Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Ciencias Exactas y Naturales e Ingeniería

Carrera de Maestría en Seguridad Informática

Trabajo Final de Maestría

Tema

Informática Forense

Título

- Integración del Modelo de Madurez de Capacidades a Laboratorios de Análisis Forense Digital -

Subtítulo

- Una mirada hacia un Sistema de Gestión de Evidencia Digital -

Autor: Lic Antonio Javier Maza

Tutor: Ing Hugo Pagola.

Octubre 2021

Cohorte: 2018

[Página dejada en blanco intencionalmente]

LICENCIA

Bajo los siguientes términos

Atribución: en cualquier explotación de la obra autorizada por la licencia será necesario reconocer la autoría (obligatoria en todos los casos).

No Comercial: la explotación de la obra queda limitada a usos no comerciales.

Sin obras derivadas: la autorización para explotar la obra no incluye la posibilidad de crear una obra derivada.

DECLARACION JURADA

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Lic. Antonio Javier Maza
DNI 27.810.784

0.1 Resumen ejecutivo

El presente Trabajo Final de Maestría tiene como finalidad presentar un esquema basado en la integración del modelo de madurez de capacidades (IMMC) que permita realizar una evaluación de los procesos y servicios de un laboratorio de análisis forense digital.

En tal sentido, el objetivo principal es brindar un marco de referencia integral, mediante un conjunto estandarizado de conceptos, prácticas y criterios, permitiendo una evaluación e categorización de un laboratorio de análisis forense digital, como así también de las múltiples partes que lo componen, haciendo foco en las personas, los procesos y la tecnología, lo que permitirá:

- Adoptar una visión integral respecto de procedimientos y estándares vinculados con el análisis forense e investigación digital.
- Realizar una autoevaluación que posibilite identificar de forma ágil el estado de madurez de una organización y adoptar una conducta proactiva.
- Incrementar la eficacia y eficiencia de las metodologías aplicadas en los laboratorios forenses digitales.
- Evaluar la posibilidad de integrar el modelo de madurez de capacidades en pos de la mejora continua.

Del mismo modo, cabe destacar la importancia e impacto del IMMC aplicado a la práctica forense, cuyo propósito es guiar a las organizaciones en la selección de estrategias de mejora continua, identificando su estadio y aquellos factores clave que le permitirán evolucionar, alcanzando niveles de excelencia a medida que se adquiera una mayora habilidad para gestionar y administrar su procesos y servicios.

Para finalizar, cabe destacar que el modelo de madurez de capacidades es un marco de trabajo que ya ha sido implementado exitosamente en diferentes organizaciones y entornos tecnológicos, en cuanto a usabilidad, claridad y aplicabilidad, permitiendo señalar deficiencias dentro de una organización y mejorar un conjunto finito de actividades de manera estable y gradual.

Palabras Clave

Madurez, Nivel de madurez, Auto evaluación, Indicadores, Reglas de buena práctica, Instructivos, Procedimientos Operativos, Manuales, Guías, Normas, Estándares, Informática Forense, Cadena de Custodia, Identificación, Preservación, Análisis, Presentación, Evidencia Digital, Incidente.

0.2 Índice de contenidos

0.3 Índice de ilustraciones

0.4 Índice de Tablas

1 Introducción

El campo del análisis forense digital ha evolucionado para convertirse en una disciplina científica emergente de gran importancia no solo en las investigaciones criminales sino también como aliada estratégica de negocios en el entorno corporativo. En la actualidad la mayoría de los laboratorios forenses digitales de nuestro país se encuentran emplazados en el seno de instituciones policiales o fuerzas de seguridad, cuyas actividades se enfrentan diariamente a un marco legal y normativo con mayores exigencias para cumplir con rigurosos estándares vinculados con la admisibilidad de la evidencia digital como pruebas dentro de una investigación judicial, además de enfrentarse a la inminente necesidad de contar con una serie de requisitos que permita su correspondiente homologación, acorde la regulación y requerimientos exigidos para la acreditación de sus instalaciones y procedimientos forenses. Estos requisitos, junto a la acumulación de casos fruto de una demanda que crece exponencialmente y la limitación de recursos, se materializan como un desafío infranqueable para los laboratorios de análisis forense digital, cuyo ritmo de trabajo podría catalogarse como vertiginoso, debiendo además sumar esfuerzos para mantener el foco en la correcta administración de casos, cumplimiento de mayores requisitos regulatorios y además implementar soluciones que permitan encontrar formas de mejorar la eficiencia y eficacia de sus procedimientos y servicios.

Basado en los paradigmas del modelo de madurez de capacidades [1], la integración de este esquema surge de los hallazgos identificados durante el desarrollo del Trabajo Final de Especialización, acentuados por la brecha que existe entre las diferentes reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de informática forense y evidencia digital.

Asimismo, mediante la metodología planteada resulta factible medir la madurez de los laboratorios de análisis forense digital en tres dimensiones clave que se definen específicamente como: personas, procesos y herramientas tecnológicas, al mismo tiempo que permite que dicha evaluación se adapte a diferentes tipos de organización. La integración de este modelo sobre la base de múltiples dominios clave permitirá proporcionar una evaluación integral sobre la madurez de capacidades de una organización, cuyos dominios son totalmente interdependientes si se comparan con otros modelos similares que se enfocan de manera más granular.

Cabe destacar que este modelo también servirá como un catalizador hacia un medio más oportuno, efectivo y eficiente para desarrollar e implementar estándares forenses digitales y mejores prácticas en el futuro.

En resumen, la integración del modelo de madurez de capacidades permitirá afrontar los desafíos señalados anteriormente mediante una propuesta metodológica superadora como alternativa para que los laboratorios forenses logren una mejora significativa en la gestión de sus recursos y de esta manera alcanzar sus objetivos a través de un sistema de evaluaciones y herramientas de planificación, todas orientadas a medir el cumplimiento y la madurez de la capacidad en múltiples dominios.

1.1 Planteamiento del problema

De las diferentes reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de informática forense y evidencia digital que fueron estudiados durante el Trabajo Final de Especialización, podría decirse que en su gran mayoría hacen hincapié en procesos, herramientas o métodos de investigación, pero no proporcionan a los laboratorios de análisis forense digital un mecanismo simple, certero y formal, que permita evaluar la eficacia y/o eficiencia de las capacidades de sus procesos y dotar de una planificación metodológica que les permita alcanzar la mejora continua de manera sencilla y efectiva.

Los laboratorios de análisis forense digital se enfrentan constantemente a una inmensa cantidad de desafíos vinculados con los profundos avances

tecnológicos, la permanente necesidad de actualizar y reevaluar sus habilidades, la ingente necesidad de adaptar las mejores prácticas, métodos ad-hoc y estándares forenses.

Podría decirse que en la actualidad las investigaciones forenses digitales revisten cada vez mayor complejidad, no solo por el volumen de información que almacenan los dispositivos informáticos, sino también por la heterogeneidad de datos y cantidad de artefactos forenses que podrían resultar de utilidad, por tal motivo se deben desarrollar nuevos enfoques para administrar los detalles del caso de una investigación de esta naturaleza [2].

Además de los desafíos tecnológicos señalados anteriormente, existen una serie de retos vinculados principalmente con la virtualización, la implementación del cifrado de información, el aumento de herramientas anti-forenses, contenido multimedia enriquecido y registros almacenados en la nube, entre otros, aunque resulta irónico que estas preocupaciones ya fueron vislumbradas hace mucho tiempo atrás y aún se materializan como potenciales escenarios de riesgo al momento de encarar una investigación forense [3].

El resultado es un conjunto de improvisados y costosos esfuerzos que los laboratorios de análisis forense digital realizan para tratar de abordar sus apremiantes requisitos legales, reglamentarios, técnicos y comerciales de forma independiente, con escasas o nulas oportunidades que les permitan evaluar su situación actual debido a que carecen de la capacidad para evaluar sus niveles de madurez en todos sus aspectos organizacionales.

En tal sentido, es menester destacar que en la actualidad no existe ningún marco o modelo metodológico que permita a un laboratorio evaluar su situación actual con respecto al cumplimiento de normativas y estándares; madurez de su capacidad, en los dominios clave de personas, procesos y herramientas tecnológicas e identificación de fortalezas, debilidades y recomendaciones para mejora a corto, mediano y largo plazo.

En vista de la amplia gama de desafíos y contratiempos que enfrentan los laboratorios forenses digitales, se puede argumentar que la madurez de la capacidad forense un aspecto más que necesario y esencial que ha sido pasado por alto desde la perspectiva de la gestión de procesos, aun cuando se ha

materializado como un importante requisito para cualquier modelo de negocios y el aseguramiento de la calidad de los servicios de análisis forense digital, siendo merecedor de una mayor investigación y esfuerzo para establecer un modelo metodológico sostenible para su progresiva implementación.

La integración del modelo de madurez de capacidades aplicada a los laboratorios de análisis forense digital puede ser implementado a una multitud de organizaciones, independientemente de su envergadura, requisitos reglamentarios y/o cumplimiento, alcance de sus servicios forenses y estado de acreditación, aportando valor agregado y una considerable reducción de costos vinculados a la gestión de recursos, sobre la base de una mejora continua de calidad y excelencia.

1.2 Objetivo General

- Brindar un marco de referencia que permita integrar el modelo de madurez de capacidades en laboratorios de análisis forense digital promoviendo una mejora significativa en la gestión de sus recursos y alcanzar sus objetivos a través de un sistema de evaluaciones y herramientas de planificación, orientadas a medir el cumplimiento y estadio de tres dominios organizativos clave: personas, procesos y herramientas tecnológicas, y sus interrelaciones.

1.3 Objetivos Específicos

- Adquirir un amplio conocimiento sobre el modelo de madurez de capacidades y evaluar su integración a la gestión de laboratorios de análisis forense digital.
- Proporcionar conciencia sobre la importancia que reviste conocer las capacidades y nivel de madurez de los laboratorios de análisis forense digital.
- Evaluar y medir la capacidad de un laboratorio de análisis forense digital y su grado de madurez sobre la base tres dominios organizativos clave: personas, procesos y herramientas tecnológicas.

- Planificar acciones correctivas de capacitación del personal, verificación de procedimientos e implementación tecnológica, sobre la base de una propuesta metodológica integradora.
- Monitorear regularmente los logros alcanzados e identificar nuevas oportunidades vinculadas a la gestión de procesos, sobre la base de una mejora continua de calidad y excelencia.

1.4 Alcance y limitaciones

En razón de la complejidad del objeto de estudio, el ecosistema digital y ciclo de vida de la evidencia digital, se definen como bases del mismo:

- Se realizará un análisis crítico sobre la posibilidad de integrar el modelo de madurez de capacidades a la gestión de laboratorios de análisis forense digital, acorde documentación técnica existente y vinculada con los pilares de la informática forense, con origen en el ámbito nacional e internacional.
- El análisis de la documentación se efectuará independientemente de los tipos de dispositivos o sistemas operativos existentes en el mercado, circunscribiéndose al plano teórico.
- En virtud del tipo de estudio practicado, no se realizarán simulaciones con dispositivos físicos, limitándose únicamente a efectuar recomendaciones sobre determinadas técnicas y/o herramientas forenses.
- Se delineará una metodología de trabajo integral que permitirá evaluar el nivel de madurez de un laboratorio de informática forense, independientemente de su naturaleza y envergadura.
- Se dejará abierta la posibilidad de realizar una revisión sobre legislación y antecedentes jurídicos en la materia, a fin de evaluar su posible vinculación e impacto sobre los procedimientos técnicos.

1.5 Criterio de selección de normas y estándares

Durante la etapa de estudio del modelo de madurez de capacidades se tuvieron en consideración reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de

informática forense y evidencia digital, habiéndose realizado una minuciosa y exhaustiva investigación sobre toda aquella documentación que potencialmente podría ser incorporada.

Cabe destacar el esfuerzo que implicó llevar adelante tal actividad, en virtud de la cantidad de documentación existente y variedad de autores, tanto de organismos oficiales como entidades del sector privado a nivel nacional e internacional, a pesar de la existencia de ciertos referentes y documentos con mayor reconocimiento en la comunidad científica internacional.

Por tal motivo, se determinó la necesidad de contar con un criterio que permita seleccionar aquellos documentos que serían añadidos al presente trabajo, el que consistió en incorporar normas cuyo contenido se encuentre estrechamente vinculado con el análisis forense digital y etapas del mismo desde una perspectiva amplia, excluyendo todo aquel documento con predominancia de cuestiones técnicas, herramientas y/o acotadas únicamente a la fase de investigación digital.

1.6 Orígenes

Durante el presente trabajo, se pretende modelar una metodología holística basada en la integración del modelo de madurez de capacidades y reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de informática forense y evidencia digital, con el objetivo de evaluar y medir la capacidad de un laboratorio de análisis forense digital y su grado de madurez sobre la base tres dominios organizativos clave: personas, procesos y herramientas tecnológicas. Entre los documentos incorporados, se encuentran:

- Requisitos generales para la competencia de los laboratorios de ensayo y de calibración (ISO/IEC 17025/2017) [4].
- Guía Para Recolectar y Archivar Evidencia (RFC 3227/2002) [5].
- Directrices para la Gestión Evidencia de Tecnología Informática (SAI HB 171/2003) [6].
- Guía para integrar técnicas forenses en respuesta a incidentes (NIST 800-86-2006) [7].

- Investigación en la Escena del Crimen Electrónico: una guía para primeros intervinientes (US DoJ NCJ 219941/2008) [8].
- Computación Forense - Parte 2: mejores prácticas (ISFS/2009) [9].
- Guía de Buenas Prácticas para evidencia basada en computadoras (ACPO/2012) [10].
- Evidencia Electrónica - Una guía básica para primeros intervinientes (ENISA/2014) [11].
- Principios para identificación, recolección, adquisición y preservación de pruebas digitales (ISO/IEC 27037/2016) [12].
- Guía de obtención, preservación y tratamiento de evidencia digital (PGN 756/2016) [13].
- Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la investigación y proceso de recolección de pruebas en Ciberdelitos (MINSEG RES 234/2016) [14].
- Modelo de madurez de capacidades (MMC V1.1) [1].

2
Materiales y métodos

En este capítulo se plasmarán una serie de conceptos que se consideran necesarios para la correcta comprensión del presente trabajo.

2.1 Marco teórico conceptual

En este apartado se aportarán conceptos del área de conocimiento general mediante conceptos y/o teorías de importancia.

2.1.1 Conceptos fundamentales básicos

A continuación, se brindan una serie de definiciones básicas relacionadas con la informática forense:

2.1.1.1 Informática

Ciencia de la información automatizada. Tiene relación con el procesamiento de datos y, para ello, utiliza las computadoras y/o los equipos de procesos automáticos de información [15].

2.1.1.2 Forense

Conjunto de disciplinas científicas que ayudan a la policía y a la justicia a determinar las circunstancias exactas de la comisión de una infracción y a identificar a sus autores [16].

2.1.1.3 Análisis forense digital

Disciplina de las ciencias forenses que se encarga de identificar, preservar, analizar y presentar datos que han sido procesados electrónicamente, y almacenados en un medio digital [17].

