciones de coste y tiempo, en estos casos se debe documentar y justificar las razones por las que no se ha usado.

- Los sistemas que puedan almacenar alguna e-evidencia deben estar protegidos contra el acceso indebido.

Cuando se utilicen escaneos activos, es decir difusión o sondeo, para dispositivos en red, los dispositivos de escaneo deben permanecer apagados hasta que se haya evaluado la posibilidad de que este interactúe con otros dispositivos a investigar. Los miembros del equipo deben recordar que ciertos dispositivos en la escena pueden detectar la presencia de dispositivos de escaneo activo, y el uso de escaneo activo puede desencadenar acciones que podrían estropear la posible evidencia digital y en circunstancias extremas resultar en la activación de trampas ocultas.

1.3. Pautas adicionales para la identificación de evidencias electrónicas

Dependiendo del tipo de dispositivo o de las circunstancias en las que nos los encontramos, a parte de las pautas generales mencionadas en el anterior punto, debemos de seguir una seria de pautas adicionales, como describimos a continuación:

- Para los dispositivos móviles apagados, los datos encontrados dentro de la cavidad de la batería pueden ser esclarecedores, especialmente si se combinan con una base de datos apropiada. Por ejemplo, podemos encontrar el IMEI, que es un número de 15 dígitos que indica el fabricante, el modelo y el país de aprobación para los dispositivos GSM. Asimismo, también podeos encontrar el ESN, un identificador único de 32 bits documentado en un chip seguro en un teléfono móvil: los primeros 8-14 bits identifican al fabricante y los restantes indican su número de serie.

- En el caso de teléfonos móviles, si se conoce el número de teléfono del dispositivo, se puede utilizar una búsqueda inversa para identificar al operador de la red.

- De todos los dispositivos móviles, identificar sus elementos asociados, como tarjetas de memoria, tarjetas SIM, cargadores y bases encontrados. También se debe intentar encontrar el embalaje original de los teléfonos móviles ya que estos podrían contener notas con códigos PIN y PUK.

- Si el dispositivo está en red, identificar los servicios proporcionados por los dispositivos para entender las dependencias y determinar la criticidad de los dispositivos dentro de la red. Una vez hecho esto, se puede tomar la decisión de desconectar o no el dispositivo de dicha red. Esto es importante si los dispositivos están realizando funciones críticas para la misión que no pueden tolerar ningún tiempo de inactividad o para evitar la destrucción de alguna potencial evidencia electrónica. Sin embargo, si parece haber amenazas basadas

en la red en curso para los dispositivos, se puede decidir desconectar el dispositivo de la red para proteger dicha evidencia.

- Si se trata de un sistema de CCTV, se debe anotar el número de cámaras conectadas al sistema, así como cuáles de estas cámaras están en funcionamiento. También se debe anotar configuración básica del sistema, como las configuraciones de visualización, las configuraciones actuales de grabación y la ubicación de almacenamiento para que, si es necesario realizar cambios para facilitar el proceso de adquisición, sea posible devolver el sistema a su estado original.

En el Anexo C se encuentra un formulario que puede ser utilizado como plantilla para comprobar que los aspectos básicos de este proceso de identificación han sido realizados, independientemente del tipo de dispositivo con el que estemos trabajando. El formulario también incluye la comprobación de varios aspectos adicionales, que pueden ser aplicables según las circunstancias.

1.4. Definición del destino final de la evidencia

El destino de los elementos incautados debe ser definido antes de comenzar cualquier actividad de búsqueda e incautación. Las copias forenses, al igual que los sistemas que precisan algún tratamiento específico, deben ser remitidos al departamento o equipo correspondiente para su procesamiento y análisis.

Para cada caso, se debe proporcionar un embalaje, documentación y transporte adecuados para proteger la cadena de custodia que comienza durante la fase de recolección de evidencias.

1.5. Equipo necesario

Es aconsejable tener una lista describiendo el material que se llevará al lugar de recolección de los dispositivos para asegurarse de que todo lo necesario esté disponible y en buen estado. A continuación, se proporciona una plantilla que puede ser personalizada de acuerdo con los elementos necesarios en cada caso.

Es crucial tener suficientes dispositivos en los cuales se almacenarán las imágenes forenses, clones o datos de fuentes remotas. Estos dispositivos deben ser preferiblemente nuevos o, al menos, deben ser limpiados de manera segura sobrescribiendo todos los datos con una secuencia de caracteres conocida, generalmente "00" en hexadecimal, para evitar cualquier posible contaminación de los datos.

La siguiente es una lista que el responsable debe tener en cuenta. Esta consiste en las herramientas forenses mínimas necesarias para que las actividades de identificación, captación y análisis resulten exitosas:

Equipo forense:
◯ Ordenador portátil con las herramientas forenses estándar necesarias instaladas
◯ Bloqueadores de escritura
◯ Credenciales de las licencias herramientas forenses
◯ Almacenamiento de memoria (HDD externos) para imágenes y destino de datos remotos
◯ HDD con software forense adicional o dispositivos de arranque
Herramientas para desmontar:
◯ Destornilladores (planos, estrella, hexagonales y otros específicos para ciertos modelos como Hewlett Packard)
◯ Alicates (estándar y puntiagudos que sirvan para cortar cables)
◯ Pinzas
Documentación de Exhibiciones:
◯ Cámara fotográfica o de video (para tomar fotos de la escena y del contenido de la pantalla)
◯ Rotuladores permanentes (para codificar e identificar el material investigado)
◯ Etiquetas (para marcar e identificar partes del equipo, fuentes de alimentación)
Recursos necesarios para el embalaje y transporte:
◯ Bolsas para evidencia y sellos
◯ Cajas de cartón para evidencia para dispositivos de almacenamiento como USB, DVDs o CDs
◯ Bolsas para evidencia con cierre antiestático
◯ Bolsas Faraday para inhibir señales a teléfonos móviles y otros dispositivos que puedan recibir datos de redes móviles o Wi-Fi

◯ Cinta adhesiva
Otros artículos:
◯ Linterna pequeña con soporte
◯ Guantes
◯ Gomas elásticas
◯ Lupas
◯ Cables de red (cruzados y directos)
◯ Mascarillas

Figura 10. Ejemplo de lista del equipo que va a ser necesario en las distintas fases del proceso de gestión de evidencias.

Fuente: Adaptación de la lista proporcionada por la INTERPOL en su guía "Guidelines for digital forensics first responders".

2. CAPTACIÓN DE EVIDENCIAS ELECTRÓNICAS

Una vez que se han identificado los dispositivos electrónicos que puedan tener almacenadas potenciales evidencias electrónicas, el responsable debe decidir si se adquirirán dichas evidencias *in situ* o si hay que trasladar dichos dispositivos para poder adquirir las evidencias que contienen. La decisión debe estar basada en las circunstancias de cada caso.

2.1. Recolección de dispositivos

La recolección es una fase del proceso de gestión de evidencias digitales, a lo largo de la cual los dispositivos se trasladan de su ubicación original a un laboratorio u otro entorno controlado. Esto se hace con el fin de, posteriormente, adquirir y analizar las evidencias. Estos dispositivos pueden encontrarse en uno de dos estados: pueden estar encendidos o apagados. En función del estado en el que se encuentre el dispositivo, se precisan estrategias y herramientas diferentes.

Este proceso implica registrar detalladamente todo el procedimiento, incluyendo el embalaje de los dispositivos antes de su transporte. Para prevenir la pérdida o daño de la prueba digital, es crucial aplicar un cuidado adecuado. Por ello, se debe determinar el plan de recolección más

adecuado en función de la situación, el coste y el tiempo. Además se debe documentar y justificar la elección del método escogido.

2.1.1. Dispositivos encendidos

El responsable puede seguir un conjunto de directrices para proceder a la recolección de un dispositivo electrónico cuando este está encendido. No todas las pautas son apropiadas para todos los casos, por lo que las categorizamos como generales y adicionales. Las actividades básicas deben aplicarse en todas las circunstancias, mientras que las actividades adicionales deben aplicarse solamente cuando sean relevantes y aplicables, dependiendo del dispositivo o circunstancias únicas.

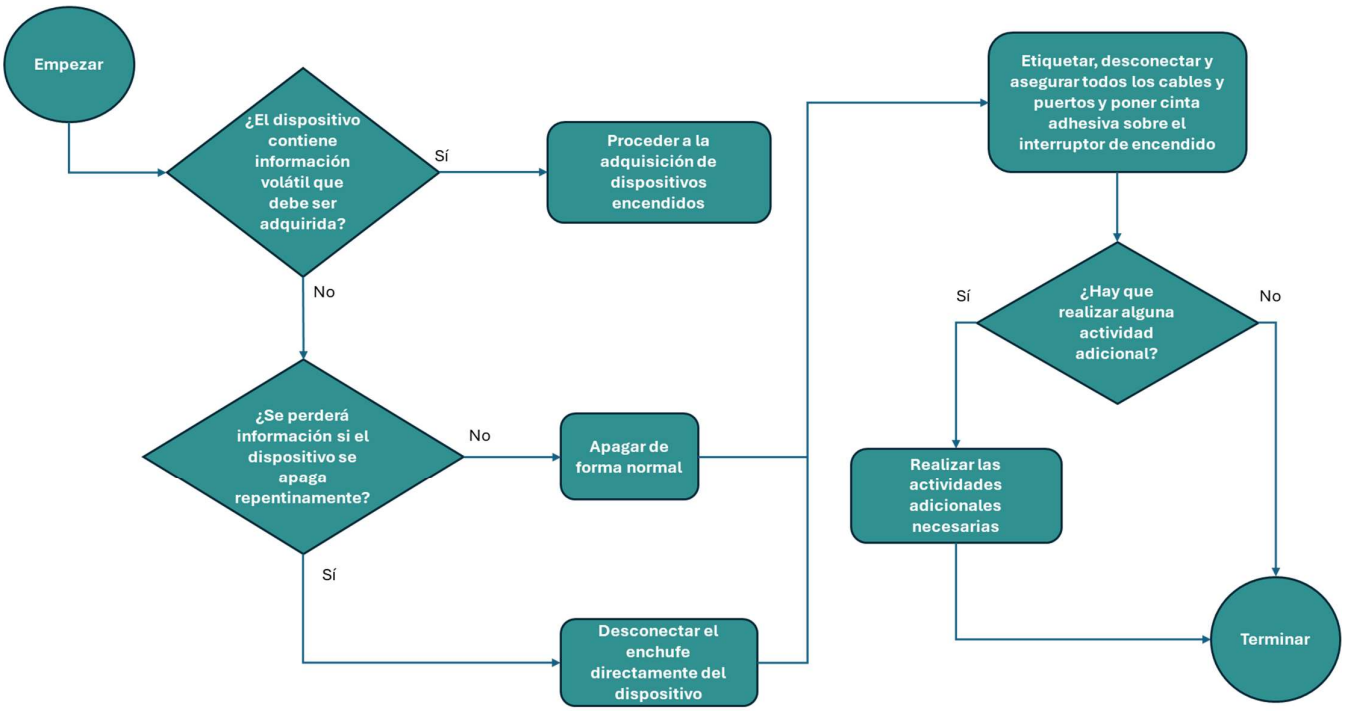

Figura 11. Diagrama de flujo de la recolección de dispositivos encendidos.

Fuente: Elaboración propia.

2.1.1.1. Pautas generales para la recolección de dispositivos encendidos

Las siguientes pautas deben ser seguidas en todos los casos que involucren la recolección de dispositivos que contengan evidencias electrónicas:

- Adquirir la información volátil y el estado actual del dispositivo electrónico antes de proceder con la desconexión del sistema. Las claves de cifrado y otra información crucial pueden residir en la memoria activa o inactiva que todavía no ha sido borrada. Realizar una adquisición lógica cuando se sospeche de cifrado. En este caso, tener en cuenta que el sistema operativo en vivo puede no ser confiable, por lo que se deben considerar el uso de herramientas apropiadas, confiables y validadas.

- La configuración del equipo puede definir si este se debe apagar mediante procedimientos administrativos normales o si se debe desconectar directamente el enchufe. En este caso se debe determinar el mejor enfoque según las circunstancias específicas. Si se decide desconectar el enchufe, retirar el cable de alimentación primero del extremo conectado al dispositivo, no del extremo conectado a la toma de corriente. Tenga en cuenta que un dispositivo conectado a un UPS puede tener datos alterados si el cable de alimentación se retira de la pared y no del dispositivo.

- Etiquetar, desconectar y asegurar todos los cables del equipo y etiquetar los puertos. Esto se hace con el fin de que el sistema pueda reconstruirse en una etapa posterior.

- Si es necesario, colocar cinta adhesiva sobre el interruptor de encendido con el fin de proteger el dispositivo contra un cambio de estado.

Hay que tener en cuenta que si se retira la energía de un dispositivo digital encendido, cualquier potencial evidencia digital almacenada en volúmenes cifrados será inaccesible, a menos que se obtenga la clave. Además se pueden perder datos en vivo potencialmente valiosos por lo que el responsable debe asegurarse de que los datos volátiles se recolecten antes de retirar la fuente de alimentación.

2.1.1.2. Pautas adicionales para la recolección de dispositivos encendidos

Las siguientes son algunas pautas adicionales, relevantes dependiendo de la configuración del dispositivo:

- Si se trata de un ordenador portátil, se debe adquirir la información volátil previo a retirar la batería. Luego, retirar la fuente batería principal (no presionar el interruptor para apagarla). Además, se debe tomar nota de si hay un adaptador de corriente presente. Si lo hay, retirar dicho adaptador después de retirar la batería. A veces, la acción de presionar el botón de encendido en un dispositivo puede estar configurada para iniciar un script que pueda modificar o eliminar datos del equipo antes de apagarse, o para advertir a los sistemas conectados de que ha ocurrido un evento inesperado para que puedan borrar datos de valor probatorio antes de ser identificados.

- Colocar cinta adhesiva sobre la ranura del disquete.

- Asegurarse de que las bandejas de las unidades de CD o DVD estén retraídas en su lugar; anotar si están vacías, contienen discos o no han sido revisadas; y cerrar la ranura de la

unidad con cinta adhesiva para evitar su apertura. Si se deja cualquier medio de arranque dentro, cuando la máquina se vuelva a encender, podría arrancar desde ese medio en lugar de desde el disco duro (o la unidad flash de herramientas forenses), dependiendo de la configuración del BIOS de la computadora.

2.1.2. Dispositivos apagados

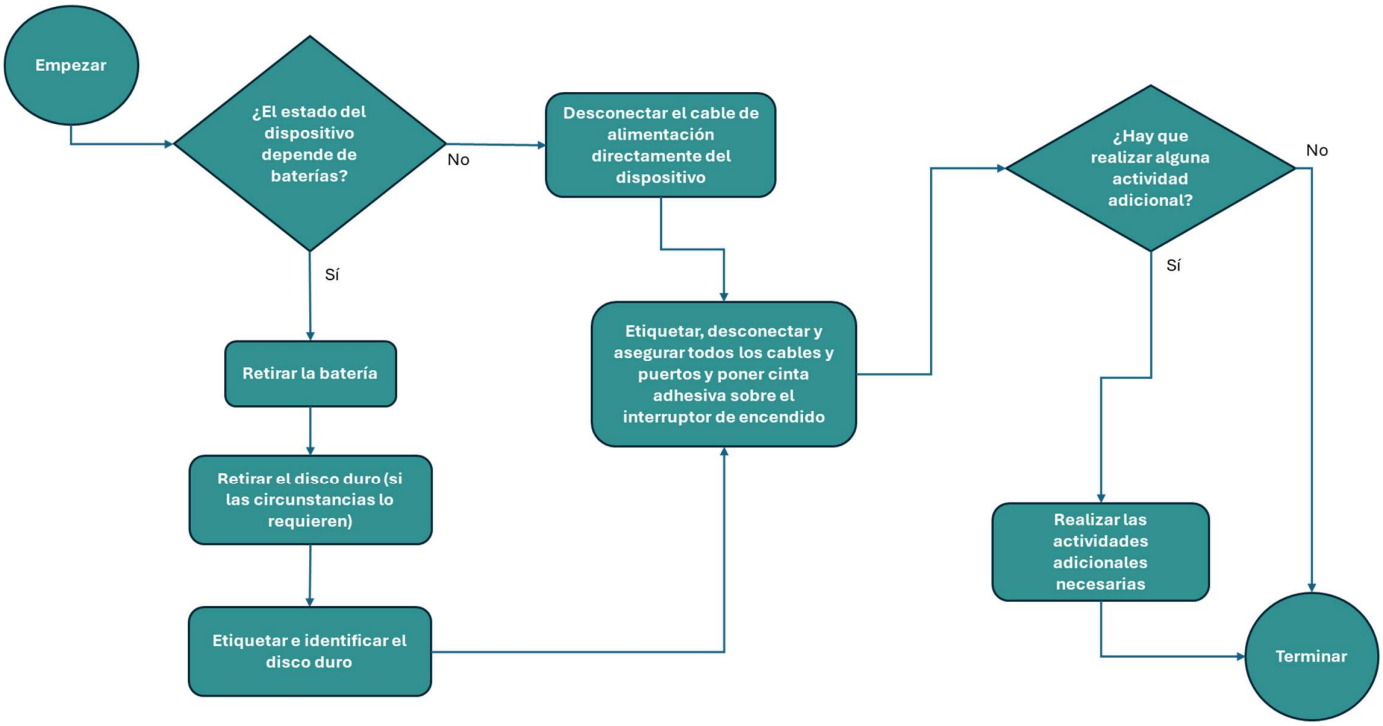

Ilustración 12. Diagrama de flujo de la recolección de dispositivos apagados.

Fuente: Elaboración propia.

2.1.2.1. Pautas generales para la recolección de dispositivos apagados

Las siguientes son las actividades básicas recomendadas para la recolección cuando el dispositivo está apagado:

- Retirar el cable de suministro eléctrico, retirando primero el extremo que está conectado al dispositivo, no el extremo conectado al enchufe.

- Desconectar y asegurar todos los cables de los dispositivos y etiquetar los puertos para que el sistema pueda reconstruirse más adelante.

- Si es necesario colocar cinta adhesiva sobre el interruptor de encendido para evitar que el dispositivo cambie de estado.

En la mayoría de los casos, el medio de almacenamiento no debe ser retirado del dispositivo hasta que vayan a ser adquiridas las evidencias, ya que retirarlo aumenta el riesgo de dañarlo o confundirlo con otro.

2.1.2.2. Pautas adicionales para la recolección de dispositivos apagados

A continuación se exponen las tareas adicionales que pueden ser relevantes para la recolección de dispositivos apagados, dependiendo de la configuración específica de dichos dispositivos:

- Asegurarse de que el ordenador portátil esté realmente apagado, ya que algunos pueden estar en suspensión. Luego, retirar la batería principal del portátil.

- Si las circunstancias exigen la extracción del disco duro, el encargado debe asegurarse de descargar la electricidad estática del dispositivo electrónico con el fin de impedir que esta dañe el disco duro. Si no es factible, no se debe proceder a la extracción. Etiquetar el disco duro como disco sospechoso y documentar sus detalles como se hizo con los demás dispositivos en la fase de identificación.

- Colocar cinta adhesiva sobre la ranura del disquete.

- Asegurarse de que las bandejas de las unidades de CD o DVD estén retraídas en su lugar; anotar si están vacías, contienen discos o no han sido revisadas; y cerrar la ranura de la unidad con cinta adhesiva para evitar que se abra.

2.1.3. Medios de almacenamiento

Diversos tipos de medios de almacenamiento digital pueden encontrarse en la escena de un incidente. Por lo general, estos son los tipos de datos menos volátiles y pueden tener la menor prioridad durante la recolección y adquisición. Esto no significa que no sean importantes, ya que en muchos casos, los medios de almacenamiento digital externos contienen las pruebas que los analistas están buscando. Para recolectarlos hay que proceder de la siguiente manera:

- Realizar el proceso de identificación previo a la adquisición.

- Etiquetar todos los sistemas de almacenamiento identificados y cualquier parte asociada con ellos. Las etiquetas de evidencia no deben colocarse directamente en las partes mecánicas del medio digital ni deben cubrir u ocultar información importante. Estos medios deben almacenarse de manera que se garantice su integridad. Siempre que sea posible, la evidencia debe sellarse con sellos a prueba de manipulaciones y el personal encargado debe firmar en la etiqueta.

- Los medios de almacenamiento digital recolectados deben almacenarse en un entorno adecuado para la preservación de los datos.

- Diferentes medios de almacenamiento digital tienen diferentes capacidades de retención de datos. Por lo tanto, se debe estar al tanto del período máximo de tiempo aceptable de retención de dicho datos.