2.1.1.4 Computación forense

Rama del análisis forense digital cuyo objetivo es el estudio de sistemas informáticos, medios de almacenamiento o documentos electrónicos [18].

2.1.1.5 Análisis forense de dispositivos móviles

Subdivisión del análisis forense digital relacionado con la recuperación de evidencia digital de dispositivos móviles [18].

2.1.1.6 Análisis forense de redes

Variante del análisis forense digital que se ocupa de la supervisión y el estudio del tráfico de la red informática en sus diferentes formatos, a fin de recolectar evidencia digital o detectar intrusos [18].

2.1.1.7 Análisis forense de datos

Rama del análisis forense digital que tiene como finalidad examinar datos estructurados con el objetivo de descubrir y determinar patrones de actividades fraudulentas [18].

2.1.1.8 Análisis forense de base de datos

Subdivisión del análisis forense digital relacionada con el estudio de bases de datos y sus metadatos [18].

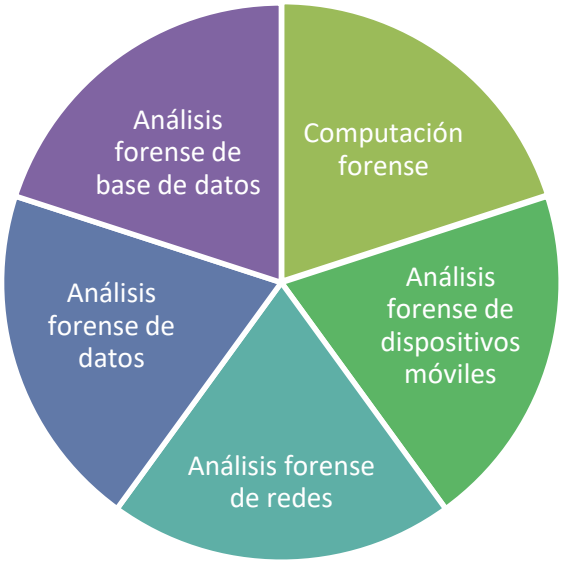

Ilustración 1: Distintos alcances del análisis forense digital.

2.1.1.9 Archivos de evidencias lógicas

Es probable que las copias de respaldo de evidencias lógicas de datos a partir de dispositivos de origen "activos" sean una fuente primaria de datos relevantes. Estos incluirían redes de datos, servidores de archivos, servidores de correo electrónico, computadoras de escritorio, computadoras portátiles, máquinas virtuales e incluso teléfonos inteligentes.

Es probable que al momento de la realización del análisis forense estos sistemas estén en uso o se hayan retirado recientemente y probablemente contengan datos que puedan conservarse o recopilarse durante operaciones regulares.

Ejemplos de datos que podrían ser obtenidos mediante copias de seguridad de evidencias lógicas incluyen documentos de texto, hojas de cálculo, imágenes, código fuente o correos electrónicos almacenados en un servidor con años de antigüedad.

Los registros electrónicos no deben ser pasados por alto como fuentes de datos relevantes, archivar es el proceso de mover datos de sistemas, como el correo electrónico, a otro sistema, como a un servidor de archivos, paquetes de datos, tablas de conexión, etc.

Del mismo modo, las copias de seguridad de sistemas y datos generadas como parte de las operaciones regulares de una empresa u organización, son una fuente de datos para preservación y recolección por parte de los investigadores forenses. Es probable, además, que existan procesos escritos, registros técnicos asociados y que se realicen de manera periódica.

Por otro lado, la mayoría de las empresas u organizaciones rotan sus medios de respaldo a través de un cronograma de almacenamiento, ya sea dentro o fuera de sus instalaciones. Dependiendo del período de tiempo en el que se requieran los datos, será necesario que el investigador forense tenga que recuperar copias de seguridad externas.

2.1.1.10 Imágenes forenses

A continuación, se brindan una serie de definiciones básicas relacionadas con la adquisición de imágenes forenses:

- Copia bit a bit: réplica exacta de los bits de un volumen lógico o de una unidad física. Cuando la copia se realiza en otro disco, se la denomina duplicado forense. Cuando la copia se realiza en uno o varios archivos, se la denomina imagen forense.
- Duplicado forense: conjunto de archivos que se obtiene creando una copia exacta de un dispositivo de almacenamiento. Dicha copia replica la estructura y contenidos en un nuevo dispositivo.
- Imagen forense: archivo o conjunto de archivos que se obtiene al crear una copia completa de un dispositivo de almacenamiento, replicar su estructura y contenidos e incluir el espacio libre y el espacio no asignado.
- Imagen forense sin formato (RAW): imagen sin formato que no contiene metadatos y no está comprimida. Puede adjuntarse por separado un archivo que contiene metadatos sobre la imagen, como fecha en que fue adquirida, nombre de la herramienta utilizada y hash criptográfico.
- Imagen forense embebida: imagen de disco que contiene incrustados metadatos sobre la imagen, tales como nombre de la herramienta utilizada, fecha de adquisición, datos relacionados al caso, investigador, evidencia relevada y hash criptográfico correspondiente.

2.1.1.11 Concepto de Hash

Se define al HASH[1] como el proceso de tomar una cantidad de datos determinada (como un archivo o el flujo de bits de un disco duro) y aplicar un algoritmo matemático complejo para generar un identificador numérico relativamente compacto (el valor hash) exclusivo de esos datos [19].

[1] El algoritmo HASH es una función algebraica unidireccional que permite representar datos de longitud variable como un dato de longitud fija, tiene como objetivo garantizar la integridad de los registros informáticos.

Como ejemplo, un valor hash generado respecto de un documento será único; si se modificara, alterara o destruyere parcialmente dicho documento, el valor hash resultante será diferente.

Existen varios puntos relevantes sobre los algoritmos hash.

- Son irreversibles. Los algoritmos (funciones hash iterativas y unidireccionales) que se utilizan para generar el valor de hash no se pueden revertir para reconstruir los datos originales de entrada [20].
- Baja probabilidad de colisiones. Las probabilidades de que dos datos no idénticos generen el mismo algoritmo es ínfima y se encuentra limitada por formato del algoritmo empleado. A modo de ejemplo se pueden citar el formato MD5[2] el cuál se trata de un algoritmo de reducción criptográfico de 128 bits cuya longitud es de 32 caracteres o el formato SHA1[3] , el cuál se trata de un algoritmo de reducción criptográfico de 160 bits cuya longitud es de 40 caracteres.

2.1.1.12 Artefacto forense

Este término hace referencia a cualquier registro informático correspondiente a una aplicación o programa de software, que desempeña alguna función específica.

2.1.1.13 Cadena de custodia

Es el registro cronológico y minucioso de la manipulación adecuada de los elementos, rastros e indicios hallados en el lugar del hecho, durante todo el proceso judicial [21].

2.1.2 La Evidencia Digital

Resulta difícil enunciar una definición universal, sin embargo se puede señalar que la evidencia digital es un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos, que por sus características deben ser recolectados y analizados con herramientas y técnicas especiales [22].

[2] Acrónimo de "Message-Digest Algorithm 5", el cuál se trata de un algoritmo de reducción criptográfico de 128 bits cuya longitud es de 32 caracteres.
[3] Acrónimo de "Secure Hash Algorithm 1", el cuál se trata de un algoritmo de reducción criptográfico de 160 bits cuya longitud es de 40 caracteres.

Cabe destacar que el término evidencia digital es una denominación empleada de manera extensa, describiendo de esta manera cualquier registro generado o almacenado en un sistema computacional o dispositivo informático, cuya clasificación puede realizarse según sus características, naturaleza, orden de volatilidad y admisibilidad:

2.1.2.1 Características

La evidencia digital es la materia prima para los investigadores forenses donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando el ambiente tan cambiante y dinámico de las infraestructuras de computación y telecomunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno [23].

Acorde a lo expuesto precedentemente, podría decirse que la evidencia digital es un constante desafío para los investigadores forenses, destacándose por su:

- Volatilidad: periodo de disponibilidad que posee en función del tiempo.
- Anonimato: capacidad de ocultar la identidad de quién generó el registro.
- Capacidad de duplicación: posibilidad de realizar copias idénticas.
- Posibilidad de alteración y modificación: capacidad de ser manipulada.
- Alta probabilidad de eliminación: fácil acceso y carencia de permisos.

2.1.2.2 Según su naturaleza

Conforme lo define el Manual de Estándares de Australia[4] HB: 171/2003 “Directrices para la Gestión Evidencia de Tecnología Informática” [6], la evidencia digital puede subdividirse en tres categorías:

- Registros almacenados en el equipo de tecnología informática (por ejemplo, correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.).
- Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).

[4] Documento elaborado por la Organización de estándares de Australia, creada con el fin de asistir a las organizaciones para combatir el crimen electrónico.

- Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática (hojas de cálculo, consultas en bases de datos, vistas parciales de datos, etc.).

Nótese que la presente clasificación engloba a la evidencia digital en su totalidad, debiendo prestar especial atención en el factor humano, dado que resulta determinante identificar si fue una persona o un dispositivo informático quien creó el contenido del registro o archivo.

2.1.2.3 Conforme el orden de volatilidad

La RFC 3227/2002 “Guía Para Recolectar y Archivar Evidencia” [5] de *Internet Society*[5], establece el siguiente orden de volatilidad y por tanto de recopilación de evidencias:

- Registros y contenidos de la caché.
- Contenidos de la memoria RAM.
- Estado de las conexiones de red, tablas de rutas.
- Estado de los procesos en ejecución.
- Contenido del sistema de archivos y de los discos duros.
- Contenido de otros dispositivos de almacenamiento.

En tal sentido, resulta pertinente hacer notar que primeros cuatro apéndices representan datos de carácter volátil, es decir que se perderán o modificarán si apaga o reinicia el sistema, resultando es por tanto muy fácil eliminar evidencias de forma inadvertida.

Por el contrario, los dos últimos apéndices, hacen referencia a medios de almacenamiento (discos rígidos, discos de estado sólido, soportes ópticos, etc), cuya información perdura en el tiempo bajo condiciones normales de uso y una adecuada cadena de custodia.

[5] Sociedad de Internet, organización no gubernamental y sin fines de lucro, con dedicación exclusiva sobre el desarrollo mundial de Internet.

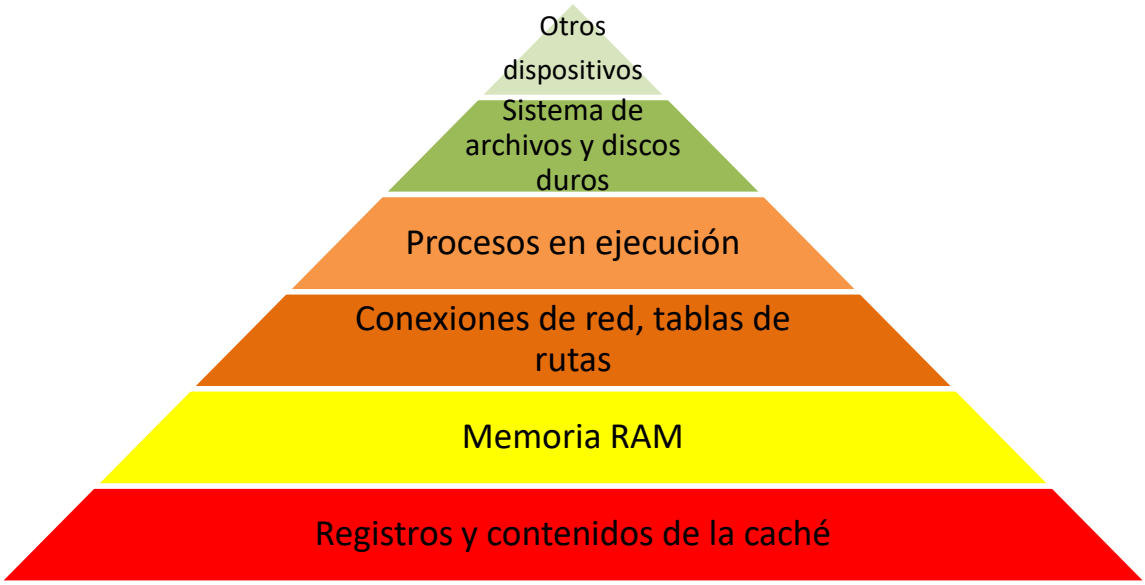

Ilustración 2: Orden de volatilidad de la Evidencia Digital.

2.1.2.4 Criterios de admisibilidad

En legislaciones modernas, existen ciertos criterios que se deben tener en cuenta [23]. Los mismos son:

- Admisibilidad: debe tener valor legal.
- Autenticidad: debe ser verídica y no haber sufrido manipulación alguna. A tal fin, se calculan firmas digitales que garantizan su integridad.
- Completitud: la prueba debe ser presentada desde un punto de vista objetivo y técnico, sin valoraciones personales o prejuicios.
- Credibilidad: debe ser creíble y de fácil comprensión.
- Confiabilidad: las técnicas utilizadas para su obtención no deben generar duda sobre su veracidad y autenticidad.

2.1.3 La Informática Forense [17]

Según el Departamento Federal de Investigaciones de los Estados Unidos, la Informática Forense es considerada una rama de las ciencias forenses, que tiene como finalidad identificar, preservar, analizar y presentar datos que han sido procesados electrónicamente, y almacenados en un medio digital.

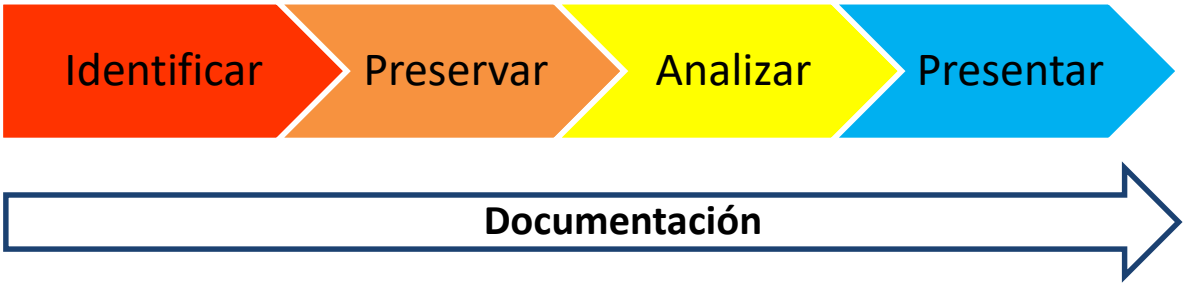

Ilustración 3: Fases del análisis forense digital.

Conforme la definición planteada, se pueden observar cuatro etapas discriminadas taxativamente como:

2.1.3.1 Identificación

Constituye el primer acercamiento a los medios de prueba digitales, implica procesos tendientes a su individualización unívoca (marca, modelo, tipo de dispositivo, etc), a fin de dilucidar posteriormente interrogantes como por ejemplo qué cosas pueden ser evidencias y cuáles no, dónde y cómo están almacenados los registros, etc.

Brinda un punto de partida que permite al investigador establecer las metodologías de adquisición y recuperación de evidencias adecuadas, así como las herramientas forenses a utilizar en los pasos subsiguientes, tanto de hardware como de software.