2.2. Adquisición de evidencias electrónicas

Un principio clave en la informática forense es trabajar con imágenes, copias o clones a bajo nivel de la información original. Por esta razón, la adquisición consiste en crear una copia de la evidencia electrónica, ya sea de un disco duro completo, una partición o archivos específicos, y en documentar las técnicas usadas y actividades realizadas. Es crucial seleccionar un método de adquisición apropiado a la situación, el coste y el tiempo disponible, y registrar detalladamente la elección del método y las herramientas empleada.

Los métodos usados para adquirir evidencias electrónicas deben ser reproducibles y repetibles o, al menos, verificables por un especialista forense competente. Además se debe capturar la evidencia de la forma menos invasiva posible con el fin de no introducir ningún cambio. Si el proceso resulta en una alteración inevitable de la información digital, las actividades realizadas deben documentarse para explicar los cambios en los datos y la razón de esos cambios.

El método de adquisición usado debe crear una copia de los datos originales, es decir, debemos realizar un clonado forense. Tanto la fuente original como la copia de la evidencia deben ser verificadas con una función *hash*, comprobando que ambas funciones producen el mismo resultado, probando así que son idénticas.

En circunstancias en las que no se pueda realizar el proceso de verificación, por ejemplo, al adquirir un dispositivo en funcionamiento, cuando la copia original contiene sectores con errores o el tiempo para la adquisición es limitado, se debe emplear el mejor método disponible y justificar adecuadamente la elección de este. Si la imagen no puede ser verificada, es necesario documentar y explicar esta limitación. Cuando no se pueda realizar el proceso de verificación en toda la fuente debido a errores en la misma, se puede utilizar la verificación de aquellas partes de la fuente que sean legibles de manera fiable. Además, en caso de que sea necesario, el método de adquisición utilizado debe ser capaz de capturar el espacio asignado y no asignado del dispositivo.

En ciertas circunstancias, puede no ser posible o permitido realizar una copia completa del dispositivo, por ejemplo, si se requiere una cantidad de almacenamiento demasiado grande para guardar la copia. En tales casos, se puede optar por una adquisición lógica que se centre únicamente en la información relevante. Esta adquisición efectúa generalmente a nivel de archivos y particiones, permitiendo la copia de archivos activos y otros datos almacenados en el espacio asignado. Dependiendo del método utilizado, es posible que los archivos eliminados y el espacio no asignado también sean copiados. Este enfoque resulta especialmente útil en situaciones donde se manejan sistemas críticos que no pueden ser apagados.

Si no se dispone de un equipo especializado en la adquisición de e-evidencias, se sugiere que al menos dos personas formen parte del equipo de adquisición y que cuenten con la ayuda de algún tipo de personal técnico especializado que sí cuente con las competencias necesarias. Los técnicos encargados de la adquisición deben estar debidamente autorizados para realizarla, por lo que si la adquisición es llevada a cabo por técnicos externos a la organización, debe existir un contrato de servicio firmado previamente entre las partes. En el caso de técnicos internos, deben tener una autorización escrita válida.

En cualquier caso, para garantizar la independencia en las actuaciones forenses, se recomienda la presencia de un fedatario público, como un secretario judicial o notario, o de terceros independientes, como delegados sindicales o peritos externos, que certifiquen el proceso.

El personal responsable de la adquisición debe adherirse a un procedimiento de adquisición documentado y emplear herramientas de hardware y software reconocidas en el campo forense. Además, deben registrar de manera documental o electrónica los pasos esenciales realizados y la metodología utilizada durante la adquisición, incluyendo un historial temporal detallado para garantizar la integridad de la cadena de custodia. Una lista de las funcionalidades que deben estar presentes estas herramientas software y hardware se encuentra en el Anexo D.

De igual forma, conviene no separar los soportes digitales de almacenamiento de los equipos en los que están ubicados, especialmente en los sistemas de videograbación o sistemas cerrados de televisión (CCTV) y ordenadores portátiles. Asimismo, en sistemas conectados a redes cableadas o inalámbricas, el personal técnico debe identificar la ubicación de almacenamiento de la información relevante, diferenciando entre almacenamiento centralizado y distribuido.

Al igual que en el proceso de recolección, los métodos de adquisición varían dependiendo del estado en el que se encuentra el dispositivo en ese momento, es decir, depende de si este está encendido o apagado.

2.2.1. Dispositivos encendidos

El análisis forense de estos sistemas, conocido como *Live Forensics*, se enfoca en los equipos que están en funcionamiento, destacando la importancia de la información volátil, principalmente aquella almacenada en la memoria RAM, ya que se pierde cuando el dispositivo se apaga. Para preservar esta información, es necesario realizar la adquisición directamente desde el sistema operativo activo, minimizando la alteración o impacto en el mismo, y luego proceder al análisis siguiendo la misma metodología aplicada en los sistemas apagados.

Con el fin de garantizar la validez de estas e-evidencias, y considerando que la adquisición de un dispositivo en funcionamiento implica el uso de técnicas intrusivas, por lo que se deberían seguir las siguientes recomendaciones:

- Documentar todos los procesos efectuados.

- Es importante reconocer que estas técnicas no garantizan su reproducibilidad. Por lo tanto, la validez de los resultados obtenidos está fuertemente ligada a la forma en que se justifiquen en el informe pericial correspondiente.

- Describir en detalle la metodología empleada durante la adquisición de datos en sistemas en funcionamiento. Además, es crucial indicar si se ha reducido al mínimo posible el impacto de las técnicas intrusivas utilizando los dispositivos de *hardware* adecuados o mediante *software*, activando comandos bien establecidos, si se accede a la evidencia mediante un entorno remoto.

- Prestar especial atención a la existencia de discos cifrados o archivos que requieran contraseñas para su acceso, así como al análisis de *software* dañino o malicioso (*malware*) de diversos tipos.

Se pueden seguir varias instrucciones para la adquisición cuando el sistema se encuentra encendido. Sin embargo, no todas las pautas son apropiadas para todos los casos. En consecuencia, las pautas se pueden categorizar como generales y adicionales, al igual que se hizo en la recolección. Además, utilizar métodos confiables debería minimizar las implicaciones de acciones que puedan modificar las evidencias.

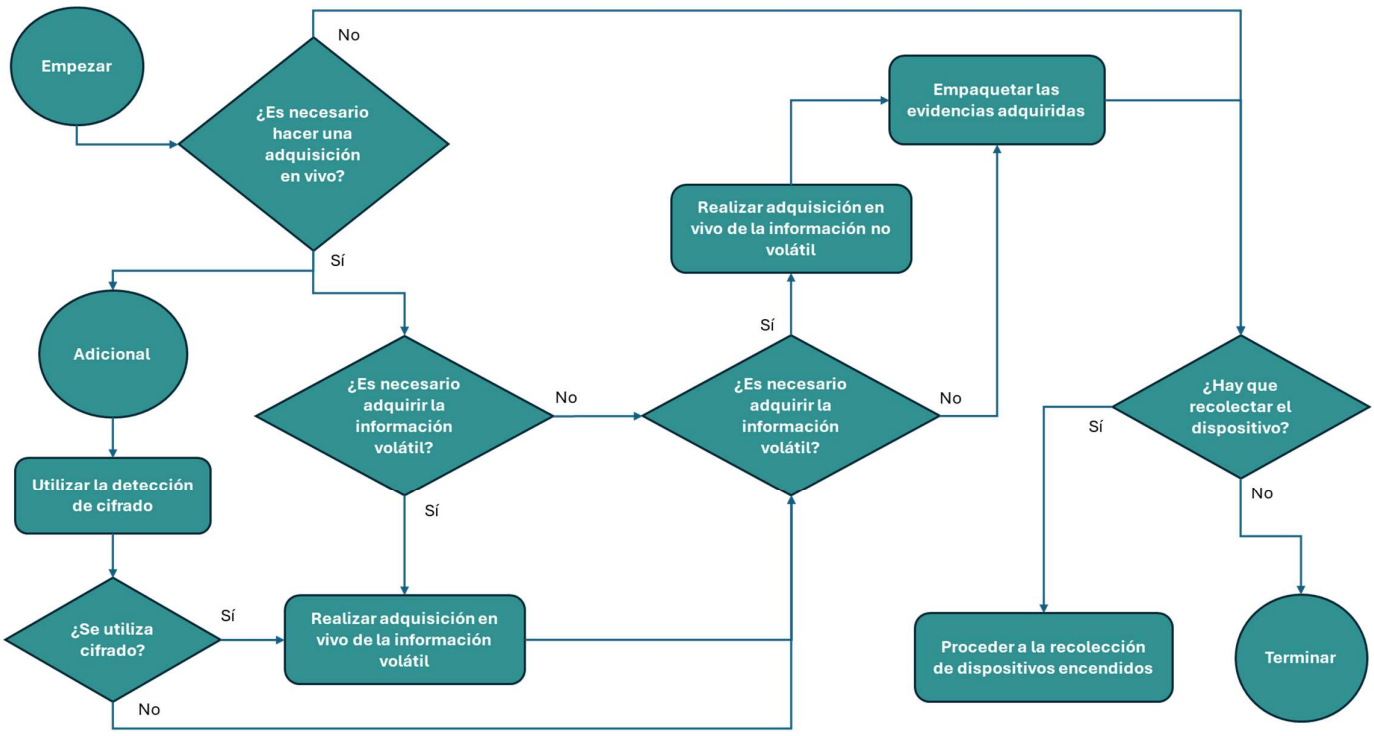

Figura 13. Diagrama de flujo de la adquisición de dispositivos encendidos.

Fuente: Elaboración propia.

2.2.1.1. Pautas generales para la adquisición de dispositivos encendidos

A continuación, se presentan las actividades básicas que se deben seguir en todos los casos que involucren la adquisición de evidencias en dispositivos digitales encendidos:

- Comenzar adquiriendo los datos volátiles, es decir, los datos almacenados en la RAM, los procesos en ejecución, las conexiones de red y la configuración de fecha y hora. La adquisición en vivo es necesaria para obtener este tipo de datos de dispositivos que aún están funcionando, ya que estos pueden contener información valiosa como el estado de la red, aplicaciones desencriptadas y contraseñas. Se puede realizar en la consola o remotamente, es decir, a través de la red. Aunque estos procesos son diferentes y requieren el uso de diferentes conjuntos de herramientas.

- No confiar en los programas del sistema. Por esta razón, el responsable debe ser competente en el uso de herramientas validadas y debe ser capaz de explicar los efectos que estas herramientas pueden tener en el sistema (por ejemplo, desplazamiento de evidencia digital potencial, contenido de la memoria que se pagina cuando se carga el software, etc.). Todas las acciones realizadas y los cambios resultantes deben documentarse y justificarse. Si no es posible determinar el efecto que tendría introducir herramientas en el sistema o los cambios resultantes no se pueden determinar con certeza, también se debe documentar.