2.1.3.2 Preservación

Tiene como finalidad salvaguardar la integridad y autenticidad de las evidencias digitales relevadas, garantizando la seguridad de la cadena de custodia. Cualquier cambio en la evidencia deberá ser documentado.

En tal sentido, se aplican DOS (2) Algoritmos HASH distintos: MD5 y SHA1. El cálculo de los mismos garantiza, en todo momento, la integridad y autenticidad de las evidencias digitales recolectadas. Es dable de mencionar, que se calculan DOS (2) algoritmos de manera simultánea, ya que de esa manera se garantiza que los mismos, de manera conjunta, resultan ser otra forma de identificar *UNÍVOCAMENTE* a tales registros.

Sin perjuicio de lo expresado, si bien los algoritmos de seguridad MD5 y SHA1 son empleados con mayor frecuencia, no solo por los investigadores forenses de todo el mundo sino también provistos por defecto mediante distintas herramientas, resulta oportuno destacar que los mismos pueden presentar colisiones[6], por cuanto existen otros formatos de mayor complejidad como por ejemplo SHA2, algoritmo de reducción criptográfico de 256 bits cuya longitud es de 64 caracteres.

2.1.3.3 Análisis

Consiste en el conjunto de técnicas y procedimientos empleados a fin de inspeccionar y examinar los datos contenidos en los medios de prueba remitidos para estudio, conforme la requisitoria pericial planteada.

Debe contener un detalle de las herramientas informáticas empleadas, así como las operaciones realizadas y resultados obtenidos. La identificación de hallazgos o recopilación de evidencia notable puede resultar complicada, puesto que no se debe dañar ninguna de sus características; teniendo en cuenta que es susceptible a variaciones y tendencia a perderse si no se trata adecuadamente.

2.1.3.4 Presentación

Consiste en el proceso de elaborar un reporte a fin de presentar la evidencia relevada en un formato legalmente aceptable y comprensible, incluso por quien no posea experiencia computacional, caso contrario el esfuerzo impreso en el trabajo no tendrá sentido.

Al mismo tiempo, se adjuntan las evidencias recolectadas mediante dispositivos de almacenamiento, permitiendo disponer en todo momento de un respaldo de los archivos que resultan de interés para la investigación.

2.1.4 Normas y estándares vinculados a la Informática Forense

En primer lugar, es importante destacar que no existe un procedimiento estándar empleado para el análisis forense digital. Sin embargo, un gran número de instituciones y organismos han creado diferentes directrices consideradas guías o reglas de buena práctica que abordan la temática desde diferentes enfoques, con

[6] Situación que se produce cuando se aplica una misma función hash sobre dos entradas diferentes y se produce el mismo resultado.

el objetivo gestionar e identificar la evidencia digital para ser empleada dentro de una investigación.

Estas reglas se basan en el método científico para concluir o deducir algo acerca de la información, presentando una serie de etapas para recolectar la mayor cantidad de evidencia digital y permitir incluso la posterior reconstrucción de determinados eventos o incidentes informáticos.

Por tal motivo y a fin de realizar el presente trabajo, conforme los criterios de selección señalados con antelación, se procederá a listar aquella documentación incorporada, en tenor de su alcance y estrecha vinculación con el análisis forense digital, brindándose además una somera descripción de su contenido, que luego será ponderado en función de una serie de parámetros delimitados cualitativamente al momento de realizar la comparación respectiva.

2.1.4.1 Guía Para Recolectar y Archivar Evidencia (RFC 3227/2002)

Esta guía fue elaborada en el año 2002 por *Internet Society*, la cual provee reglas de buena práctica para determinar la volatilidad de la evidencia digital, decidir qué y cómo recolectarla, y determinar su almacenamiento y documentación. Dentro de estructura se aprecian:

- Introducción.
- Principios de recolección de evidencia digital.
- El proceso de recolección.
- El proceso de archivo.
- Herramientas necesarias.

2.1.4.2 Directrices para la Gestión Evidencia de Tecnología Informática (SAI HB 171/2003) [6]

El documento fue confeccionado por *Standards Australia International*[7], con el fin de asistir a las organizaciones para combatir el crimen electrónico, estableciendo puntos de referencia para la preservación y la recolección de la

[7] Estándares Internacionales de Australia, es un organismo que tiene como finalidad el desarrollo y aplicación de estándares técnicos y productos y servicios relacionados.

evidencia digital. Detalla el ciclo de administración de evidencia de la siguiente forma:

- Diseño de la evidencia.
- Producción de la evidencia.
- Recolección de la evidencia.
- Análisis de la evidencia.
- Reporte y presentación.
- Determinación de la relevancia de la evidencia.

2.1.4.3 Guía para integrar técnicas forenses en respuesta a incidentes (NIST 800-86-2006) [7]

Esta guía pertenece al *National Institute of Standards and Technology*[8], la misma establece normas y directrices, incluyendo requisitos mínimos para proporcionar una adecuada seguridad de la información en las operaciones y activos de una organización. Posee la siguiente disposición:

- Introducción.
- Establecer y organizar las capacidades forenses.
- Realizar el proceso forense.
- Recolectar datos de archivos de datos.
- Usar datos de sistemas operativos.
- Recabar datos del tráfico de red.
- Emplear datos de aplicaciones.
- Utilizar datos de múltiples fuentes.
- Anexos (recomendaciones, escenarios, glosario, acrónimos, recursos de impresión, herramientas y recursos en línea).

[8] Instituto Nacional de Estándares y Tecnología, agencia de la Administración de Tecnología del Departamento de Comercio de Estados Unidos que promueve la innovación y competitividad industrial mediante el avance de la ciencia, los estándares y la tecnología.

2.1.4.4 Investigación en la Escena del Crimen Electrónico: una guía para primeros intervinientes (US DoJ NCJ 219941 /2008) [8]

Esta guía fue concebida en el seno del *United States Department of Justice* [9], centra su enfoque en la identificación y recolección de evidencia. Contempla los siguientes aspectos:

- Tipos de dispositivos electrónicos.
- Herramientas y equipamiento forense.
- Reglas de preservación y evaluación de la escena del hecho.
- Pasos para documentación de la escena.
- Procedimientos para recolección de evidencia.
- Elementos para preservación de la evidencia.
- El análisis forense y clasificación de delitos.
- Anexos (glosario, recursos legales, técnicos y de capacitación).

2.1.4.5 Computación Forense - Parte 2: mejores prácticas (ISFS/2009) [9]

Esta guía de buenas prácticas fue redactada por *Information Security and Forensic Society*[10], contemplando procedimientos y requerimientos involucrados en el análisis forense de la evidencia digital, desde el examen de la escena del delito hasta la presentación de los correspondientes reportes. Su estructura se encuentra conformada por:

- Introducción a la computación forense.
- Calidad en la computación forense.
- Evidencia digital.
- Recolección de evidencia.
- Consideraciones legales.

[9] Departamento de Justicia de los Estados Unidos, Ministerio del gobierno de Estados Unidos, encargado de la administración de la justicia.

[10] Sociedad de Seguridad de la Información y Computación Forense, organismo de Hong Kong cuya misión es abogar y hacer cumplir el profesionalismo, integridad e innovación en tal materia.

- Anexos.

2.1.4.6 Guía de Buenas Prácticas para evidencia basada en computadoras (ACPO/2012) [10]

Este documento fue elaborado por *Asociation of Chief Police Officers*[11], tiene por finalidad ser empleado como guía de buenas prácticas para casos con equipos de computación y diferentes dispositivos electrónicos que puedan ser considerados como evidencia. Enumera los siguientes aspectos:

- Principios de la evidencia digital.
- Agentes de la ley en la escena del delito.
- Agentes de la ley investigadores.
- Expertos en recuperación de la evidencia digital.
- Testigos.
- Anexos (casos de estudio, recursos técnicos y de capacitación).

2.1.4.7 Evidencia Electrónica - Una guía básica para primeros intervinientes (ENISA/2014) [11]

La guía se redactó por European Network and Information Security Agency[12], la misma provee principios de calidad para la detección, la prevención, la recuperación y el análisis de la evidencia digital. Contempla los sistemas, los procedimientos, el personal, el equipo y los requerimientos necesarios desde la escena del delito hasta su presentación. Su esquema abarca:

- Objetivos.
- Alcance.
- Fondo.
- Introducción.

[11] Asociación de Jefes de Policía de Inglaterra, Gales e Irlanda del Norte, es una sociedad limitada sin fines de lucro que lidera el desarrollo de prácticas policiales en diferentes temáticas.

[12] Agencia Europea de Seguridad de las Redes y de la Información, agencia de la Unión Europea que tiene como finalidad contribuir al desarrollo de una cultura de red y seguridad de la información para el beneficio de los ciudadanos, consumidores, empresas y organizaciones de la región.

- Reunión de evidencia electrónica.
- Principios de recopilación de evidencia electrónica.
- Antes de llegar a la escena del crimen.
- Juego de herramientas para los primeros intervinientes.
- Computadora portátil forense del primer interviniente.
- Herramientas y comandos del primer interviniente.
- Al llegar a la escena.
- Implementación.
- Memoria forense.
- Examen de pruebas.
- Extracción.
- Análisis.
- Evaluación y presentación de la evidencia.
- Observaciones finales.
- Anexos.

2.1.4.8 Principios para identificación, recolección, adquisición y preservación de pruebas digitales (ISO/IEC 27037/2016) [12]

Esta guía fue elaborada por el *International Standarization Organization*[13] e *International Electronic Comission* [14], proporcionando pautas para actividades específicas en el manejo de evidencia digital potencial. Estos procesos son: identificación, recopilación, adquisición y preservación de la evidencia digital. Contempla los siguientes apartados:

- Introducción.

[13] Organización Internacional de Normalización, organización con sede en Suiza que tiene como finalidad crear y promover estándares propietarios, industriales y comerciales a nivel mundial.

[14] Comisión Electrotécnica Internacional, organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas en Estados Unidos.

- Alcance.
- Referencia normativa.
- Términos y definiciones.
- Términos abreviados.
- Visión de conjunto.
- Componentes clave de identificación, recopilación, adquisición y preservación de evidencia digital.
- Instancias de identificación, colección, adquisición y preservación.
- Anexos (descripción de competencias básicas del primer interviniente y requisitos mínimos de documentación).

2.1.4.9 Guía de obtención, preservación y tratamiento de evidencia digital (PGN 756/2016) [13]

En virtud de las actividades desarrolladas por la Unidad Fiscal Especializada en Ciberdelincuencia[15], se elaboró un documento señalando una serie de herramientas de investigación como forma de reforzar las actividades del Ministerio Público Fiscal en aquellos casos donde se deba tratar con evidencia digital. El mismo tiene como finalidad establecer aquellos principios que permitirán llevar a cabo investigaciones y recolección de pruebas electrónicas en materia de ciberdelitos, contemplando diferentes aspectos.

- Introducción.
- La evidencia digital.
- Principios de tratamiento de la evidencia digital
- Recolección y preservación de evidencia digital.
- Presupuestos Generales.
- Principios especiales.

[15] Fiscalía especializada en materia de ciberdelincuencia, que tiene como finalidad la lucha contra el cibercrimen de manera articulada con otras áreas de la Procuración General de la Nación que se dedican a la investigación del crimen organizado.

- Embalaje, traslado y resguardo de la evidencia digital.
- Manipulación idónea del hardware.
- Imagen o copia forense y uso de hash.
- Aspectos a tener en cuenta al momento de analizar la evidencia digital recolectada en función de los delitos a investigar.

2.1.4.10 Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la investigación y proceso de recolección de pruebas en Ciberdelitos (MINSEG RES 234/2016) [14].

Debido a que las cifras de los ciberdelitos se incrementan exponencialmente con el correr de los años, el estado nacional ha propiciado la creación de Unidades Especiales de Investigación en aquellas Fuerzas de la ley dependientes del Ministerio de Seguridad, cuya actuación se encuentra normada mediante la Resolución 234/2016 "Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos".

Dicho protocolo de actuaciones tiene como finalidad establecer los principios para llevar a cabo investigaciones y recolección de pruebas electrónicas en materia de ciberdelitos, contemplando diferentes aspectos.

- Reglas generales, definiciones y principios.
- Principios generales de intervención.
- Principios específicos de intervención.
- Pautas específicas de actuación.
- Capacitaciones.

2.1.4.11 Requisitos generales para la competencia de los laboratorios de ensayo y de calibración (ISO/IEC 17025/2017)

Esta guía fue elaborada por el *International Standarization Organization*[16] e *International Electronic Comission*[17], contiene requisitos que permiten a los

[16] Op. cit.

[17] Op. cit.

laboratorios demostrar que operan de forma competente y que tienen la capacidad de generar resultados válidos. Cabe destacar que los laboratorios que cumplen con este documento también operarán en general de acuerdo con los principios de la Norma ISO 9001. Su estructura, contemplan los siguientes apartados:

- Introducción.
- Objeto y campo de aplicación.
- Referencias normativas.
- Términos y definiciones.
- Requisitos generales (Imparcialidad / Confidencialidad).
- Requisitos relativos a la estructura.
- Requisitos relativos a los recursos (Personal / Instalaciones y condiciones ambientales / Equipamiento / Trazabilidad metrológica / Productos y servicios suministrados).
- Requisitos del proceso (Revisión de solicitudes / Selección, verificación y validación de métodos / Muestreo / Manipulación de los ítems de ensayo y calibración / Registros técnicos / Evaluación de la incertidumbre / Aseguramiento de la validez de los datos / Informe de resultados / Quejas / Trabajo no conforme / Control de los datos y gestión de la información).
- Requisitos del sistema de gestión (Opciones / Documentación / Control de documentos / Control de registros / Acciones para abordar riesgos y oportunidades / Mejora / Acciones correctivas / Auditorías internas / Revisiones por la Dirección).
- Anexos (Trazabilidad metrológica y opciones del sistema de gestión).

2.1.5 Aspectos legales en nuestro país

A fin de brindar un panorama sobre el marco legal vigente en nuestro país al momento de haberse realizado el presente trabajo, se describirán sucintamente aquellas normas consideradas de interés y que guardan relación con la temática propuesta.

2.1.5.1 Contexto general

En un principio, dentro de la normativa penal de nuestro país no se encontraban contemplados aquellos delitos relacionados con el uso de las nuevas tecnologías de la comunicación e información.

Sin embargo, a fin de suplir este vacío legal, surgieron ciertas figuras penales que relacionaban esta temática con ciertas leyes especiales.

- Ley 11723 de Propiedad Intelectual, contempla aquellos delitos relacionados con los derechos de autor [24].
- Ley 22362 de Registros Marcarios, ampara los delitos que atentan contra las designaciones marcarias [25].
- Ley 25326 de Protección de Datos Personales, cuyo bien jurídico tutelado es la intimidad y privacidad de información sensible [26].
- Ley 24766 de Confidencialidad, que ampara la sustracción de secretos comerciales contenidos en medios informáticos [27].
- Ley Penal Tributaria 24769, que contempla la alteración dolosa de registros [28].
- Ley Antidiscriminatoria 23592, norma los delitos relacionados con conductas xenofóbicas [29].