- Al adquirir datos volátiles, usar un contenedor de archivos lógico siempre que sea posible y documentar su valor hash una vez que contenga los archivos de datos volátiles. Cuando esto no sea posible, se debe usar un contenedor como un archivo ZIP, luego se debe realizar un *hash* de este archivo y documentar su valor. Los contenedores de archivos resultantes deben almacenarse en un medio de almacenamiento digital que haya sido formateado para este propósito. En estos casos en los que el dispositivo esta encendido, el *hash* es dinámico, es decir, según el instante temporal en que se efectúe se obtendrá uno distinto. Aun así, su uso en sistemas encendidos no debería afectar a su posible valor legal.

- Ejecute el proceso de creación de imagen en el almacenamiento no volátil en vivo utilizando una herramienta de creación de imágenes validada. La copia de la evidencia digital resultante debe guardarse en un medio de almacenamiento digital que haya sido preparado para este propósito. Aunque es preferible usar un medio de almacenamiento digital nuevo, el uso de copias de evidencia digital de procesos validados asegura la integridad de los datos cuando se reconstruyen. Por lo tanto, un medio de almacenamiento digital que haya sido saneado será suficiente.

- Si la imagen debe almacenarse en un contenedor de archivos lógico, asegurarse de que la imagen no pueda ser corrompida o dañada.

2.2.1.2. Pautas adicionales para la adquisición de dispositivos encendidos

Las pautas adicionales que son relevantes para la adquisición de dispositivos digitales encendidos, dependiendo de la configuración del dispositivo digital específico, son las siguientes:

- Adquirir los datos volátiles en la RAM cuando se sospeche el uso de cifrado. Primero, verificar la sospecha inspeccionando el disco en bruto o utilizando alguna utilidad de detección de cifrado. El sistema operativo en vivo puede no ser confiable, por lo que se deben usar herramientas confiables y validadas.

- Usar una fuente de tiempo confiable y documentar la hora de cada acción realizada.

- Asociar al responsable de la adquisición con la evidencia digital adquirida utilizando firmas digitales, biometría o fotografía.

- **Dispositivos móviles**

Debido a la capacidad de estos dispositivos para conectarse a redes inalámbricas, es crucial proteger o aislar adecuadamente los dispositivos móviles para prevenir la manipulación accidental de los datos almacenados y evitar que se modifiquen los archivos internos relacionados con su ubicación y la celda de radiocomunicaciones.

Una metodología a seguir para la adquisición de información contenida en estos dispositivos móviles encendidos debe ser la siguiente:

- Realizar una copia o clonado de las secciones accesibles de la tarjeta SIM original utilizando un lector de tarjetas con su *software* correspondiente, y luego insertar esta tarjeta clonada en el dispositivo móvil. Al no tener las credenciales de acceso a la red inalámbrica de la tarjeta SIM original, la tarjeta clonada previene que el dispositivo se conecte a la red, eliminando la necesidad de procesar las evidencias dentro de una cámara de Faraday o equipo similar.

- Después de iniciar el terminal móvil con la tarjeta clonada insertada, realizar una copia a nivel bajo de los datos almacenados en la memoria o memorias internas del dispositivo.

- Si las herramientas forenses no son compatibles con un modelo específico de dispositivo móvil o si no se cuenta con el cableado adecuado, se puede documentar los datos visibles en la pantalla del dispositivo en el informe pericial. Alternativamente, se puede seguir el mismo procedimiento que con los sistemas apagados: extraer la información de la memoria del dispositivo mediante *hardware* especializado y luego utilizar el *software* adecuado para interpretar los datos obtenidos.

Toda la información obtenida de las memorias del dispositivo móvil debe ser resumida digitalmente utilizando un algoritmo criptográfico para crear un *hash*. Esto asegura que los datos extraídos no se alteren si es necesario realizar copias adicionales o imágenes de los mismos.

- **Entornos virtualizados**

En entornos virtualizados, uno o más equipos físicos se simulan dentro de una máquina física, utilizando sus recursos disponibles. De este modo, estos equipos virtuales operan simultáneamente como si fueran dispositivos físicos independientes.

El entorno virtualizado puede encontrarse en un equipo local o en un entorno empresarial, y la tecnología empleada puede ofrecer una virtualización completa o parcial, dependiendo del hardware del equipo o del software utilizado. Cada máquina virtual en este entorno está compuesta por varios archivos, incluyendo el de configuración del *hardware*, el de memoria, y uno o varios discos duros, ya sean físicos o virtuales. Estos discos duros virtuales se representan mediante archivos de imagen con extensiones como **.vhd, *.vmd, *.img*, entre otros. Estos se almacenan en los dispositivos o sistemas de almacenamiento disponibles en el equipo que aloja el entorno virtualizado.

La información que se debe capturar con herramientas forenses es la siguiente:

- Los discos duros virtuales, es decir, los archivos de imagen.

- Si se suspende el equipo virtual, sería posible obtener un volcado de la memoria RAM utilizada en un archivo que, posteriormente, debería analizarse de manera similar al volcado de una memoria física real.

En este ámbito, una vez obtenidos todos los ficheros de configuración de la máquina virtual y los discos virtuales utilizados, se podrá recrear el entorno original del equipo virtualizado para llevar a cabo su análisis forense.

2.2.2. Dispositivos apagados

Es más fácil manejar un dispositivo digital apagado en comparación con un dispositivo digital encendido porque no es necesario adquirir los datos volátiles. Durante la adquisición de los datos guardados en un sistema apagado, es importante seguir las siguientes recomendaciones generales:

- El medio digital destinado a almacenar el clonado forense o copia de los datos originales debe ser sometido a un borrado seguro y estar dentro de su periodo de vida útil. Este no debe contener información previa, por lo que debe ser testeado de forma segura.

- Asegurarse de que el dispositivo esté realmente apagado.

- Usar dispositivos bloqueadores para prevenir la escritura de datos nuevos sobre los ya almacenados, para así garantizar la no alteración de los datos originales.

- Si es apropiado, retirar el almacenamiento del dispositivo digital apagado. Etiquetar dicho almacenamiento como sospechoso y documentar todos los detalles como se hizo en el proceso de identificación.

- Efectuar un *hash* de la información original al mismo tiempo que se realiza el proceso de clonado u adquisición de la imagen a bajo nivel, utilizando herramientas *hardware* o *software* validadas en el ámbito forense.

- Ejecutar el proceso de creación de imágenes utilizando una herramienta de creación de imágenes validada para crear una copia de evidencia electrónica.

- Efectuar un *hash* de la información copiada, comprobando que este y el original coinciden, lo cual asegura la integridad de los datos almacenados tanto en el disco original como en las copias o imágenes sucesivas que se generen.

Posteriormente los discos medios originales deben ser nuevamente precintados y sellados junto con los equipos en los que estaban instalados, y almacenados en un área designada específicamente para ese propósito.

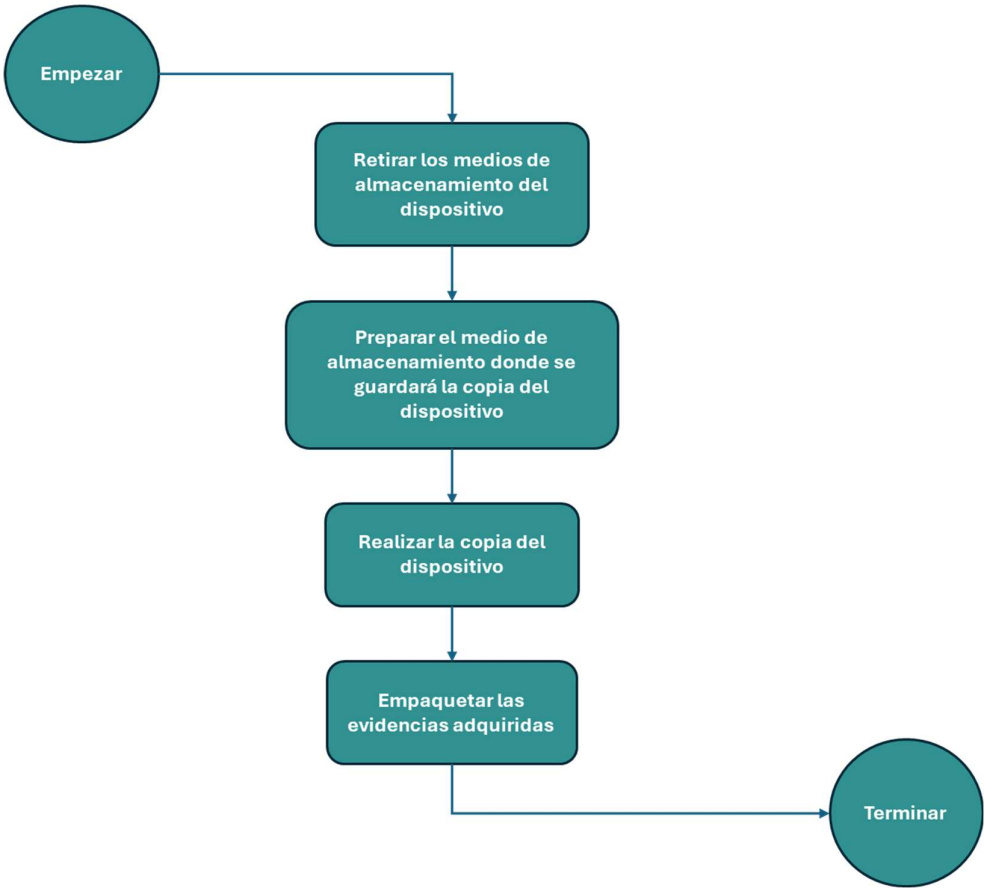

Figura 14. Diagrama de flujo de la adquisición de dispositivos apagados.

Fuente: Elaboración propia.

- **Dispositivos móviles**

Un caso particular dentro de estos sistemas apagados son los dispositivos móviles. En estos casos, es crucial estudiar y extraer la información de la tarjeta SIM, siempre que se disponga del número PIN o PUK correspondiente. En ausencia de estos, se debe solicitar el número PUK a la operadora de telefonía propietaria de la tarjeta mediante una autorización judicial, utilizando el número ICCID de la tarjeta como referencia.