2.1.5.2 Ley 26388 [30]

A fin de distinguir aquellas actividades criminales relacionadas con el uso de la tecnología de la información y propósito de lo anterior, en el año 2008 fue sancionada la ley 26388, conocida localmente como la ley de delitos informáticos, la cual tipifica e incorpora al Código Penal diferentes conductas delictivas vinculadas a esta temática.

- Daños informáticos.
- Fraudes informáticos.
- Alteración de pruebas.
- Pornografía infantil.

- Delitos contra la privacidad.
- Delitos contra la seguridad pública e interrupción de las comunicaciones
- Falsificación de documentos electrónicos.

2.1.5.3 Ley 26904 [31]

A fin de incorporar el acoso por medios electrónicos al Código Penal, en el año 2013 fue sancionada la ley 26904, conocida localmente como la ley de ciberacoso, la cual tipifica e incorpora conductas delictivas contra la integridad sexual de los menores por medio de:

- Comunicaciones electrónicas.
- Telecomunicaciones.
- Cualquier otra tecnología de transmisión de datos.

2.1.5.4 Normativa complementaria

- Resolución Nro 580/2011 de La Jefatura de Gabinete de Ministros, crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad en el ámbito de la Oficina Nacional de Tecnologías de Información (ONTI) [32].
- Disposición Nro 3/2011 de La Oficina Nacional de Tecnologías De Información (ONTI), establece el “Formulario de adhesión al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad” [33].
- Disposición Nro 2/2013 de la Oficina Nacional de Tecnologías de Información (ONTI), crea el grupo de trabajo “ICIC – CERT” (Computer Emergency Response Team) en el marco del “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad” [34].
- Decreto Nro 1067/2015, establece que en el Organigrama de la Administración Pública Nacional se instituye a la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad en el ámbito de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros [35].

- Disposición Nro 5/2015 de la Jefatura de Gabinete, crea en la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad el "Registro de Equipos de Respuesta ante Incidentes de Seguridad Informática" [36].
- Resolución Nro 1046/2015 de la Jefatura de Gabinete de Ministros, establece la estructura organizativa de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad [37].
- Resolución PGN Nro 3743/15 de la Procuración General de la Nación, crea la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) [38].
- Ley Nro 27.126, establece dentro de las funciones de la Agencia Federal de Inteligencia (AFI) la producción de inteligencia criminal referida a los delitos federales complejos relativos a ciberdelitos [39].
- Resolución PGN Nro 756/16 de la Procuración General de la Nación, brinda una serie de recomendaciones para analizar y preservar evidencia digital [13].
- Resolución Nro 234/16 del Ministerio de Seguridad de la Nación, establece un Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la investigación y proceso de recolección de pruebas en Ciberdelitos [14].
- Decisión Administrativa Nro 564/2018 de la Jefatura de Gabinete de Ministros, establece la Dirección de Investigaciones del Ciberdelito en el ámbito de la Dirección Nacional de Investigaciones [40].
- Decisión Administrativa Nro 641/2021 de la Jefatura de Gabinete de Ministros, establece los requisitos mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional [41]

2.2 Marco Teórico Referencial

En esta sección se brindarán los conceptos que se consideran primordiales para la comprensión del desarrollo del presente trabajo.

2.2.1 Modelo simplificado de análisis forense digital

A partir del estudio realizado en el Trabajo Final de Especialización sobre diferentes reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de informática forense y evidencia digital, resultó factible identificar que el proceso de análisis forense digital se encuentra conformado por seis etapas distintas de procesamiento y definir las habilidades necesarias para realizar las diversas actividades requeridas en cada una de ellas.

Por tal motivo, las etapas identificadas se analizaron y se tradujeron en un modelo simplificado que se adapta no solo a las investigaciones forenses sino también a los procesos llevados a cabo en el laboratorio de análisis forense digital, permitiendo identificar los elementos clave de cada proceso y relacionarlo directamente con los exámenes forenses, sus fuentes de entrada y los pasos específicos involucrados en cada etapa del procesamiento.

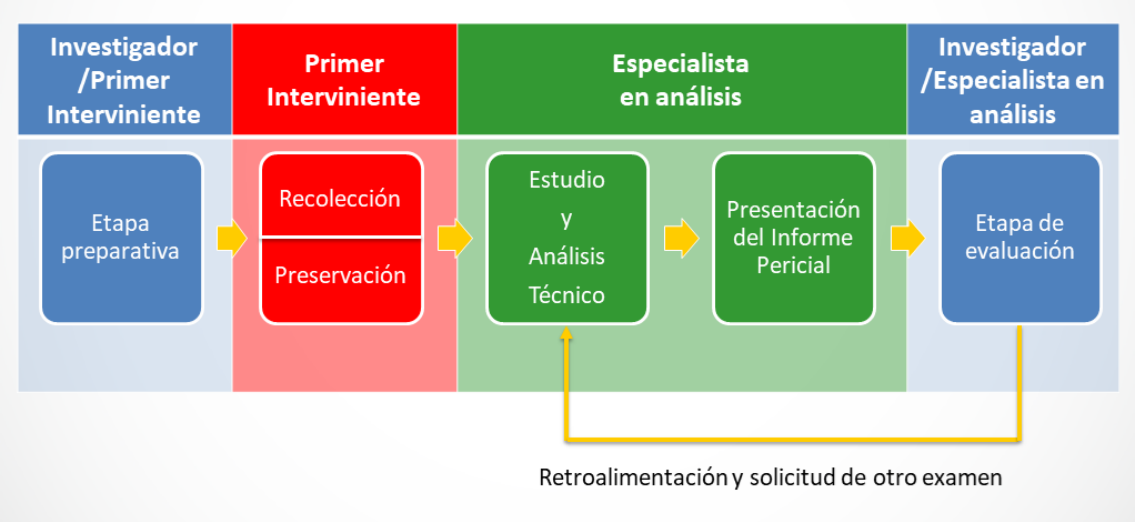

Ilustración 4: Modelo simplificado de análisis forense digital.

A continuación, se detalla cada una de las etapas que componen el modelo simplificado junto a las actividades específicas que fueron consideradas para realizar la evaluación correspondiente, cuyas matrices se encuentran plasmadas en los Anexos correspondientes.

2.2.1.1 Etapa preparativa[18]

Es aquella etapa donde se enuncian actividades preliminares para responder ante el incidente o requerimiento planteado, que tiene como finalidad planificar y organizar el proceso de investigación digital, según las siguientes actividades específicas:

- Recepción del requerimiento; mantiene estrecha relación con la manera en que el personal interviniente recibe el requerimiento y plazos de cumplimiento.
- Revisión de capacidades; implica la identificación de capacidad para dar respuesta ante el requerimiento planteado.
- Definición del alcance; establece las actividades a realizar por parte del personal interviniente.
- Equipamiento básico; brinda un detalle orientativo de aquel equipamiento básico necesario para dar cumplimiento a requerimiento solicitado.
- Planificación y diseño; marca una orientación sobre cómo deben programarse las actividades a fin de evacuar el requerimiento encomendado.

2.2.1.2 Etapa de identificación [19]

Es el primer acercamiento a los medios de prueba digitales, permitiendo al investigador su individualización unívoca y prever metodologías adecuadas para su adquisición, recuperación y preservación, según las siguientes actividades específicas:

- Tipos de infraestructura; permite conocer el entorno y ponderar su magnitud (computadoras personales, servidores, servicios en la nube).
- Tipos de dispositivos; implica la identificación univoca de aquellos dispositivos que podrían contener evidencia digital.

[18] Ver Anexo “Tabla 1: Etapa preparativa”.

[19] Ver Anexo “Tabla 2: Etapa de identificación”.

- Valoración de posibles evidencias; establece la recolección de evidencias digitales según su vinculación con los hechos investigados.
- Otras evidencias físicas; contempla la identificación de evidencias físicas tales como anotaciones, manuales, periféricos, etc.
- Requisitos previos a la adquisición; aporta aquella información necesaria para la obtención de copias de respaldo.

2.2.1.3 Etapa de preservación [20]

Tiene como finalidad salvaguardar la integridad y autenticidad de las evidencias digitales identificadas, mediante la cadena de custodia correspondiente, según las siguientes actividades específicas:

- Orden de volatilidad; señala los diferentes estadios de la evidencia digital según su capacidad de permanecer en el tiempo.
- Tipos de evidencia (Física/Lógica); implica la posibilidad de obtener evidencias digitales en el laboratorio forense o bien en el mismo lugar de la incautación.
- Algoritmos de seguridad; indica puntos de control de integridad mediante la implementación de firmas digitales HASH.
- Consideraciones legales; guarda relación con el cumplimiento de la normativa legal vigente.
- Cadena de custodia; establece la necesidad de contar con mecanismos que permitan la trazabilidad de los elementos incautados.

2.2.1.4 Etapa de análisis [21]

Tiene como finalidad establecer la existencia de evidencia notable y documentar dichos hallazgos, conforme la requisitoria pericial planteada, según las siguientes actividades específicas:

[20] Ver Anexo “Tabla 3: Etapa de preservación”.

[21] Ver Anexo “Tabla 4: Etapa de análisis”.

- Lista de artefactos forenses; establece posibles elementos a identificar, como por ejemplo archivos de usuario, historial de internet, redes sociales, etc.
- Línea de tiempo; comprende ordenar los eventos identificados en función del tiempo a los efectos de correlacionar datos.
- Firmas de archivo; permite identificar técnicas anti-forenses para ocultar y/o enmascarar información.
- Palabras clave; establece búsquedas específicas mediante nombres propios, alias, número de documento, direcciones de correo electrónico, etc.
- Técnicas y herramientas para procesamiento; aporta aquella información necesaria para el análisis de la información recolectada.

2.2.1.5 Etapa de presentación[22]

Involucra aquellas actividades que permiten elaborar un reporte a fin de presentar y remitir los hallazgos relevados, según las siguientes actividades específicas:

- Reporte de resultados; versa sobre la elaboración de un documento donde se encuentren plasmados los resultados obtenidos.
- Remisión de hallazgos; se encuentra ligada con la forma en que se remiten las evidencias recolectadas, ya sea mediante unidades externas de almacenamiento o soportes ópticos tipo CD/DVD.
- Mecanismos para su preservación; implica la adopción de copias de respaldo que garanticen la disponibilidad de aquellas evidencias recolectadas.
- Modelos de trabajo; versa sobre la existencia de documentos y/o casos de estudio para adoptar como ejemplos de trabajo.
- Recomendaciones; indica una serie de variables que deben tenerse en cuenta, como por ejemplo tiempos de cumplimiento, alcance de la investigación, etc.

[22] Ver Anexo “Tabla 5: Etapa de presentación”.

2.2.1.6 Etapa de evaluación [23]

Es aquella etapa complementaria que permite evaluar los resultados obtenidos a fin de ponderar la utilidad de los mismos, aportando información que permita la toma de decisiones según las siguientes actividades específicas:

- Análisis de los resultados obtenidos; permite encauzar la investigación a raíz de los resultados obtenidos.
- Ponderación de los resultados obtenidos; comprende catalogar los eventos identificados en función de su preponderancia.
- Revisión de metodologías aplicadas; permite identificar posibles errores durante el análisis practicado.
- Identificación de interrogantes adicionales; contempla establecer o descartar nuevas hipótesis sobre el hecho investigado.
- Reformulación del alcance; establece nuevos puntos de pericia sobre los elementos analizados en función de las evidencias evaluadas.

2.2.2 Normalización de los laboratorios de análisis forense digital

En la actualidad y cada vez con mayor frecuencia, no es raro que los abogados defensores intenten atacar la credibilidad de los examinadores forenses, los procesos del laboratorio de análisis forense digital, sus registros e informes técnicos periciales y cualquier conclusión relacionada.

En tal sentido, de esta afirmación se desprende qué si es posible poner en duda la recopilación y el manejo inicial de las evidencias digitales, el resultado obtenido a partir de su procesamiento y análisis resulta totalmente discutible, ya que la evidencia fruto de tales procesos es tildada de permeable y podría ser cuestionada por no ser irrefutable, afectando su valor probatorio e impidiendo su incorporación en todo proceso legal.

[23] Ver Anexo “Tabla 6: Etapa de evaluación”.

2.2.2.1 Principales desafíos

Los esfuerzos concentrados en los procedimientos técnicos aplicados en el campo del análisis forense digital han generado una brecha que con el tiempo se acentúa debido a que toda investigación digital no debe dejar de lado desafíos en los ámbitos procesal, social y legal.

Existen una serie de componentes clave que brindan una visión integradora de las investigaciones relacionadas con el análisis forense digital, este enfoque de amplio espectro abarca los siguientes aspectos:

- Técnico: el ritmo vertiginoso del ecosistema tecnológico en el que nos encontramos inmersos se encuentra sujeto a cambios que ocurren muy rápidamente. Así, por ejemplo, el creciente incremento de la capacidad de almacenamiento de los dispositivos y velocidad de inserción en el mercado son solo dos puntos a tener en cuenta debido a la dificultad que representan al momento de ser analizados mediante el uso de herramientas forenses disponibles en la actualidad. Además, no debemos pasar por alto la falta de experiencia y capacitación que prevalece entre los examinadores forenses.
- Procesal: los analistas forenses deben recopilar todos aquellos artefactos que en el extenso mundo digital puedan ser motivo de examen y observación, cuyos volúmenes de datos hasta ahora resultan inauditos. En tal sentido, cabe destacar que los procedimientos y protocolos analíticos no se encuentran estandarizados ni existe una terminología estándar utilizada por los profesionales e investigadores.
- Social: la privacidad individual y las necesidades de recopilación y análisis de información se contraponen constantemente. La incertidumbre acerca de la precisión y eficacia de las técnicas actuales ocasiona un cuello de botella motivo de la constante necesidad de almacenar copias de respaldo guarden durante períodos de tiempo muy prolongados. Tal circunstancia ocasiona un perjuicio contra los recursos materiales, que en la mayoría de los casos resulta más que finito.
- Legal: a pesar de contar con los mayores avances tecnológicos del mercado, su aplicabilidad varía según el marco legal vigente en cada país,

siendo discutible su utilización en caso de cualquier incumplimiento con la normativa regulatoria correspondiente.

Del mismo modo, debemos tener en cuenta que toda evidencia digital presentada en el marco de procesos judiciales debe cumplir con estrictos requisitos de aceptación y admisibilidad. Por tal motivo, los laboratorios de análisis forense digital necesitan contar con sistemas de gestión de la calidad con el fin de obtener su acreditación mediante la adopción e implementación de procesos normalizados.

2.2.2.2 Requisitos generales para la competencia de laboratorios forenses

La ISO/IEC 17025:2017 es un estándar que puede aplicarse generalmente a una amplia variedad de laboratorios de prueba (y calibración), como lo es el caso de laboratorios donde se realizan ensayos ambientales, farmacéuticos, de alimentos, de pruebas de materiales, servicios de salud y, en ausencia de una alternativa mejor, también puede ser adoptado por laboratorios de análisis forense digital.

Esta norma, requiere un abordaje específico sobre los problemas que afectan directamente la calidad de los datos (resultados) y la competencia técnica del personal. Su principal objetivo es garantizar que los principios de calidad se apliquen de manera coherente y que cualquier desviación se encuentre documentada, controlada y restringida. La ISO 17025:2017 es considerada como un medio para garantizar que los principios científicos relacionados con las pruebas de laboratorio y sistemas de gestión de calidad sean aplicados uniformemente por aquellos laboratorios acreditados.

Ahora bien, respecto a esta norma como estándar general de garantía de calidad para laboratorios de pruebas y calibración, cabe destacar que no considera ciertas características que inciden directamente la implementación de un laboratorio de análisis forense digital, entre las que se incluyen:

- Como estándar podría ser de gran utilidad para hacer cumplir el sistema de gestión de calidad, sin embargo, también es importante señalar la relación costo/beneficio vinculada con factores como tiempo y recursos, dado que su implementación y mantenimiento requieren de procesos adicionales y gastos generales que deberían afrontarse para cumplir con la normativa.
- Se requieren una serie de métodos de prueba documentados para

"exámenes" en particular, debiéndose aquilatar además ciertas medidas de incertidumbre, situación que no se puede traducir a los procedimientos vinculados con el análisis forense digital.

- En la mayoría de ensayos científicos de laboratorio, el equipo de prueba debe calibrarse antes del inicio. Esta premisa no siempre puede ser cumplida en el campo del análisis forense digital, por ese motivo es necesario adaptar la ISO 17025 a lo que es práctico y realista para el cómputo forense.

Acorde lo expresado, si bien la ISO 17025 proporciona una base constituida por un conjunto mínimo de requisitos como punto de partida, requiere cierta adaptación para abordar los desafíos comerciales, técnicos y de óptima eficiencia de un laboratorio de análisis forense digital.

Por otro lado, esta norma no tiene en cuenta los requisitos del modelo de madurez de capacidades vinculados con personas, procesos y herramientas tecnológicas, ni es adecuada para atender las diferencias técnicas en diferentes procesos del modelo simplificado de análisis forense digital planteado.

2.2.2.3 Sistema de gestión de calidad basado en procesos

La familia ISO 9000 es un conjunto de normas que tienen como finalidad implementar un sistema de gestión de calidad dentro de una organización, aumentar la productividad, reducir los costos innecesarios y garantizar la calidad de los procesos y productos.

Acorde a lo señalado por la Norma ISO 9000, el enfoque de la metodología basada en procesos permite gestionar un conjunto de actividades mutuamente relacionadas o que interactúan entre sí, las cuales transforman elementos de entradas en resultados [42]. Estos procesos deben tener una misión y objetivos claros dentro del sistema de gestión, al mismo tiempo que tienen que ser medibles para analizar su cumplimiento, contar con los recursos necesarios para su funcionamiento y un responsable que garantizará el control y el buen funcionamiento del mismo.

Por otro lado, según la Norma ISO 9001, un mapa de procesos se encuentra compuesto principalmente de tres tipos de procesos que siguen una determinada secuencia lógica [43]:

- Procesos operativos; están ligados directamente con la realización del producto o la prestación del servicio. Por tal motivo, tendrán un mayor impacto en la eficiencia y mejora continua del sistema de gestión, como así también los resultados obtenidos.
- Procesos estratégicos; se encuentran vinculados a procesos de la dirección y son principalmente a largo plazo. Guardan estrecha relación con procesos de planificación.
- Procesos de apoyo; estos proveen recursos que son necesarios para llevar a cabo los demás procesos. Se encuentran relacionados con los recursos y logística.

Hablar de la norma ISO 9001 2015, es hablar de la gestión por procesos, esto rompe el esquema departamental que suele haber en las organizaciones, centrando la gestión en las actividades y no en qué departamento las ejecuta. Esto provoca que el organigrama pase a ser una herramienta estructural, pero no operativa, lo que supone un cambio importante de paradigma. Lo habitual será tener procesos en los que intervengan distintos departamentos de manera transversal, y los intervinientes asuman un determinado rol en cada uno de ellos.

En tal sentido, el mapa de procesos consiste en la forma de proporcionar una vista de alto nivel de los procesos que componen un sistema de gestión y mostrar cómo estos interactúan entre sí. Cada organización debe determinar los procesos necesarios para el sistema de gestión de la calidad y su aplicación, debiendo determinar la secuencia e interacción de los mismos [43].

2.2.3 Integración del modelo de madurez de capacidades (IMMC)

El IMMC es un marco de trabajo que permite evaluar o valorar el estado de madurez de una organización dentro de un esquema definido, permitiendo identificar claramente cuándo un esquema organizacional es ad-hoc y desorganizado en comparación con un programa altamente estructurado y repetible.

Esta metodología fue desarrollada originalmente por el *Software Engineering Institute*[24], una cohorte de grupos gubernamentales y expertos de la industria, que en sus orígenes fue diseñado para ser aplicado en el campo de la ingeniería de software, pero que luego se generalizó rápidamente migrando hacia otras áreas de evaluación de capacidades.

En enero de 2013, se formó el Instituto IMMC en el seno de la Universidad Carnegie Mellon para continuar la investigación y difusión del marco de trabajo. Cabe destacar que se debe tener en cuenta que este marco de trabajo no es un estándar y como tal no proporciona información detallada sobre el logro de los objetivos que se están midiendo.

Originalmente el marco estaba diseñado para servir como una guía para comprender las implementaciones actuales y los mecanismos alternativos para implementar los niveles de madurez mediante un esquema claro y sencillo de comprender.

2.2.3.1 Niveles del IMMC

El marco de trabajo propone una metodología de evaluación estadística para que la gestión organizacional clasifique y comprenda cómo mejorar sus procesos mediante una evaluación integral.

En tal sentido, en función de los resultados obtenidos el IMMC debe brindar una cierta orientación sobre las acciones que se pueden realizar para mejorar los procedimientos evaluados en lugar de enumerar explícitamente los pasos para lograr el siguiente nivel de madurez.

Conforme lo expresado, puede inferirse que a medida que aumenta la capacidad de la organización, los resultados producidos se alinearán mejor con las expectativas y la precisión. Del mismo modo, a medida que mejoran los resultados del IMMC, una organización debería experimentar una disminución de costos, tiempo de desarrollo, acompañado de mayor productividad y calidad.

Para identificar el grado de madurez de una organización, este marco de trabajo define los siguientes niveles:

[24] Instituto federal estadounidense de investigación y desarrollo, entidad financiada por el Departamento de Defensa de los Estados Unidos y administrado por la Universidad Carnegie Mellon.

- Nivel 0: Incompleto. Los procesos no se ejecutan o se ejecutan incorrectamente. No existen objetivos y ni estándares claramente definidos.
- Nivel 1: Realizado. Los procesos son caóticos y ad hoc. En este nivel, una organización no podría esperar un resultado estable ni de calidad, sus actividades productivas se encuentran emparejadas con la experiencia de la persona o equipo involucrado.
- Nivel 2: Gestionado. Se ha proporcionado visibilidad para que la gerencia comprenda el estado de los procesos y existen controles establecidos, esperándose que los servicios sigan los planes del proyecto que cumplen con los estándares y requisitos planteados.
- Nivel 3: Definido. Los procesos se entienden, documentan, siguen y son coherentes con claridad. Los procesos maduros definidos se mejoran mediante los atributos de mayor detalle, existen controles de calidad proactivos, una comprensión más profunda de las relaciones y métricas detalladas.
- Nivel 4: Optimizado. Los procesos se mejoran continuamente a través de la innovación tecnológica. Las mejoras se miden y evalúan mediante métricas y marcadores. La capacidad de la organización para impartir cambios rápidamente como oportunidades es el resultado de un ciclo de mejora constante del proceso. Sus procesos están en una madurez de nivel muy superior debido al análisis de variaciones y previsibilidad.

Cabe destacar que los niveles de madurez de IMMC no se pueden omitir ni pasar por alto, a medida que el grado de madurez se incrementa, estos niveles se sustentan en el éxito de los niveles inferiores.

Podría decirse que cada grado de madurez es el fruto de la evolución natural de una organización, sin embargo, una organización con un nivel de madurez inferior puede intentar realizar procesos de un nivel superior, aun pese a que existe un alto riesgo de inconsistencia.

En general el IMMC se presenta como un marco de trabajo sencillo que se puede modificar para adaptarse a la mayoría de situaciones y, en el caso de esta

investigación, se puede utilizar para mostrar los niveles de madurez de un laboratorio de análisis forense digital.

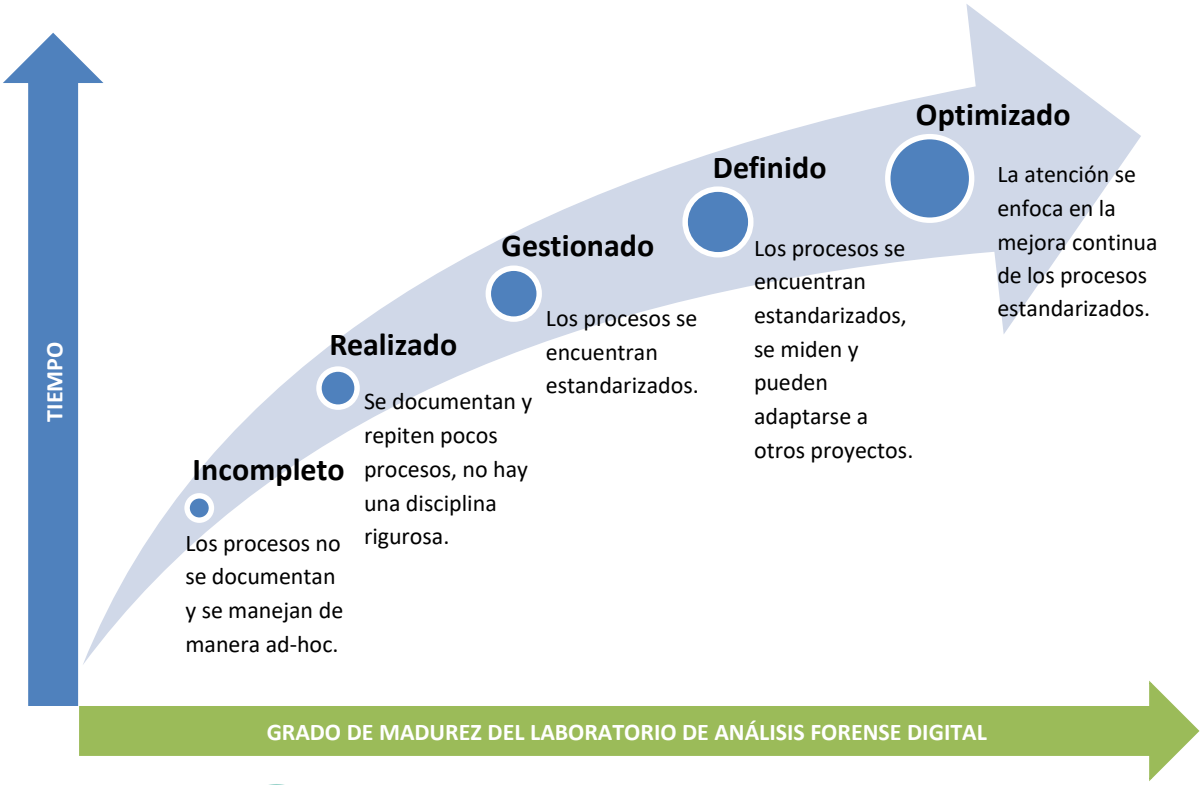

Ilustración 5: Niveles del marco IMMC.

2.2.3.2 Indicadores de desempeño, mejora de procesos y madurez

Medir el desempeño de un laboratorio de análisis forense digital puede llegar a ser un proceso cargado de subjetividad, quizás incluso puede encontrarse basado en experiencias previas y acotadas, cuyas mediciones de desempeño e indicadores tienden a enfocarse en elementos tales como:

- Conformidad con los objetivos de nivel de servicio establecidos.
- La cantidad de casos gestionados o dispositivos recibidos/analizados.
- El volumen de datos procesados durante un período determinado.

Estas nociones pueden ser catalogadas como “falsos” indicadores de rendimiento, los cuales en el peor de los casos se promocionan como indicadores del rendimiento de un laboratorio y se adoptan como criterios para lograr mejoras y eficiencia, situación que en el corto o mediano plazo cae por su propio peso, ocasionando dispendio innecesario de recursos y tiempo.

Las mejoras en los procesos pueden lograrse efectivamente mediante el diseño de métodos aceptados para medir los procesos, productos y resultados, como piezas fundamentales para cualquier estrategia de mejora. Lograr la eficiencia a través de la mejora del desempeño consiste en llevar adelante un proceso de evaluación integral sobre un proceso o conjunto de procesos específicamente seleccionados, para luego identificar posibles correcciones para lograr una mayor eficiencia, calidad o resultados.

Por tal motivo, es menester señalar que la medición del desempeño consiste en cuantificar la eficiencia y eficacia de acciones pasadas, definición que contrasta absolutamente con una acepción vinculada con el proceso de evaluar qué tan bien se administran las organizaciones y el valor que brindan a los clientes y otras partes interesadas.

Para finalizar, un proceso de mejora definido acorde los términos del marco IMMC [44], tiene cinco elementos básicos:

- Comprensión del estado actual de la organización y sus procesos.
- Una visión del/los proceso/s que se desea/n mejorar.
- Una lista priorizada de acciones de mejora necesarias.
- Elaborar una planificación para materializar estas acciones.
- Recursos y compromiso para ejecutar la planificación diagramada.

2.2.3.3 Una crítica al marco IMMC

Los modelos de madurez se han convertido en herramientas populares que se utilizan para una variedad de tareas, como calificar las capacidades de un proceso de fabricación e identificar elementos que ayuden a aumentar el nivel general de madurez de ese proceso o evaluar la situación de una organización.

El término madurez es utilizado ampliamente y se refiere al grado de formalidad y optimización de los procesos, ahora sobre los métodos utilizados para crear los modelos podría decirse que estos se basan simple y llanamente en sus predecesores, a menudo bien conocidos, sin un aporte crítico sobre qué tan apropiados podrían llegar a ser estos supuestos que forman la base de los modelos.

El IMMC es esencialmente un marco de trabajo que permite guiar a una organización en el proceso evolutivo que la llevará de la carencia de madurez de procesos y vulnerabilidad ante serios problemas de eficiencia hacia una entidad bien estructurada, madura y eficiente.

En resumen, el uso de este modelo es un medio para que las organizaciones sometan sus prácticas a un sistema científico de control y evaluación de procesos con el fin de ayudar a calificar y posiblemente mejorar su eficiencia general.

La función del IMMC consistirá entonces en identificar y documentar el ordenamiento lógico de tareas que deben realizarse para definir, administrar, monitorear y mejorar los procesos de la organización en lugar de indicar exactamente cómo se deben realizar las actividades específicas.