También existe información en el terminal móvil, por lo que es necesario realizar una copia a bajo nivel de los datos almacenados en la memoria o memorias internas del dispositivo, incluyendo archivos de audio, imágenes, entre otros.

Toda la información obtenida de la tarjeta SIM y de las memorias del dispositivo móvil debe ser resumida en un *hash* utilizando un algoritmo criptográfico. Esto asegura que los datos extraídos no se alteren, por si fuese necesario crear copias adicionales o imágenes de los mismos.

- **Dispositivos críticos**

En algunos casos, los dispositivos digitales no pueden ser apagados debido a la naturaleza crítica de los sistemas. Estos sistemas, como servidores en centros de datos que también podrían estar prestando servicios a clientes inocentes, sistemas de vigilancia, sistemas médicos y muchos otros que podrían verse afectados si se interrumpen o apagan. Se debe tener especial cuidado al tratar con estos sistemas.

Cuando el dispositivo digital no se pueda apagar, se debe realizar una adquisición en vivo o parcial.

2.3. Adquisición parcial

La adquisición parcial puede realizarse por varias razones, tales como:

- La capacidad de almacenamiento del dispositivo excede los límites para poder adquirirse.
- Un dispositivo es demasiado crítico para ser apagado.
- Cuando aparte de la información de interés hay otros datos irrelevantes dentro del mismo sistema.
- Cuando la adquisición está limitada por la autoridad legal, como una orden de registro.

Cuando se decide efectuar una adquisición parcial, las actividades de adquisición deben incluir las siguientes actividades:

- Identificar carpetas, archivos o cualquier opción de sistema relevante para adquirir los datos deseados.

- Realizar una adquisición lógica de esos datos identificados.

3. ANÁLISIS

En esta parte del proceso el objetivo principal es dar respuesta a preguntas relacionadas con el tiempo de intrusión, su origen, dispositivos afectados, métodos de intrusión utilizados, así como la lista de datos alterados y/o accedidos, además de cualquier otra actividad realizada en las evidencias que puede ser relevante. Todas estas tareas deben ser realizadas de forma metódica, auditable, repetible y defendible.

Las siguientes son las acciones previas que se deben tener en cuenta durante análisis de las evidencias electrónicas:

1. Comprobar que el objeto y alcance está dentro de nuestra competencia.

2. Estudiar la documentación adjunta a las evidencias electrónicas para componer un mapa contextual de las mismas, estableciendo relaciones que pudieran tener dichas evidencias entre sí y con los distintos implicados en el hecho bajo estudio.

3. Supervisar la cadena de custodia previa, respondiendo a las preguntas sobre qué evidencias se tomaron, quién las recolectó, dónde se encontraron y cuándo se realizaron las recolecciones. También es necesario verificar quién fue el responsable y dónde se almacenaron las evidencias hasta que llegaron al lugar de análisis.

4. Solicitar las autorizaciones necesarias.

5. Comprobar que las evidencias no están deterioradas y, por lo tanto, se pueden estudiar.

6. Si aparecen nuevas evidencias que no habían sido contempladas en un principio, iniciar nuevo proceso de gestión, custodia y trazabilidad comenzando con su identificación. Más allá de esto, se debe informar al solicitante del análisis sobre la existencia de tales evidencias y, si es necesario, obtener los permisos pertinentes para proceder con su estudio.

7. Especificar la hora de la BIOS del equipo informático en el que se encuentran instalados los discos duros o medios digitales que contienen la información relevante.

8. Establecer criterios de prioridades.

Es probable que el análisis sea un proceso iterativo, ya que el análisis de una evidencia puede llevar a reconsiderar otras. La identificación y evaluación solo pueden llevarse a cabo con información contextual suficiente que permita al responsable tomar decisiones informadas sobre cada elemento en consideración (por ejemplo, información sobre el incidente sospechoso, el sistema en cuestión y la naturaleza de las fuentes de evidencia electrónica que se están examinando). Por lo tanto, el personal encargado debe ser competente para realizar sus funciones en el análisis.

Los procesos utilizados para examinar la evidencia electrónica deben estar completamente validados para sus funciones en la investigación. De igual manera, no deben alterar ni dañar su contenido. Si existe la posibilidad de daño a la evidencia, se deben tomar las medidas necesarias para minimizar este riesgo (por ejemplo, usando un bloqueador de escritura para minimizar la posibilidad de modificar inadvertidamente el contenido de un disco duro). Sin embargo, si el daño es inevitable, se debe justificar por qué se ha realiza la acción que ha resultado en tal daño.

Si se sospecha de que se ha hallado alguna evidencia relacionada con un incidente diferente, este hecho se debe comunicar inmediatamente al encargado de la investigación y esperar nuevas instrucciones. Los responsables deben consultar con las autoridades pertinentes antes de proseguir con la investigación, ya que exceder la autoridad del mandato de investigación puede hacer que todos los resultados (no solo aquellos relevantes para el incidente recién descubierto) sean inutilizables en procedimientos legales y administrativos.

Los encargados del análisis deben ser imparciales. Esto quiere decir que si se encuentra una evidencia que refuta o apoya la premisa, esto debe ser reportado junto con la evidencia que lo respalda. Igualmente, un investigador independiente, no relacionado con la investigación, debería ser capaz de examinar los procesos y decisiones tomados por el equipo original y lograr los mismos resultados. Para que esto ocurra, se debe haber seguido una secuencia debidamente documentada de procesos atómicos (normalmente definidos dentro del contexto de procesos validados por separado), que hayan sido registrados manteniendo registros detallados.

3.1. Uso de herramientas

Las herramientas (combinaciones de *software*, *hardware* y *firmware*) pueden ser de gran ayuda en el proceso de análisis. La elección de herramientas debe estar fundamentada en los requisitos establecidos y en los procedimientos que forman parte del análisis.

Por otro lado, las actividades que involucren nuevas herramientas deben pasar por un proceso de validación y confirmación antes de su implementación. El concepto de validación requiere considerar el uso previsto de la herramienta. Por lo tanto, el requisito es únicamente validarlas para la forma en que se utilizará en la investigación. Una herramienta que se sabe que tiene defectos aún puede ser utilizada, siempre que se demuestre que el proceso en el cual participa la herramienta es adecuado para su uso previsto.

3.2. Tipos de análisis

3.2.1. Análisis estático

El análisis estático normalmente se realiza sobre una copia de la evidencia electrónica original para evitar su alteración o destrucción accidental. Este consiste en la inspección de posibles evidencias digitales con el fin de determinar su valor como prueba digital (por ejemplo, identificando artefactos, construyendo cronologías de eventos, examinando el contenido de archivos y datos eliminados...). En este proceso simplemente se realiza una inspección de las evidencias y se interpretan los resultados utilizando procesos adecuados (por ejemplo, cargándolas en visores apropiados), pero nunca se pondrá en marcha ningún código ejecutable.

Este método es especialmente adecuado para el análisis de datos consecuentes (contenidos de archivos de registro, contenidos de paquetes de red, contenidos de volcado de memoria) y metadatos (permisos de archivos y marcas de tiempo). Sin embargo, en algunas instancias puede que el análisis estático no sea suficiente para comprender completamente la importancia de las evidencias digitales, como puede ser en casos de intrusión o exfiltración de datos mediante malware.

3.2.2. Análisis en vivo

En algunas circunstancias, puede ser necesario o beneficioso examinar una versión en vivo de la evidencia electrónica. Esto puede ser particularmente útil cuando se trata de sistemas como mensajería instantánea, smartphones/tabletas, intrusión en redes, redes complejas, dispositivos de almacenamiento cifrados o código polimórfico sospechoso.

Existen dos formas distintas de análisis en vivo:

- Análisis en vivo de sistemas que no pueden ser copiados ni clonados.

- Análisis en vivo de sistemas que pueden ser copiados o clonados.

3.2.2.1. Análisis en vivo de sistemas no copiables ni clonables

Cuando no es posible, por razones técnicas u operativas, o cuando existe un riesgo significativo de pérdida de evidencias digitales al intentar clonar o copiarlas, puede ser necesario realizar un análisis en vivo en un sistema saltándose el proceso de adquisición.

En estas circunstancias, los investigadores deben tener mucho cuidado para minimizar el riesgo de dañar las evidencias digitales, ya que se trata de las originales, y deben asegurarse de tener un registro completo y detallado de todos los procesos realizados. Se debe garantizar que cualquier persona que realice un análisis en vivo esté completamente capacitada para hacerlo y sea capaz de explicar sus procesos, así como cualquier alteración de los datos.

3.2.2.2. Análisis en vivo de sistemas copiables o clonables

Cuando un sistema sí puede ser copiado o clonado, puede ser adecuado o necesario examinar dicho sistema interactuando directamente con él u observándolo en funcionamiento. En tales circunstancias, se debe emular, en *hardware* o *software*, el entorno original lo más fielmente posible, utilizando máquinas virtuales verificadas, copias del *hardware* original o incluso, pero no recomendable, el hardware original real para permitir un análisis en vivo.

Es necesario adoptar las acciones adecuadas para asegurar que cualquier cambio necesario para permitir que la copia funcione en el emulador no altere materialmente la operación del sistema ni las posibles evidencias digitales bajo análisis. Por ejemplo, hay veces que al usar una emulación cuando se trata de infecciones de *malware* sospechosas estas variantes de *malware* pueden detectar que están siendo ejecutadas en un entorno virtual y modificar su comportamiento o negarse a ejecutarse.

3.2.3. Recuperación de los ficheros borrados

Este proceso implica identificar las entradas de archivos o carpetas eliminadas en las estructuras de localización de archivos (como tablas FS, MFT, etc.), o en estructuras similares, dependiendo de su ubicación. Es decir, se debe llevar a cabo una recuperación parcial o completa de la información eliminada en los diferentes soportes de almacenamiento, así como recuperar datos en áreas del disco no asignadas o no utilizadas. Además, se debe obtener las carpetas y archivos «huérfanos» que permanecen dentro de diversos ficheros, de los cuales se ha perdido la conexión.

Igualmente, este proceso consiste en realizar una búsqueda de archivos completos o de sus fragmentos en los dispositivos de almacenamiento. Esta búsqueda se realizará a través de las cabeceras dichos archivos o fragmentos.

Para garantizar la trazabilidad de toda la información recuperada, el informe pericial debe especificar claramente la fuente de la información extraída y el método empleado para su recuperación.