3
Resultados

La estandarización de cualquier laboratorio técnico, incluidos los de análisis forense digital, no solo tiene que ver con su credibilidad, sino también con otros aspectos como la mejora continua y calidad de sus servicios. En este sentido, el conjunto de normas ISO 9001 e ISO/IEC 17025, permiten identificar y abordar riesgos y oportunidades a través de la planificación y la implementación de un sistema de gestión basado en procesos.

Si tomamos como punto de partida el contexto que enmarca las actividades vinculadas al análisis forense digital, podremos apreciar que los riesgos y oportunidades provienen de una tasa de cambio casi constante, variaciones en los conjuntos de habilidades y experiencia de los examinadores forenses, como así también los recursos propios de un laboratorio de estas características.

Estas variaciones pueden significar que diferentes laboratorios realicen sus actividades basadas en métodos no formalizados y en el peor de los casos podría llegar a suceder que los resultados no fueran realmente reproducibles. Esta circunstancia no solo afectaría la credibilidad de este laboratorio y sus examinadores forenses, sino también de la profesión en su conjunto.

En este sentido, si bien la norma ISO/IEC 17025:2017 especifica los requisitos de competencia para los laboratorios en general, incluyendo premisas como imparcialidad y coherencia, resulta cuestionable que esta norma cubra íntegramente con todos los aspectos que la ciencia forense digital necesita, no solo por la rapidez con que evoluciona el análisis forense digital sino también por las múltiples posibilidades que presentan los casos de estudio.

Por otro lado, la gestión de calidad de los laboratorios de análisis forense digital podría reposar sobre un modelo diagramado en función del conjunto de normas ISO 9001, haciendo foco en la gestión de procesos como camino hacia la mejora continua.

Por tal motivo, esta investigación propone la integración del modelo de madurez capacidades a los laboratorios de análisis forense digital, como mecanismo de evaluación integral y abordaje de los tres dominios organizacionales clave: Personas, Procesos y Herramientas tecnológicas.

Ilustración 6: Dominios clave del IMMC.

Estas tareas no podrían haberse llevado a cabo sin haber realizado previamente una revisión de diferentes reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de informática forense y evidencia digital, cuyo estudio fue cubierto ampliamente en el Trabajo Final de Especialización que sirvió de punto de partida para establecer los lineamientos generales de esta investigación.

Dados los pormenores de la complejidad del escenario planteado y los múltiples obstáculos que presenta la estandarización de un laboratorio de análisis forense digital, se desprende la imperiosa necesidad de contar con un sistema de gestión solidario con sólidos lineamientos como las reglas de buena práctica forense, garantizando en todo momento un proceso reproducible de identificación, preservación, análisis y presentación de la evidencia digital, para afianzar su valor probatorio.

En el presente capítulo se expondrán los resultados obtenidos a partir del análisis practicado sobre la base de la propuesta metodológica planteada, en función de las fases que componen el análisis forense digital y otros aspectos de relevancia, para luego esbozar los procesos vinculados con la implementación de un Sistema de Gestión de Evidencia Digital y la integración del modelo de madurez de capacidades aplicado a este campo de las ciencias forenses.

3.1 Personas: Identificación de roles y competencias requeridas

Cabe destacar que, a cada etapa del modelo simplificado de análisis forense presentado, le corresponden determinadas tareas y/o actividades específicas, las que deben ser ejecutadas por especialistas, cuyos roles requieren una formación particular y diferentes grados de especificidad.

Valga la redundancia, resulta oportuno enfatizar que tales roles y grado de capacidad técnica hacen al perfil profesional del especialista en informática forense, cualidades que se encuentran relacionadas de forma directamente proporcional con aquellas diligencias que deben materializarse.

Por tal motivo, se identificaron los roles, actividades y competencias requeridas correspondientes al investigador, primer interviniente en manejo de evidencia digital y especialista en análisis de evidencia digital, como piezas claves que de forma conjunta interactúan en torno al análisis forense digital.

Ilustración 7: Roles y responsabilidades.

3.1.1 El investigador [25]

Es la persona encargada de planificar y organizar todo el proceso de investigación digital, coordinando diferentes actividades a desarrollarse. Por lo general, este rol puede ser desempeñado por un individuo designado por la organización involucrada o autoridad judicial competente, a fin de velar por el cumplimiento de aquellos objetivos planteados para el desarrollo de la investigación.

3.1.2 El primer interviniente en manejo de evidencia digital [26]

Es la persona involucrada en la identificación, recolección y preservación de la evidencia digital en la escena del incidente. Este rol corresponde a profesionales que poseen amplia experiencia, habilidad y conocimientos en el manejo de evidencia digital, lo que será crucial para su preservación en virtud de la fragilidad que presenta.

3.1.3 El especialista en análisis de evidencia digital [27]

Es la persona que lleva adelante el análisis y procesamiento de las evidencias digitales recolectadas, para luego elaborar el informe pericial correspondiente. Este rol corresponde a profesionales que poseen experiencia, conocimientos y habilidades con alto grado de especificidad en el análisis de evidencia digital, además pueden ejecutar aquellas actividades correspondientes a los primeros intervinientes.

3.2 Procesos: Gestión de calidad

Según los requisitos estipulados en la Norma ISO 9001, para el presente proyecto se delinearon diferentes procesos que permitirán la implementación de un Sistema de Gestión de Evidencia Digital, acorde al manual y política de calidad correspondientes.

Cabe destacar que el manual de calidad tiene como finalidad describir el alcance del Sistema de Gestión de Evidencia Digital, como así también señalar

[25] Ver Anexo “Tabla 7: Roles y responsabilidades - Investigador”.
[26] Ver Anexo “Tabla 8: Roles y responsabilidades - Primer interviniente”.
[27] Ver Anexo “Tabla 8: Roles y responsabilidades – Especialista en análisis de evidencia digital”.

aquellos procesos necesarios para su funcionamiento, demostrando su capacidad para proporcionar informes, satisfacer los requisitos y reglamentarios que debe cumplimentar la organización, incluyendo procesos de mejora continua y la gestión de No Conformidades.

Del mismo modo, la política de calidad establece una serie de compromisos asumidos por la organización, con la finalidad de garantizar el cumplimiento de todos los requisitos necesarios, legales, reglamentarios y aquellos adicionales vinculados en materia de calidad de los servicios forenses prestados.

3.2.1 Procesos estratégicos.

3.2.1.1 Objetivos y planificación del sistema de gestión.

Todo sistema de gestión debe asegurar el correcto desarrollo de aquellas actividades necesarias para la adecuada incorporación de los cambios que afecten al Sistema de Gestión de la Calidad, de manera que se mantenga el estándar ante ciertas modificaciones que puedan afectar a la producción o prestación de los servicios, dado que los mismos no son estáticos, sino que presentan distintos escenarios con el paso del tiempo.

En ese sentido, los objetivos y planificación del sistema de gestión permitirán describir aquellas actividades necesarias para asegurar la calidad en la prestación de los servicios forenses ante eventuales cambios, de manera que los mismos se apliquen de manera controlada y efectiva.

Respecto de los objetivos de calidad, estos deben ser medibles y coherentes con la política de calidad, mientras que la planificación del sistema de gestión actuará como un permanente garante del Sistema de Gestión de la Calidad, manteniendo en todo momento su integridad y asegurando el cumplimiento de los objetivos de la calidad, tomando como información de entrada futuros cambios en la organización, su estrategia de negocios, infraestructura y recursos humanos.

3.2.1.2 Responsabilidad y revisión por la Dirección.

Este procedimiento tiene como finalidad establecer cómo se deben realizar las revisiones del Sistema de Gestión de la Calidad para asegurar su eficaz y eficiente implementación.

A tal efecto se define un Comité y Responsable de Calidad para la gestión de la calidad, como encargados de promover, supervisar y coordinar el desarrollo de normas, procedimientos y medidas organizacionales que velen por la integridad de la información, la continuidad de servicios, la protección de los activos de información y la asignación de responsabilidades para el cumplimiento de las mismas.

La organización se encargará además de establecer un Comité de Calidad del que formarán parte los miembros de las diferentes áreas de la organización, representantes de la alta dirección y especialistas en materia de gestión de calidad, entre sus funciones generales se encuentran:

- Revisión y aprobación de la Política de Calidad y Responsabilidades Generales.
- Comunicar a la organización la importancia de satisfacer tanto los requisitos del cliente como los legales y reglamentarios
- Definir y evaluar las métricas de Calidad
- Definir las necesidades de asesoramiento por parte de especialistas externos en materia de Calidad.
- Control y Revisión de los objetivos de Calidad y de los cambios que afecten al SGC.
- Aseguramiento de la disponibilidad de recursos.
- Asegurar que se determinan los requisitos del usuario y se cumplen con los propósitos de la satisfacción del mismo.
- Establecer los procesos de comunicación apropiados dentro de la organización y que la misma se efectúa considerando la eficacia del SGC.

Por otro lado, el responsable de calidad tendrá las siguientes responsabilidades y autoridad para hacer cumplir las mismas en el ámbito de la gestión de la calidad:

- Garantizar que se implementan y mantienen los procesos necesarios para el correcto funcionamiento del SGC.
- Informar al Comité de Calidad sobre el desempeño del SGC y cualquier desvío o necesidad de mejora respecto al mismo.
- Asegurar la toma de conciencia respecto a calidad en todos los niveles organizativos.

3.2.1.3 Medición, seguimiento y análisis.

Todo sistema de gestión vinculado con un proceso de mejora continua requiere de una serie de elementos de medida que permitan determinar objetivamente el cumplimiento, mejora o necesidades del mismo comparándose con objetivos declarados con anterioridad por la organización.

Por lo tanto, también es necesario definir el modo en que se medirán estos controles o grupos de controles, como así también especificar los aspectos que se tomarán, medirán y utilizarán para evaluar la eficacia de los controles generando resultados claramente comparables y reproducibles.

Del mismo modo, resulta oportuno señalar que se entiende por Indicador de Calidad a toda aquella herramienta objetiva y cuantificable que permite efectuar el seguimiento de un parámetro a lo largo del tiempo, debiéndose definir los siguientes conceptos:

- Indicador: Nombre del indicador.
- Propietario: Persona responsable del indicador.
- Periodicidad: Periodicidad con la que se mide el indicador.
- Método de Cálculo: Explicación de los datos que componen la fórmula a emplear.
- Valor de Referencia: Fin cuantificado que se pretende conseguir.

3.2.1.4 Auditorías internas.

Auditar consiste principalmente en estudiar los niveles de cumplimiento del sistema de gestión de la organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias establecidos.

A partir de esta definición, el disponer de un procedimiento para llevar a cabo las auditorías internas de una organización supone un mecanismo para obtener una correcta planificación de actividades y recursos para realizar los procedimientos intrínsecos del propio proceso de auditoría, facilitando su desarrollo y minimizando el impacto en los demás procesos durante el transcurso de la misma.

Asimismo, este procedimiento establecerá la protección necesaria y adecuada sobre la documentación generada y las herramientas de auditoría empleadas en el sistema de gestión de calidad con el fin de limitar su acceso y garantizar su confidencialidad.

Respecto a su periodicidad, las auditorías internas del Sistema de Gestión de la Calidad se llevarán a cabo de forma anual, de acuerdo con un programa preestablecido, sin embargo, podrán efectuarse auditorías internas fuera del programa en casos excepcionales como, por ejemplo:

- Cuando se produzcan cambios importantes en la estructura de la organización que puedan afectar al Sistema de Gestión de la Calidad establecido.
- Cuando exista sospecha de que no se cumplen los requisitos de calidad establecidos, o se haya materializado una incidencia o no conformidad grave que no había sido prevista.
- Cuando se produzcan cambios en el propio Sistema de Gestión de la Calidad.

3.2.1.5 Gestión de no conformidades.

En primer lugar, resulta oportuno indicar que como “No Conformidad” se entiende a todo incumplimiento de un requisito del sistema, ya sea una necesidad o expectativa establecida, generalmente explícita u obligatoria.

Todo personal sujeto al sistema de gestión podrá identificar posibles no conformidades y/o debilidades, ya sea cuando las mismas son efectivas (es decir el evento que causa la no conformidad se ha materializado) o bien cuando se sospecha que existe una situación de riesgo que pudiera generar una No Conformidad en el futuro debido a la existencia de una vulnerabilidad latente.

En tal sentido, la gestión de no conformidades permitirá detectarlas y corregirlas, así como también realizar su tratamiento para ejecutar aquellas acciones preventivas y de mejora continua, definiendo el proceso, responsabilidades y plazos para su corrección.

Entre las no conformidades, a modo de ejemplo pueden señalarse:

- Alteraciones en el funcionamiento o rendimiento normal de los departamentos que componen la organización.
- Fallos en la ejecución de los procesos de calidad.
- Incumplimiento de las directrices establecidas en la política de calidad o cualquiera de sus normas o procedimientos.
- Productos no Conformes (P. Ej un Informe que no cumple con los requisitos)
- Quejas y reclamos de los Clientes/Usuarios.

3.2.1.6 Mejora continua.

Este procedimiento tiene como finalidad establecer aquellos sistemas que permitan la puesta en marcha de acciones correctivas o preventivas y la actualización de la documentación pertinente, que traten de forma adecuada las causas de las no conformidades detectadas o potenciales con objeto de evitar que éstas se repitan o produzcan.

Entre las acciones señaladas se pueden indicar:

- Acción inmediata o reparadora: es aquella que se adopta para solucionar un problema puntual que probablemente no se producirá de forma repetitiva.
- Acción correctiva: se adopta tras el estudio en detalle de una no conformidad, ya sea por su gravedad, porque se produce o bien podría

producirse de forma repetitiva, con el fin de buscar y erradicar la causa que la origina.

- Acción preventiva: son acciones adoptadas con el fin de evitar en el futuro posibles no conformidades que aún no se han materializado, anticipándose a situaciones que aún no se manifestaron, aunque son potenciales.

3.2.2 Procesos operativos.

3.2.2.1 Recolección, preservación y adquisición.

La recolección y adquisición de evidencias digitales puede darse en un número muy disperso de escenarios siendo muy importante lograr un balance entre la calidad de la evidencia recolectada, el tiempo de recolección empleado y el costo asociado al mismo.

Además, el proceso de priorización debe considerar el material y personal disponible para la recolección, adquisición y conservación de la evidencia digital, así como el orden de recopilación de la evidencia minimizando el riesgo de repudio en fases posteriores.

En tal sentido, durante este procedimiento se deberá tener especial atención en diferentes aspectos operativos, a saber:

- Principios fundamentales: deberá cumplir con los principios de relevancia, confianza y suficiencia, garantizando su pertinencia, repetitividad y completitud.
- Recolección: consiste en el apropiado manejo de los dispositivos que potencialmente contienen evidencias digitales, desde que son recogidos hasta su trasladado a un laboratorio u otro entorno controlado para la adquisición y preservación.
- Preservación y traslado: la actividad más importante radica en garantizar la conservación de las evidencias digitales, manteniendo su integridad y autenticidad, así como su correcta cadena de custodia.
- Cadena de custodia: la trazabilidad de las evidencias digitales debe encontrarse disponible en cualquier momento de la investigación, aportando un riguroso registro vinculado con su tratamiento y custodia.

- Evaluación de riesgos: todo el proceso de adquisición y recolección de la evidencia digital se encuentra expuesto a ciertos riesgos que podrían comprometer las evidencias obtenidas, el investigador deberá realizar una evaluación sistemática de los riesgos y su potencial impacto en la investigación.
- Adquisición: el método empleado debe producir una copia exacta de aquellos registros o dispositivos electrónicos que pudieran ser considerados como evidencias digitales, debiendo contemplarse la verificación de las copias realizadas mediante conjuntos de funciones hash.
- Competencia del personal: todo el personal implicado en la recolección, adquisición y preservación de la evidencia digital debe tener competencias técnicas que serán debidamente acreditadas.
- Calibración de los equipos: para garantizar la exactitud y evitar el repudio de las evidencias adquiridas, deberán validarse o calibrarse las herramientas empleadas periódicamente.

3.2.2.2 Análisis forense.

El análisis forense digital pretende investigar lo ocurrido durante un determinado momento o intervalo de tiempo, que puede encontrase asociado con un incidente de seguridad, una intrusión, una práctica delictiva o un evento de características similares.

Este proceso busca dar respuesta a ciertos interrogantes que envuelven a toda investigación: quién realizó las acciones, qué activos se vieron afectados y en qué grado, cuándo tuvo lugar, dónde se originó, cómo fue llevado a cabo y de ser posible por qué.

La evidencia recolectada debe ser analizada para extraer la información relevante e identificar una serie de eventos vinculados con los hechos investigados, por tal motivo se establecen una serie de exigencias de calidad siguiendo los siguientes requisitos:

- Organización interna: en primer lugar, se verificará que se dispone de los oficios, requerimientos judiciales o de terceros que habiliten a la organización para llevar a cabo las tareas de análisis forense.

- Identificación del proyecto: el mismo será identificado unívocamente con datos como por ejemplo una codificación interna, denominación del solicitante, tipo de estudio practicado, fecha de inicio y personal encargado del mismo.
- Planificación de actividades: analizar las evidencias digitales dependerá del tipo de fuente de datos (computadoras, teléfonos celulares, circuitos cerrados de televisión, drones, etc.). Antes de iniciar el análisis debe comprobarse la integridad de la evidencia y su cadena de custodia, verificando que la misma es confiable.
- Asignación de personal: el jefe de proyecto asignará un equipo acorde las actividades que deberán desarrollarse, como así también los conocimientos y disponibilidad del personal disponible.
- Tareas vinculadas con el análisis forense: las actividades de investigación forense deberán realizarse sobre las copias obtenidas. Estas copias evitarán que las acciones realizadas puedan alterar los datos originales (ya sea del propio dispositivo recogido o bien de la evidencia adquirida).
- Redacción del informe: los principales lectores de estos informes son jueces, directivos de empresas u organismos, entre otros.; es decir que son personas que no tienen perfil técnico. Por tal motivo, el lenguaje del informe no debe ser excesivamente técnico y, en el caso que deban emplearse estos términos, deberá procurarse una explicación de forma clara.
- Contenido de los informes: este tipo de documentos deberá contar con apartados donde se definan claramente las partes interesadas, los elementos analizados, el objetivo de la investigación, los estudios practicados, resultados obtenidos y conclusiones arribadas.
- Verificación y aseguramiento de la calidad: se ejecutarán aquellos controles especificados durante la planificación, para comprobar que el análisis forense ha cumplido satisfactoriamente con la misma y evaluar aquellos acontecimientos que pudieran haber surgido durante su desarrollo.

3.2.2.3 Recuperación de datos.

Los servicios de recuperación de datos pueden ser requeridos cuando no se puede acceder a toda o parte de la información contenida en un medio de almacenamiento y el acceso a estos datos resulta necesario para la investigación.

Las actividades para la recuperación de datos serán diversas y dependerán en gran medida del factor que causó la pérdida de la información contenida en los medios de almacenamiento. De este modo, una pérdida de información por motivos lógicos podrá requerir únicamente de la aplicación de procesos software tales como reparación del índice del volumen de ficheros, mientras que una pérdida de datos por motivos físicos podrá requerir de la apertura del medio de almacenamiento y la utilización de medios físicos tales como el desmontaje de los platos, sustitución de cabezales, etc.

El escenario más frecuente de pérdida de datos se debe a un fallo en la gestión de datos por el sistema operativo o bien que los datos han sido eliminados por los canales habituales. En este caso la información propiamente dicha se encuentra en el sistema de almacenamiento, pero se ha eliminado o dañado el índice que establece la ubicación de los datos en el volumen. Por tanto, en estos casos, la información podrá recuperarse en un alto porcentaje de manera completa siempre y cuando no haya sido sobre escrita posteriormente a la eliminación.

El segundo escenario contempla la pérdida de información debido a un daño físico en los medios de almacenamiento, por lo tanto, la recuperación de datos requerirá de una primera acción de reparación física del dispositivo para posteriormente analizar la información contenida que no ha sido dañada. Típicamente en este escenario existe la posibilidad de no poder recuperar todos los datos dado que la cantidad de datos que puedan recuperarse dependerán en gran medida de la afectación que haya sufrido el dispositivo de almacenamiento.

Por último, cabe la posibilidad de que la información haya sido ocultada bien mediante técnicas de estenografía o cifrado. En estos casos el trabajo requerirá de un análisis detallado para detectar posible información oculta mediante técnicas de estegoanálisis o criptoanálisis. Dada la complejidad, existe una alta posibilidad de no poder recuperar la información.

Durante el desarrollo del proceso de recuperación de datos, deberán documentarse detalladamente todas las acciones que se realicen de modo que pueda reproducirse los resultados obtenidos en caso de ser necesario.

3.2.2.4 Asesoría.

En aquellas oportunidades donde se requiere realizar labores de asesoramiento y consultoría para diferentes organismos, no se tiene en cuenta la inversión de recursos que significa para la organización, por tal motivo resulta necesario establecer un procedimiento que permita valorar y documentar este tipo de servicios, sobre la base de las siguientes actividades:

- Entrevistas con el solicitante: deberán documentarse mediante una constancia de reunión, que será archivada junto a la documentación de proyecto. Pueden incorporarse otros elementos como contenido multimedia (grabación en audio/video de la entrevista), con el previo consentimiento del entrevistado, garantizándose además la confidencialidad de las actas o grabaciones realizadas.
- Informe de asesoría: Como resultado de la ejecución del proceso, se generará un reporte de resultados de acuerdo a los requisitos establecidos para la generación de informes, agregando además un detalle de las recomendaciones efectuadas por la organización para llevar adelante el proyecto de análisis forense.
- Visto bueno del solicitante: en caso de avanzar con el proyecto de análisis forense, se requerirán los oficios, requerimientos judiciales o de terceros que habiliten a la organización para llevar a cabo las tareas pautadas.

3.2.3 Procesos de apoyo.

3.2.3.1 Control de documentos y clasificación.

El objetivo de este procedimiento es describir la metodología utilizada en la organización para realizar el control de todos los documentos y datos del sistema de gestión, ya sean de origen interno como externo, incluyendo su aprobación, revisión y actualización, así como identificar, recoger, codificar, mantener al día, proteger y brindar un destino final a los registros de calidad.

Acorde los requisitos y necesidades de documentación, resulta posible recomendar una serie de documentos que definen al sistema de gestión de calidad de la organización, entre los que se encuentran:

- El manual de calidad: Es el documento básico que describe los distintos elementos del sistema de gestión de calidad de la organización, no constituye un fin en sí mismo, sino una herramienta necesaria que sirve como referencia permanente durante la implementación y aplicación de dicho sistema.
- Procedimientos de Operativos: los distintos métodos y medidas adoptadas por la organización en su Manual de Calidad son desarrollados en procedimientos, estos pueden ser de carácter general, aplicables a todas las actividades sujetas al sistema de gestión o específicos, es decir aquellos necesarios para desarrollar las funciones propias de cada área.
- Procesos: estos documentos son aquellos que reflejan los procesos planificados y desarrollados que son necesarios para la realización del producto o prestación de los servicios objeto del sistema de gestión de calidad.
- Procedimientos de Trabajo: constituyen un documento específico que define cómo se ejecuta un proceso. Este documento describe con suficiente detalle cada una de las actividades para la realización de un proceso o parte del mismo siendo por tanto más dependiente de la tecnología, herramientas y recursos empleados.
- Formatos, Fichas y Registros: son aquellos documentos que proporcionan la información necesaria para asegurarnos del funcionamiento del sistema de calidad implementado. Estos registros permiten la reproducibilidad y la comprobación de los resultados, así como el análisis de los datos registrados con el fin de una mejora continua.

Del mismo modo, la organización deberá brindar un repositorio para garantizar la disponibilidad de los documentos del sistema de gestión, como así también establecerá una codificación que permita su correcta individualización mediante una nomenclatura claramente identificable.

3.2.3.2 Gestión de recursos.

La gestión de recursos humanos constituye un punto fundamental y en consecuencia así deberá ser considerado por la organización, asegurándose que el personal sea consciente de la pertinencia e importancia de sus actividades y como las mismas contribuyen al logro de los objetivos de la calidad.

El proceso de incorporación de personal se puede dividir en varias fases claramente diferenciadas:

- Proceso de Selección de Personal: el mismo deberá ser realizado siguiendo la política de contratación establecida por la dirección de la entidad para cumplir con las buenas prácticas de selección y contratación, según la legislación vigente. La selección y verificación de candidatos será acorde al perfil descrita en las ofertas de trabajo pertinentes, asegurando la competencia necesaria para cumplir con las actividades y tareas del puesto.
- Contratación: tiene por objeto garantizar que los empleados y usuarios de terceros vinculados con la organización sean informados previo al comienzo de la relación contractual y que estos comprendan sus obligaciones y responsabilidades en relación con la gestión de la calidad relacionados con las tareas que vayan a desempeñar, así como verificar que son aptos para los roles que les fueron asignados.
- Formación: para mantener un nivel adecuado de concienciación y formación de los usuarios, de manera que contribuyan al logro de la calidad, se procurará organizar periódicamente formación sobre la gestión de la calidad y las competencias necesarias para el desempeño de cada puesto de trabajo.
- Cese o cambio de puesto de trabajo: Los empleados, contratistas y terceros que abandonen la organización o cambien de puesto de trabajo deberán asumir las responsabilidades pertinentes asociadas a cualquier acuerdo de confidencialidad, así como términos y condiciones del empleo.
- Devolución de activos: al término de la relación contractual el empleado devolverá todos los activos que tenga en posesión incluyendo, pero no restringiéndose a computadoras personales, teléfonos móviles, dispositivos

de almacenamiento, información almacenada en medios propios, llaves y/o tarjetas de acceso, licencias de software, documentos corporativos, tarjetas de crédito, etc.

- Derechos de acceso: el cese o cambio de puesto de trabajo de un empleado, contratista o tercero, va asociado con la retirada de los derechos de acceso en caso de ser cese y a su actualización en caso de cambio de puesto de trabajo en los sistemas de información de la organización. Todo cese de empleado será notificado por el responsable del área correspondiente al administrador de sistemas para que proceda a la baja de los derechos de acceso lógico entre los que se comprende acceso al dominio, servicios de red, cuentas de correo electrónico y acceso remoto, entre otros.

3.2.3.3 Formación/Entrenamiento.

Este proceso tiene como finalidad establecer un sistema que permita detectar y planificar las necesidades de formación del personal y regular las distintas actividades formativas de manera que los empleados tengan en todo momento la capacidad de responder de la forma más adecuada a las necesidades del cliente.

Asimismo, incluye el realizar el seguimiento de la cualificación y formación en materia de análisis forense digital de la organización, así como la evaluación de la eficacia de las acciones formativas realizadas, a tal efecto se deberán tener en cuenta los siguientes requisitos:

- Detección de las necesidades de formación: las necesidades de formación del personal de la organización sobre cualquier tipo de materia relacionada con el análisis forense digital y temas afines pueden ser detectadas por los propios empleados, el responsable de calidad, la coordinación u otras partes interesadas cuando resulte pertinente.
- Evaluación de las necesidades: la decisión sobre la formación a impartir será responsabilidad última del Comité de Calidad, que considerará su pertinencia respecto a los resultados de mejora de calidad esperados.
- Planificación de la Formación: Una vez evaluada la necesidad y siendo

esta aprobada, el Comité de Calidad planificará la formación, ya sea interna o externa, gratuita o no, indicando el contenido de la misma, responsable de impartirla, público al que se dirige, modalidad y fecha prevista, entre otros aspectos.

- Registro de las acciones formativas: toda formación profesional deberá ser registrada, cuyos diplomas de asistencia o aprobación serán documentados por el área correspondiente junto al legajo personal de cada empleado para su archivo.
- Registro de la educación, formación, habilidades y experiencia de los empleados: el área de recursos humanos mantendrá actualizado el legajo personal de cada empleado, consignando información sobre el puesto que ocupa, experiencia profesional y conocimientos anteriores a su incorporación, como así también de aquella formación recibida a partir de su incorporación a la organización.
- Revisión de la eficacia del plan de formación: su eficacia será evaluada en función de si las necesidades han sido cubiertas o no, como así también si existe una mejora medible acorde los objetivos planteados por la organización.

3.2.3.4 Infraestructura, equipos y ambiente de trabajo.

El objeto del presente procedimiento es garantizar que la organización proporciona y mantiene la infraestructura, el equipamiento y el ambiente de trabajo necesarios para lograr la conformidad con los requisitos de calidad de sus servicios. A tal efecto se deben tener presentes los siguientes aspectos:

- Identificación de la infraestructura y el equipamiento: la infraestructura necesaria para la correcta prestación de los servicios de la organización comprende tanto a los edificios y espacios de trabajo, como al equipamiento informático ya sea de hardware y software,) como así también los servicios de apoyo tales como la red de comunicación y sistemas de información.
- Controles de seguridad física: debido al tipo de servicios prestados, la organización deberá garantizar la seguridad física de sus ubicaciones de

trabajo mediante vigilantes en el perímetro del edificio o video vigilancia, procedimiento de control de visitas y/o registro de accesos, sistemas de alarma y detección de intrusos, zonas de acceso restringido bajo llave o acceso biométrico y otros controles de seguridad física similares.

- Evaluación e idoneidad de los equipos informáticos y software: cuando se requieran equipos informáticos, hardware dedicado o software para la ejecución de los procesos que dan soporte a los servicios ofrecidos por la organización, tanto si son desarrollados internamente como si son comprados deberá evaluarse previamente si los mismos son apropiados para su fin antes de aprobar su compra.
- Seguridad en los equipos informáticos y software: debido al tipo de servicios prestados, la organización deberá garantizar la seguridad en sus equipos informáticos y software de manera que se preserve la confidencialidad, disponibilidad e integridad de la información bajo su custodia.
- Control de los equipos de seguimiento y medición: la organización deberá determinar aquellos equipos hardware y aplicaciones software que necesiten un seguimiento y medición por su especial relevancia en la realización de los procesos. El mantenimiento y calibración de estos equipos y/o aplicaciones será especialmente crucial para los procesos de recolección, adquisición y preservación de evidencias digitales.
- Ambiente de trabajo: la organización deberá proporcionar y gestionar un ambiente de trabajo adecuado para lograr la realización de sus servicios, entendiendo como ambiente una combinación de factores humanos y físicos, que incluirá condiciones adecuadas de calor, humedad, temperatura y circulación de aire para las personas y equipamiento informático, condiciones adecuadas de higiene, limpieza, ruido, vibración y contaminación, ubicación adecuada del lugar de trabajo y ergonomía.