3.2.4. Estudio de las particiones y sistemas de archivos

Este proceso consiste en examinar las distintas estructuras de almacenamiento en los dispositivos, como particiones, volúmenes físicos y sistemas RAID, donde se encuentran diversos volúmenes lógicos que albergan los sistemas de archivos. La configuración de estas estructuras puede variar según el tipo de sistema de particionado empleado.

Este proceso debe incluir entre sus tareas básicas las siguientes:

- Enumerar los contenedores y particiones actuales y las que hubieran podido existir anteriormente.

- Identificar las zonas o espacios de disco ocultos, como las HPA, DCO u otras que pudiera haber según la tecnología del fabricante.

- Identificar los distintos sistemas de archivos que pudiera haber en los contenedores y particiones, con la identificación del contenedor que almacena el sistema operativo de inicio y tipo de arranque o selector multiarranque.

- Identificar los sistemas de archivos de los discos compactos, en especial, las distintas pistas de las sesiones de grabación que pueden existir en los diferentes formatos de estos medios, los archivos cifrados y/o protegidos con contraseña, unido a la localización de los volúmenes o discos cifrados.

- Montar los archivos contenedores de otros tipos, como pueden ser los comprimidos, compuestos y empaquetados, verificando las cabeceras de los distintos formatos de archivos y sus resúmenes digitales.

En el caso del análisis de la memoria RAM, se debe estudiar, para un momento temporal concreto, los procesos activos, los ficheros abiertos, los puertos y tomas de corriente activas, así como, las distintas claves de acceso a los programas o volúmenes cifrados del soporte de almacenamiento físico correspondiente.

3.2.5. Estudio del sistema operativo

Este proceso consiste en analizar los sistemas operativos instalados en los volúmenes lógicos de los dispositivos de almacenamiento, examinar la actividad de los usuarios en estos sistemas y revisar las políticas de seguridad aplicadas.

Dicho proceso engloba los siguientes pasos:

- Identificar el sistema operativo principal del equipo y su localización.

- Identificar el sistema o sistemas operativos utilizados, su fecha de instalación, así como sus revisiones o actualizaciones.

- Identificar los distintos usuarios y sus privilegios y permisos dentro del sistema operativo, además de las fechas de último acceso al equipo de cada uno de ellos y su política de seguridad.

- Identificar los dispositivos de *hardware* y *software* reconocidos por el sistema o que pudieran haber estado instalados anteriormente.

3.2.6. Estudio de la seguridad implementada

Este proceso tiene como objetivo evaluar si las evidencias electrónicas enviadas para su análisis han sido comprometidas. Se investigan diversos niveles de vulnerabilidad en las evidencias, que pueden resultar de métodos de intrusión, modificación, eliminación o sustracción de la información almacenada en los dispositivos originales.

Se debe identificar cualquier software malicioso (como virus o troyanos) presente en las particiones detectadas, evaluando el nivel de intrusión en el sistema y determinando qué archivos han sido comprometidos y de qué manera.

3.2.7. Análisis detallado de los datos obtenidos

Este consiste en examinar minuciosamente las evidencias electrónicas, aprovechando los análisis previamente descritos. Para ello, se debe emplear *software* reconocido en el ámbito forense. Además, este análisis debe ceñirse rigurosamente a las cuestiones formuladas por la entidad o el organismo que solicitó el estudio forense.

Este análisis implica simultáneamente clasificar los datos y, si es necesario, realizar un proceso previo de indexado, que facilitará las búsquedas de los elementos a identificar en los soportes digitales. Para ello, se emplearán palabras clave o códigos alfanuméricos específicos. Es importante documentar las palabras o criterios de búsqueda utilizados durante este indexado.

Durante el proceso de indexado, se deben separar los archivos cuyo contenido no es claramente legible a primera vista, como los archivos comprimidos, dejando estos datos sin indexar inicialmente. Una vez que se haya tratado esta información, debe integrarse nuevamente en el proceso de indexación general. Además, este procedimiento permite excluir los archivos que corresponden a aplicaciones comerciales instaladas en el soporte de almacenamiento digital, de modo que se enfoquen los análisis detallados en otros datos relevantes.

Una lista de las tareas que deben llevarse a cabo durante el análisis forense detallado de las evidencias electrónicas puede ser, por ejemplo, la siguiente:

Actividades para el análisis de datos detallado
◯ Determinar la información del sistema: *hardware* instalado y reconocido por el sistema operativo, fecha, hora y usuario de la última actividad del sistema, datos de la configuración regional, etc.
◯ Estudio de los dispositivos físicos conectados en algún momento al equipo informático, como pueden ser: agendas personales digitales, teléfonos móviles, lápices de memoria, impresoras, escáneres, equipos multifunción, cámaras fotográficas y de vídeo, tarjetas de memoria y otras unidades de almacenamiento externo.
◯ Estudio del escritorio o pantalla principal de visualización y de la papelera de reciclaje.

◯	Identificar las conexiones de red y las tarjetas instaladas con identificación de la MAC, además de los protocolos usados y direcciones IP.
◯	Estudio de las comunicaciones realizadas desde el equipo informático.
◯	Estudio del registro del sistema y *logs* de auditoría del propio sistema operativo.
◯	Analizar la información contenida en los espacios no asignados en las particiones y en el espacio físico no ocupado por los archivos lógicos, entre el cual se incluyen las áreas o espacio del disco sin asignar actualmente por el sistema.
◯	Analizar la información de los archivos de hibernación, paginación, particiones y archivos *swap*, etc.
◯	Análisis de la cola de impresión.
◯	Visualizar los enlaces a archivos, así como los archivos accedidos de forma reciente.
◯	Estudio de las carpetas de los distintos usuarios.
◯	Estudio de las aplicaciones instaladas relativas a programación, grabación y tratamiento de imágenes, procesamiento de audio, imagen y vídeo, *software* de uso contable y de gestión económica, programas ofimáticos, etc.
◯	Estudio de los metadatos.
◯	Análisis de aplicaciones de virtualización, con el fin de determinar los soportes virtuales creados y su configuración.
◯	Estudio de las bases de datos instaladas y sus sistemas gestores.
◯	Estudio de *software* de cifrado y los ficheros y particiones cifradas, así como la posibilidad de que este venga implementado en el sistema operativo.
◯	Estudio de la navegación por Internet, con determinación de las *cookies* y análisis de la distintas carpetas que presenten historial de navegabilidad en dicha red.
◯	Análisis de los correos electrónicos y correos vía web.
◯	Análisis de los registros de mensajería instantánea y conversaciones, junto con las listas de contactos.

Figura 15. Ejemplo de lista de posibles actividades para realizar un análisis de datos detallado.

Fuente: Elaboración propia con información proveniente de la norma UNE-EN ISO/IEC 27042:2016.

4. PRESENTACIÓN

El análisis forense realizado debe resultar en un informe pericial. Este debería combinar términos técnicos con un lenguaje claro y accesible, orientado hacia el organismo o entidad que solicitó el estudio, bajo la premisa de que el público destinatario no necesariamente es personal técnico ni tiene un conocimiento profundo de las nuevas tecnologías.

Después de redactar el informe pericial, los equipos y soportes digitales analizados deben ser devueltos al organismo que solicitó el estudio, acompañados de un recibo o documento de control de evidencias. Este recibo debe ser devuelto a la entidad que lo emitió una vez que el informe y las muestras hayan llegado al solicitante, lo que concluye la trazabilidad y el proceso de custodia de las evidencias analizadas.

4.1. Interpretación de la información

4.1.1. Acreditación de los hechos

Al redactar el informe y, por lo tanto, al evaluar las evidencias, se debe tener cuidado en distinguir entre los hechos que se han encontrado y la información que se ha inferido. Por ejemplo, la presencia de un archivo existente en un dispositivo es un hecho. Si ese archivo es un adjunto de un correo electrónico en una bandeja de entrada, se puede inferir que el archivo fue creado en el dispositivo como resultado de haber sido recibido en un correo electrónico; por lo tanto, esto es información inferida. Sin embargo, si el archivo se encontró en un directorio creado por el usuario con un nombre de archivo especificado por el usuario, se puede inferir que el usuario tomó una decisión consciente de crear o guardar el archivo. Las inferencias sobre archivos, como estas, pueden corroborarse examinando otras partes del sistema de archivos para obtener información adicional.

Es necesario mantener en mente las distinciones entre hechos e información inferida, asegurándose de que todos los hechos necesarios para respaldar cualquier conclusión estén presentes y verificados. Al informar sobre hechos e información inferida, se debe indicar la distinción entre ambos y el proceso lógico que llevó a cualquier inferencia debe ser transparente y reproducible.

4.1.2. Factores que afectan a la interpretación

Durante el análisis y la interpretación, el personal debe tener en cuenta la calidad de las posibles evidencias digitales disponibles (por ejemplo, integridad, fuente y propósito original, posibilidad de que se hayan implementado medidas de ofuscación de la evidencia).

El propósito de la interpretación es ofrecer una explicación de los hechos descubiertos durante el análisis, enmarcándolos dentro del contexto proporcionado. Si existe más de una explicación razonable, deben reportarse las todas ellas. Si la información contextual cambia, la interpretación también puede cambiar. Por último, si los hechos se prestan a más de una interpretación, todas

ellas, o al menos las más plausibles, deben presentarse como resultado del análisis, indicando, su respectiva probabilidad.

4.2. Contenido del informe

Si no existe ninguna política empresarial que defina el contenido, los informes forenses resultantes del análisis de las evidencias deberían contener, como mínimo:

- Una declaración clara de las cualificaciones o la competencia del autor para participar en la investigación y elaborar el informe.
- Una declaración clara de la información proporcionada al equipo antes de que comenzara la investigación (incluida la naturaleza del informe).
- La naturaleza del incidente bajo investigación.
- El momento y la duración del incidente.
- La ubicación del incidente.
- El objetivo de la investigación.
- Los miembros que forman equipo de investigación, así como sus roles y acciones.
- El tiempo y la duración de la investigación.
- La ubicación de la investigación.
- Los detalles fácticos de las evidencias electrónicas encontradas durante la investigación.
- Cualquier daño a posibles evidencias electrónicas que se haya observado durante la investigación, además de la forma en que puedan afectar a los procesos posteriores.
- Las limitaciones de cualquier análisis realizado (por ejemplo, conjuntos de datos incompletos o restricciones operativas o de tiempo).
- Una lista de las actividades realizadas, incluyendo, cuando corresponda, cualquier herramienta empleada.

Algunos informes también pueden contener:

- Una interpretación de las pruebas digitales tal como la entiende el investigador (por ejemplo, un relato de cómo pudo haber ocurrido un ataque externo y llevado a la presencia de las pruebas digitales encontradas). Si es posible más de una interpretación, se deben incluir todas las interpretaciones posibles, con una indicación de sus respectivas probabilidades. La interpretación puede presentarse como una opinión si es necesario.
- Conclusiones.

Cuando un informe contenga una o más opiniones, el autor debe distinguir claramente entre hechos y opiniones, y justificar cualquier opinión expresada.

5. PRESERVACIÓN

El proceso de gestión de la información digital requiere preservar las evidencias originales para asegurar que mantengan su validez y fiabilidad en todo momento. Esto también garantiza que cualquier otro experto pueda reproducir los estudios realizados, permitiendo así la posibilidad de contraanálisis o revisiones adicionales sobre la misma información.

Toda organización o empresa debe considerar los siguientes principios al tratar con evidencias electrónicas:

- Contar con protocolos específicos que garanticen la integridad de las evidencias, previniendo su manipulación debido a modificaciones intencionadas, descargas electrostáticas, campos magnéticos o conexiones accidentales a redes inalámbricas.

- Los técnicos deben prestar especial atención al almacenar las evidencias en soportes apropiados, garantizando no solo su integridad, sino también la preservación de otras posibles evidencias como huellas, restos orgánicos relacionados con el ADN o diversas partículas.

- Manipular las evidencias utilizando vestimenta adecuada, diseñada específicamente para evitar descargas electrostáticas, y abstenerse de portar dispositivos que emitan señales de radiofrecuencia que puedan alterar el espectro radioeléctrico en la escena. Por este motivo, puede ser necesario emplear soportes aislados que prevengan interferencias externas capaces de modificar los datos originales.

A su vez, el personal técnico responsable de la preservación de las e-evidencias debe seguir las siguientes directrices:

- Precintar y sellar todas las evidencias encontradas en soportes adecuados, asegurándose de que permanezcan intactas hasta que los peritos o especialistas designados inicien su análisis, prestando especial atención a los dispositivos que necesiten estar conectados a una fuente de energía externa.

- Hasta que se finalice la pericia correspondiente, todas las evidencias o muestras se deben almacenar en un lugar seguro, siempre y cuando los medios así lo permitan. En ausencia de dicho lugar, almacenarlas en una caja fuerte.

5.1. Proceso de empaquetado

Durante el empaquetado efectuado para la preservación de las evidencias y dispositivos electrónicos, es importante asegurar estos elementos de manera que se elimine la posibilidad de

degradación o manipulación de la información. La degradación puede resultar de la exposición a ondas magnéticas, corriente eléctrica, calor, humedad, sequedad, choques, vibraciones, etc. La manipulación puede resultar de un acto intencional de modificar o permitir cambios en la evidencia electrónica.

Todos los dispositivos recolectados y las evidencias adquiridas deben estar protegidas contra pérdidas, manipulaciones y daños. La actividad más importante en este proceso de preservación es mantener la integridad, autenticidad y la cadena de custodia de las evidencias electrónicas. Además, estos deben almacenarse en una instalación que cuente con medidas de seguridad física, como sistemas de control de acceso, vigilancia, detección de intrusos, o en otro entorno controlado. Los principales objetivos de la seguridad física son proteger y prevenir la pérdida, el daño y la manipulación, así como permitir la auditoría.

Los dispositivos digitales recolectados deben pasar por un proceso embalaje adecuado, con el fin de evitar la contaminación de los dispositivos digitales antes de su transporte o almacenaje. Se puede utilizar un embalaje resistente a los golpes para evitar daños físicos en cualquiera de los componentes de los dispositivos.

5.1.1. Pautas generales para el empaquetado de evidencias electrónicas

Las siguientes pautas generales describen las acciones mínimas que deben tomarse durante este proceso de empaquetado:

- No tocar las cintas magnéticas. Levantarlas por sus carcasas protectoras o áreas que no contienen datos (por ejemplo, los bordes de los discos ópticos). Esto solo debe hacerse si se usan guantes sin pelusa.

- Se debe etiquetar toda evidencia digital, los dispositivos digitales recolectados y cualquier parte de hardware asociada con los dispositivos con etiquetas a prueba de manipulaciones. Algunas jurisdicciones tienen requisitos específicos sobre el formato de etiquetado de material probatorio. La etiqueta no debe colocarse directamente en las partes mecánicas del dispositivo digital ni debe cubrir u ocultar información importante de identificación.

- En los dispositivos con aberturas y componentes móviles estos deben sellarse con etiquetas a prueba de manipulaciones, y el responsable debe firmar el sello.

- Los dispositivos conectados a baterías que contienen datos volátiles deben ser revisados regularmente para asegurarse de que siempre tengan suficiente suministro de energía.

- Almacenar los dispositivos en un contenedor adecuado para su naturaleza y contra potenciales amenazas.

- Empaquetar los dispositivos de manera que se evite el daño por golpes, vibraciones, gran altitud, calor y exposición a radiofrecuencia durante el transporte.

- Los medios de almacenamiento magnético deben guardarse en un embalaje que sea magnéticamente inerte, antiestático y libre de partículas.

- El uso de una bolsa de Faraday u otro embalaje con blindaje de radiofrecuencia puede aumentar el drenaje de la batería. Esto puede requerir la provisión de energía auxiliar al dispositivo mientras está dentro de la bolsa.

5.1.2. Pautas adicionales para el empaquetado de evidencias electrónicas

Aparte de las actividades generales descriptas anteriormente, y dependiendo de las circunstancias concretas, se deberá, adicionalmente, evaluar la ejecución de las siguientes pautas:

- Usar guantes sin pelusa y asegurarse de que, si estos no se usan, las manos estén limpias y secas.

- Resguardar los dispositivos de la influencia de fuentes electromagnéticas (radios policiales, altavoces, máquinas de rayos X…). El área de embalaje debe estar libre de electricidad estática.

- El área de embalaje debe estar libre de polvo, grasa y contaminantes químicos que puedan acelerar la oxidación o causar la acumulación de humedad en la capa magnética.

- Minimizar la posibilidad de transferencia de señal que puede resultar en una mala calidad de esta.

- Las áreas de empaquetado deben estar libres de luz ultravioleta. La luz UV puede causar la degradación del ADN o dañar algunos tipos de medios.

- Proteger los dispositivos contra cambios bruscos de temperatura que puedan causar choques térmicos.

- Al finalizar el análisis de los datos relevantes de cualquier dispositivo móvil, no se debe reintroducir ni la batería ni la tarjeta SIM original, para evitar que, en caso de encendido accidental, se altere el archivo de localización (LOCI) de la SIM o se modifique el registro de llamadas almacenadas.

5.2. Transporte de las evidencias electrónicas

Durante el embalaje y el transporte, se debe ser consciente de que cualquier descarga electrostática puede dañar el valor probatorio de la evidencia digital. Además, los dispositivos digitales deben estar bien embalados durante el transporte para evitar daños por golpes y vibraciones.

El proceso de transporte debe permitir un ambiente controlado. El nivel de humedad y la temperatura deben ser adecuados para los dispositivos digitales. Igualmente, se debe evitar mantener la evidencia y dispositivos digitales en el vehículo de transporte por períodos prolongados. También se debe evitar su exposición a la luz ultravioleta (UV).

Por último, recordar que se debe mantener la cadena de custodia durante todo el proceso de transporte para prevenir posibles manipulaciones o alteraciones, y mantener la integridad y autenticidad de los dispositivos y evidencias electrónicas. Cuando las circunstancias no lo permiten y el personal responsable no puede acompañar la evidencia se pueden utilizar mecanismos de envío apropiados y autorizados para asegurar la seguridad adecuada de esta durante el transporte. Los documentos del transporte y la verificación de la integridad del paquete deben formar parte de la cadena de custodia. Además, en este tipo de casos se recomienda cifrar la evidencia para su transporte.

Anexo B. Glosario y abreviaturas

Cadena de custodia: proceso documentado que se utiliza para seguir, preservar y controlar la evidencia desde el momento en que es recopilada hasta su presentación en un tribunal.

Colusión: acuerdo secreto entre dos o más partes para cometer un acto ilícito, fraudulento o engañoso con el fin de obtener una ventaja ilegal o perjudicar a terceros.

Contraánalisis / Contrapericia: repetición o revisión de un análisis previo con el objetivo de verificar, corroborar o cuestionar los resultados obtenidos en la primera evaluación.

Esteganálisis: técnica utilizada para detectar, analizar y, en ocasiones, extraer información oculta dentro de archivos digitales, como imágenes, videos, audio o texto.

Evidencia electrónica / Evidencia digital / E-evidencia: información o dato almacenado o transmitido en formato digital que puede ser utilizado como prueba en un proceso legal, judicial o de investigación.

E-discovery: proceso mediante el cual se identifican, recopilan, procesan, revisan y preservan datos electrónicos con el fin de utilizarlos como evidencia en procedimientos legales, investigaciones o litigious.

Hash: función criptográfica que convierte una entrada de datos (como un archivo o un mensaje) en una cadena de caracteres de longitud fija, que actúa como una «huella digital» o resumen único de los datos originales.

Impugnación: acto de cuestionar, refutar o desacreditar la validez o legalidad de una decisión, acción, documento o prueba en un contexto judicial, administrativo o legal.

Informática forense: rama de la ciencia forense que se enfoca en la identificación, recolección, preservación, análisis y presentación de evidencia digital de manera legal y metodológica.

Integridad: propiedad de un sistema o de la información que garantiza que los datos no han sido alterados, modificados o corrompidos de manera no autorizada.

Ofuscación: proceso de modificar un programa de manera que su código fuente sea difícil de entender, analizar o interpretar, pero que siga siendo funcional.

Peritaje: proceso mediante el cual un experto o perito en una disciplina específica evalúa, analiza y emite un informe sobre un asunto técnico, científico, o especializado, con el objetivo de proporcionar evidencia objetiva y experta en un contexto judicial o administrativo.

Volatilidad: facilidad con la que los datos pueden cambiar o desaparecer.

ADN	Ácido Desoxirribonucleico	LOCI	*Location of Cell Information* (Ubicación de Información de Células)
AENOR	Asociación Española de Normalización y Certificación	LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales
AUTELSI	Asociación de Empresas de Electrónica, Tecnologías de la Información, Telecomunicaciones y Contenidos Digitales	MAC	*Media Access Control* (Control de Acceso al Medio)
BFSI	*Banking, Financial Services, and Insurance* (Servicios Bancarios, Financieros y de Seguros)	MFT	*Master File Table* (Tabla de Archivos Maestros)
BIOS	*Basic Input/Output System* (Sistema Básico de Entrada/Salida)	NAS	*Network-Attached Storage* (Almacenamiento Conectado en Red)
BYOD	*Bring Your Own Device* (Trae Tu Propio Dispositivo)	NIS	*Network and Information Systems* (Sistemas de Redes e Información)
CAGR	*Compound Annual Growth Rate* (Tasa de Crecimiento Anual Compuesta)	ODS	Objetivos de Desarrollo Sostenible
CCTV	*Closed-Circuit Television* (Televisión de Circuito Cerrado)	OLAF	*European Anti-Fraud Office* (Oficina Europea de Lucha contra el Fraude)
CD	*Compact Disc* (Disco Compacto)	PC	*Personal Computer* (Ordenador Personal)
CRM	*Customer Relationship Management* (Gestión de Relaciones con el Cliente)	PDA	*Personal Digital Assistant* (Asistente Digital Personal)
DCO	*Digital Certificate of Origin* (Certificado Digital de Origen)	PDF	*Portable Document Format* (Formato de Documento Portátil)
DVD	*Digital Versatile Disc* (Disco Digital Versátil)	PED	*Personal Electronic Device* (Dispositivo Electrónico Personal)
ERP	*Enterprise Resource Planning* (Planificación de Recursos Empresariales)	PIN	*Personal Identification Number* (Número de Identificación Personal)
ESI	*Electronically Stored Information* (Información Almacenada Electrónicamente)	PUK	*Personal Unblocking Key* (Clave de Desbloqueo Personal)
ESN	*Electronic Serial Number* (Número de Serie Electrónico)	PYMES	Pequeñas y Medianas Empresas
FInES	*Framework for the Integration of Environmental and Social Aspects* (Marco para la Integración de Aspectos Ambientales y Sociales)	RAID	*Redundant Array of Independent Disks* (Conjunto Redundante de Discos Independientes)

FS	*File System* (Sistema de Archivos)	RAM	*Random Access Memory* (Memoria de Acceso Aleatorio)
GPS	*Global Positioning System* (Sistema de Posicionamiento Global)	RFC	*Request for Comments* (Solicitud de Comentarios)
GSM	*Global System for Mobile Communications* (Sistema Global para Comunicaciones Móviles)	RFIC	*Radio Frequency Integrated Circuit* (Circuito Integrado de Radiofrecuencia)
HDD	*Hard Disk Drive* (Unidad de Disco Duro)	RGPD	Reglamento General de Protección de Datos
HPA	*Host Protected Area* (Área Protegida por el Host)	SAN	*Storage Area Network* (Red de Área de Almacenamiento)
HTML	*HyperText Markup Language* (Lenguaje de Marcado de Hipertexto)	SEC	Sistema Estadístico de Criminalidad
IA	Inteligencia Artificial	SGEE	Sistema de Gestión de Evidencias Electrónicas
ICAM	Ilustre Colegio de la Abogacía de Madrid	SIM	*Subscriber Identity Module* (Módulo de Identidad del Suscriptor)
ICCID	*Integrated Circuit Card Identifier* (Identificador de Tarjeta de Circuito Integrado)	SSD	*Solid State Drive* (Unidad de Estado Sólido)
IDS	*Intrusion Detection System* (Sistema de Detección de Intrusiones)	TFG	Trabajo de Fin de Grado
IMEI	*International Mobile Equipment Identity* (Identidad Internacional de Equipo Móvil)	TI	Tecnologías de la Información
INTERPOL	*International Criminal Police Organization* (Organización Internacional de Policía Criminal)	TIC	Tecnologías de la Información y la Comunicación
IoT	*Internet of Things* (Internet de las Cosas)	UE	Unión Europea
IP	*Internet Protocol* (Protocolo de Internet)	UNE	Una Norma Española
IPS	*Intrusion Prevention System* (Sistema de Prevención de Intrusiones)	UPS	*Uninterruptible Power Supply* (Sistema de Alimentación Ininterrumpida)
ISO	*International Organization for Standardization* (Organización Internacional de Normalización)	USB	*Universal Serial Bus* (Bus Universal en Serie)
JSON	*JavaScript Object Notation* (Notación de Objetos JavaScript)	UV	Ultravioleta
LAN	*Local Area Network* (Red de Área Local)	WAN	*Wide Area Network* (Red de Área Amplia)
LEC	Ley de Enjuiciamiento Civil	Wi-Fi	*Wireless Fidelity*
LECrim	Ley de Enjuiciamiento Criminal	ZIP	Zona de Información Protegida
LIFe	Laboratorio de Informática Forense europeo		

Anexo C. Plantilla de identificación de evidencias electrónicas

Identificación de evidencias				
Identificador de Evidencia				
Tipo de dispositivo				
Marca		Modelo		
Número de serie				
Número de licencia				
Capacidad de almacenamiento				
Estado	◯ Encendido	Descripción o fotografía de la pantalla:		
	◯ Apagado			
Ha cambiado el estado?	◯ Sí	Por qué?:		
	◯ No			
Fuente de alimentación	◯ Cargador / Cable	Se ha encontrado?	◯ Sí	
	◯ Batería		◯ No	
Nivel de batería	%	Se está cargando el dispositivo?	◯ Sí	
			◯ No	
Marcas identificativas				
Está el dispositivo conectado a la red?	◯ Sí	Servicios proporcionados:		
	◯ No			

Se ha utilizado el detector de señales inalámbricas?	◯ Sí	Interacciones:								
	◯ No									
Nivel de criticidad del sistema	1	2	3	4	5	6	7	8	9	10
	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯
	Muy crítico									Nada crítico

Dispositivos móviles			
IMEI		ESN	
Número de teléfono		Operador red	
Tarjetas de memoria recolectadas			
Tarjeta SIM adquirida			
PIN		PUK	
Sistema CCTV			
Número de cámaras conectadas		Número de cámaras en funcionamiento	
Configuración de visualización			
Configuraciones actuales de grabación			
Ubicación de almacenamiento			

Anexo D. Funcionalidades mínimas de las herramientas hardware y software

Funcionalidades mínimas de las herramientas hardware forense
◯ Efectuar un duplicado forense con el que obtener un clon forense o imagen fiel de los datos originales.
◯ Acceder a cualquier área protegida, siendo capaces de operar sobre dispositivos de memoria y otros elementos de almacenamiento digital de datos.
◯ Acceder a los soportes magnéticos sin alterar su contenido.
◯ Extraer datos de los dispositivos móviles.
◯ Estar dotados de sistemas de bloqueo de escritura sobre los soportes originales.
◯ (opcional) Contar con aceleradores hardware para la recuperación de contraseñas.
Funcionalidades mínimas de las herramientas software forense
◯ Efectuar una captura exacta de los datos hallados en el dispositivo o medio bajo estudio.
◯ Generar resúmenes digitales (“hash”) de las imágenes o clonados forenses para mantener la validez legal de los datos.
◯ Indexar por tipos de documentos y por procesos.
◯ Obtener informes forenses de diversa precisión para presentar la información hallada ante cualquiera que lo solicite.
◯ Parametrizar la granularidad de la adquisición.
◯ Recuperar archivos y carpetas eliminadas.
◯ Recuperar particiones, pudiendo reconstruir la estructura de los volúmenes.
◯ Analizar los archivos de registro y configuración de los dispositivos hardware bajo estudio.
◯ Analizar los resúmenes digitales (“hash”) existentes.
◯ Analizar las firmas de archivos.
◯ Realizar búsquedas en el espacio de disco no asignado.

◯	Generar listados detallados de archivos, carpetas y direcciones URL junto con las fechas y horas de visita a las mismas.
◯	Reconstruir los artefactos de Internet, siendo los principales los relacionados con la navegación web, el correo electrónico, las herramientas de intercambio de ficheros y la mensajería instantánea.
◯	Recuperar los archivos de registros (“logs”) de seguridad y las trazas de los paquetes de red.

Anexo E. Relación del trabajo con los objetivos de desarrollo sostenible de la agenda 2030

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No procede
ODS 1. **Fin de la pobreza.**				X
ODS 2. **Hambre cero.**				X
ODS 3. **Salud y bienestar.**				X
ODS 4. **Educación de calidad.**			X	
ODS 5. **Igualdad de género.**				X
ODS 6. **Agua limpia y saneamiento.**				X
ODS 7. **Energía asequible y no contaminante.**				X
ODS 8. **Trabajo decente y crecimiento económico.**			X	
ODS 9. **Industria, innovación e infraestructuras.**			X	
ODS 10. **Reducción de las desigualdades.**				X
ODS 11. **Ciudades y comunidades sostenibles.**				X
ODS 12. **Producción y consumo responsables.**				X
ODS 13. **Acción por el clima.**				X
ODS 14. **Vida submarina.**				X
ODS 15. **Vida de ecosistemas terrestres.**				X
ODS 16. **Paz, justicia e instituciones sólidas.**			X	
ODS 17. **Alianzas para lograr objetivos.**				X

«Los Objetivos de Desarrollo Sostenible (ODS) constituyen un llamamiento universal a la acción para poner fin a la pobreza, proteger el planeta y mejorar las vidas y las perspectivas de las personas en todo el mundo. En 2015, todos los Estados Miembros de las Naciones Unidas aprobaron 17 Objetivos como parte de la Agenda 2030 para el Desarrollo Sostenible, en la cual se establece un plan para alcanzar los Objetivos en 15 años.»

La relación de este TFG con los ODS es relativamente baja debido a su enfoque específico en la gestión de evidencias electrónicas. Los ODS con mayor relevancia para este trabajo son el ODS 4, el ODS 8, el ODS 9 y el ODS 16:

- El ODS 4 se refiere a la educación de calidad, lo cual es fundamental para la formación de peritos informáticos, quienes necesitan una educación avanzada.

- El ODS 8 fomenta el progreso económico y la creación de empleo; las nuevas tecnologías demandan profesionales capacitados para asegurar su adecuado uso, lo que hace que la profesión de perito tenga un futuro prometedor.

- El ODS 9 aboga por la introducción y promoción de nuevas tecnologías, la facilitación del comercio internacional y el uso eficiente de los recursos. La labor de los peritos informáticos y las organizaciones que protegen los sistemas críticos contribuye al funcionamiento adecuado de instituciones públicas y privadas.

- Finalmente, el ODS 16 impulsa la paz, la justicia y el fortalecimiento de instituciones sólidas, valores que los peritos y la legislación buscan mantener en su compromiso con la verdad y el bienestar común.