3.2.3.5 Compras.

El proceso de compras, incluyendo la adquisición de componentes o servicios proporcionados por terceros, es un proceso de soporte relevante en

cualquier sistema de gestión de calidad, debiéndose considerar los siguientes aspectos:

- Solicitudes de Compra/Pedidos de Compra: El proceso de compras se inicia cuando se detecta una necesidad en la organización. Resulta recomendable contar con registro de proveedores, actualizando el mismo en función de necesidades específicas que pudieran surgir paulatinamente. Cada proyecto de compra deberá contar con un seguimiento de inicio a fin, instancia en la que se verificará que el producto cumpla con los requisitos y especificaciones establecidas. Caso contrario se generará un incidente de devolución.
- Selección y evaluación inicial de proveedores: estos serán seleccionados atendiendo criterios como prestigio y experiencia en el sector, proveedores con certificaciones de calidad, exclusividad de un determinado producto o servicio, representación de productos certificados y buena relación precio-calidad.
- Seguimiento y evaluación continua de los proveedores: estos deberán ser evaluados con una periodicidad anual, o extraordinariamente cuando el proveedor acumule una serie de incidentes que se consideren graves desde su última evaluación o una que por su naturaleza obligue a reevaluarlo.

3.2.3.6 Requisitos legales.

Todos los requisitos, tanto legales como regulatorios o contractuales, deben definirse documentarse y mantenerse actualizados de forma explícita para ser cumplidos. Por tal motivo, este proceso tiene como finalidad identificar las leyes relacionadas con la actividad de la organización y el ámbito del análisis forense digital, debiéndose considerar aspectos como:

- Legislación sobre Delitos Informáticos.
- Seguridad de la Información.
- Seguridad del personal.
- Seguridad física y ambiental.

- Contratos con terceras partes.
- Privacidad de la información.
- Auditoría de sistemas.
- Exportación de datos a otros países.
- Infraestructura de los sistemas.
- Legislación específica para transacciones económicas realizadas electrónicamente.
- Derechos de propiedad intelectual.
- Normas técnicas de referencia.

3.2.4 Mapa de procesos.

A fin de identificar las interrelaciones entre cada uno de los procesos que componen el sistema de gestión, se presenta el siguiente mapa de procesos que podrían incluirse en cada uno de los tres grandes bloques: estratégicos, operativos y de soporte.

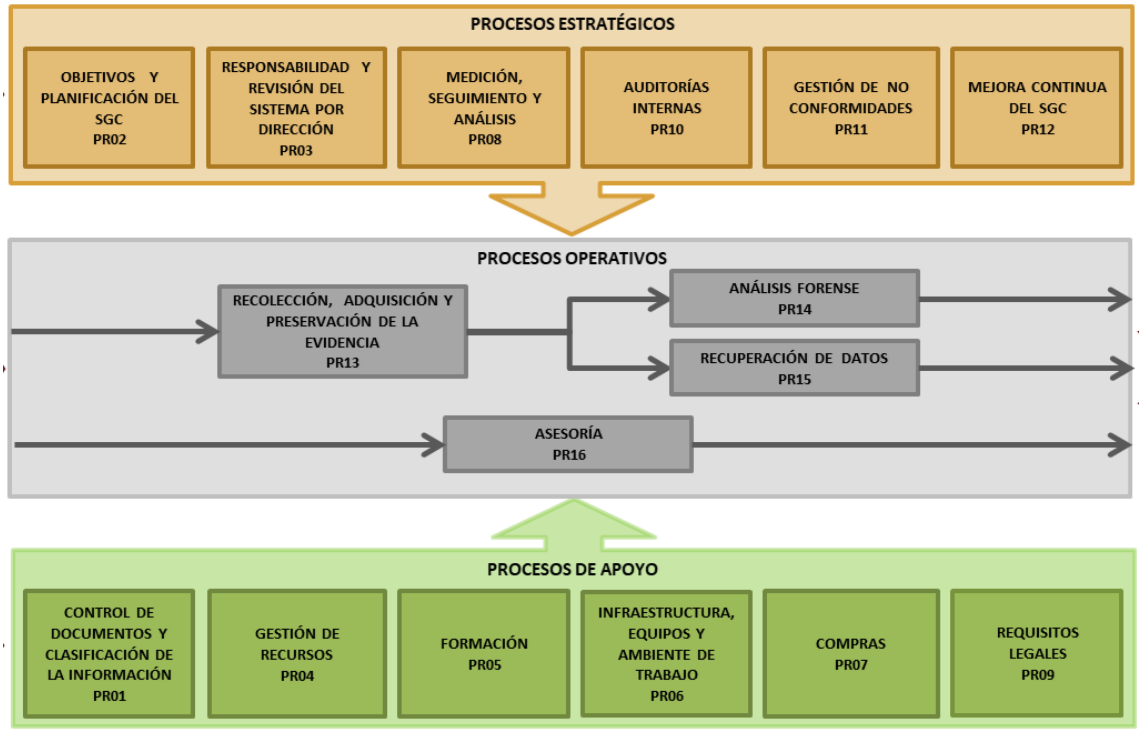

Ilustración 8: Mapa de procesos del Sistema de Gestión de Evidencia Digital.

3.3 Herramientas tecnológicas

Debido al constante avance tecnológico y dinámica del ecosistema digital, las instalaciones y equipamiento del laboratorio forense digital deben contemplar entornos que permitan su adaptabilidad, escalabilidad y alta disponibilidad, apuntalados por una sólida infraestructura y seguridad en tecnología de la información.

Un laboratorio de análisis forense digital debe contemplar el acceso a equipo forense especializado que resulta necesario para cumplir con los servicios ofrecidos por la organización, produciendo resultados forenses correctos acorde técnicas y procedimientos específicos. Este equipo puede encontrase en forma de hardware, software bajo licencia libre y comercial.

Del mismo modo, es altamente recomendable que antes de su uso, el equipo y/o herramientas forenses sean probados y verificados para garantizar que pueda producir los resultados correctos.

3.3.1 Software.

Al realizar una compra de software, la organización debe considerar el precio inicial, las tarifas anuales de licencia, las tarifas de mantenimiento y las tarifas de capacitación.

El costo de las licencias puede ser significativo, por lo que se deberá realizar un estudio exhaustivo e incluirlo en la planificación del presupuesto para las subsiguientes tarifas anuales, circunstancia que podría resultar crítica en caso de no realizar las previsiones necesarias para su mantenimiento.

Por otro lado, debe asegurarse de que el software obtenido coincida correctamente con los requisitos del laboratorio de análisis forense digital y los servicios prestados o que se deseen prestar en el futuro, teniendo como premisas fundamentales la interoperabilidad y compatibilidad de las herramientas forenses.

Algunas aplicaciones forenses de código abierto ofrecen amplias funciones y pueden ser utilizados por los investigadores, pero es posible que este software carezca de oportunidades de apoyo y capacitación.

El laboratorio de análisis forense digital también debe considerar la implementación de un sistema de gestión de casos para su funcionamiento. Este sistema permitirá administrar la base de datos de casos, pruebas, nombre del examinador y resultados forenses.

3.3.2 Hardware.

El hardware también debe recibir un mantenimiento adecuado de forma periódica, para lo cual se recomienda tener un plan programado y un inventario pormenorizado de los equipos forenses.

Un elemento importante que debe considerar la organización, además del almacenamiento y la copia de seguridad de los datos operativos, es el almacenamiento de la evidencia electrónica. Los tres tipos de datos con los que puede necesitar tratar el laboratorio de análisis digital son la evidencia original, las copias forenses y los datos generados y/o hallazgos obtenidos durante el análisis.

Es fundamental que la infraestructura tecnológica del laboratorio de análisis forense digital cuente con un servidor grande, potente y rápido debido al volumen de datos y evidencia electrónica que deberá procesar y almacenar. Se debe implementar además un estricto procedimiento de respaldo y archivo para garantizar disponibilidad de la información y resiliencia de la organización.

Contar con este tipo de tecnología garantiza la escalabilidad y personalización de los recursos en función de las necesidades de la organización, sumado a que ofrece mayor capacidad de procesamiento y almacenamiento, circunstancia que es un claro beneficio a la hora de ejecutar actividades mediante aplicaciones forenses que demandan cada vez mayores recursos de esa naturaleza.

Del mismo modo, resulta oportuno señalar que entre las principales ventajas se pueden destacar:

- Performance: cuenta con la capacidad de reducir significativamente los tiempos de procesamiento y al mismo tiempo incrementa sustancialmente la capacidad de almacenamiento.
- Flexibilidad: contribuye principalmente a la escalabilidad, motivo por el cual los proyectos de crecimiento de la organización se verían beneficiados en

el tiempo.

- Autonomía: la administración central permite tener plena administración de los usuarios, control de accesos o gestión del banco de evidencias digitales.
- Estabilidad: contar con los mejores recursos de conectividad y hardware garantiza mejores condiciones de desempeño.
- Seguridad: debido a que se cuenta con servidores dedicados, la administración de seguridad será exclusiva de la organización.

3.3.3 Herramientas y accesorios.

Las herramientas y accesorios como cables, destornilladores y extensiones eléctricas son tan importantes como el software y el hardware en un laboratorio de análisis forense digital. Algunos trabajos requieren que el desmontaje y re ensamblado dispositivos electrónicos, por lo que resulta necesario tener acceso a herramientas y accesorios de buena calidad.

A continuación, se agrega un listado con los posibles elementos que un laboratorio de análisis forense puede necesitar para realizar las tareas diarias:

- Prolongador de energía.
- Cables y adaptadores.
- Destornilladores de precisión.
- Kit de herramientas.
- Manta y pulsera antiestática.
- Pincel / cepillo antiestático.
- Cámara fotográfica y grabadora de video.
- Caja de almacenamiento o contenedor para transportar equipo.
- Elementos de magnificación.
- Sobres para evidencias.
- Etiquetas autoadhesivas.

- Marcadores permanentes.
- Bolsa de Faraday.

Ilustración 9: Diseño del laboratorio de análisis forense digital.

3.4 IMMC: Evaluación del grado de madurez de un laboratorio de análisis forense

Como cierre de esta investigación, se propuso diagramar un marco metodológico que permitiese integrar el modelo de madurez de capacidades en el seno de los laboratorios de informática forense, facilitando la comprensión y reconocimiento de los pasos necesarios para evolucionar hacia un estadio superior, en pos de la mejora continua.

En tal sentido, el desarrollo del IMMC tiene como finalidad proporcionar un mecanismo de autoevaluación que permita catalogar el grado de madurez de un laboratorio de análisis forense digital, independientemente de su naturaleza y/o envergadura.

A tal efecto, se empleó un modelo de encuesta cerrada como herramienta de autoevaluación, a partir de este cuestionario cualitativo la organización puede

realizar una autoevaluación mediante la clasificación de diferentes aspectos intrínsecos y puntuar el impacto de las preguntas utilizando una escala Likert[28] de cinco puntos.

Para establecer el puntaje de la escala se utilizó el número cinco como “muy de acuerdo” y uno como “muy en desacuerdo”, las fases generales del ICMM se construyeron en base a las etapas del modelo simplificado de análisis forense digital planteado en la presente investigación, realizada a raíz de la revisión de diferentes reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de informática forense y evidencia digital.

Debido al tipo de metodología empleada, este cuestionario puede ser aplicado fácilmente a una organización para comprender rápidamente su nivel de madurez respecto de las actividades y procedimientos que realiza en el campo del análisis forense digital, como así también facilita reconocer aquellos pasos necesarios para alcanzar mejoras que le permitan progresar y afianzarse como laboratorio forense digital.

3.4.1 Puntaje del IMMC.

Durante el presente proyecto se planteó un sistema de categorización por medio de la integración del modelo de madurez de capacidades aplicado a un laboratorio de informática forense, a fin que una organización o una parte interesada comprenda mejor cuáles son las capacidades actuales y qué pasos se pueden tomar para madurar su programa al siguiente nivel. Dicha evaluación se estructura en base a las etapas propias del análisis forense digital, consignadas en el modelo simplificado que se desarrollara previamente, acorde el puntaje correspondiente a los siguientes niveles o grados de madurez.

[28] En 1932 Rensis Likert publica este tipo de escalas de medición que en la actualidad es utilizada principalmente en la investigación de mercados para la comprensión de las opiniones, permitiendo determinar el nivel de acuerdo o desacuerdo de los encuestados.

Grado de Madurez	Puntaje
Nivel 1: Incompleto.	1
Nivel 2: Realizado.	2
Nivel 3: Gestionado.	3
Nivel 4: Definido.	4
Nivel 5: Optimizado.	5

Tabla 1: Puntaje asignado dentro del IMMC.

3.4.2 Etapa de identificación

En esta sección el IMMC se enfoca en identificar la capacidad para llevar a cabo procedimientos como triage[29], identificación de dispositivos electrónicos, documentación de la escena y actividades realizadas, la seguridad física de las pruebas y los procedimientos de aislamiento. Evaluar esta etapa permitirá comprender las mejoras que se pueden realizar en las actividades vinculadas con la preparación de los materiales e identificación y manejo de diferentes fuentes de evidencias digitales.

[29] Proceso mediante el cual se recopila, reúne, analiza y priorizan evidencias digitales.

3.4.2.1 Triage en el lugar del hecho

Descripción de los procedimientos	Grado de Madurez Puntaje
• Se proporciona poca o ninguna orientación para las decisiones que se toman en la escena del crimen. • Se deja que los investigadores utilicen su mejor criterio y la obtención de pruebas a menudo es un fracaso o produce resultados incompletos.	Incompleto (Pts: 1)
• Los investigadores realizan el proceso de clasificación de manera inconsistente y lo mejor que pueden. • La escena del crimen se preserva de forma rudimentaria. • Rara vez se obtienen órdenes judiciales y autorizaciones antes de los procedimientos de triage.	Realizado (Pts: 2)
• El proceso de triage se encuentra claramente documentado y es seguido por los investigadores para asegurar la escena. • Las órdenes judiciales y otras autorizaciones necesarias se obtienen antes de llegar al lugar.	Gestionado (Pts: 3)
• El proceso de triage se encuentra claramente documentado y es seguido por los investigadores para asegurar la escena. • Los riesgos y amenazas se identifican antes de iniciar la investigación. • Las órdenes judiciales y otras autorizaciones necesarias se obtienen antes de llegar al lugar.	Definido (Pts: 4)
• El proceso de decisiones es claro y se aplica como guía para permitir la alineación con los estándares de la organización. Esto reduce las cargas de trabajo, aprovecha los recursos existentes, ofrece colecciones en vivo y produce resultados inmediatos. • El proceso de clasificación se encuentra claramente documentado y es seguido por los investigadores. • Los riesgos y amenazas se identifican antes de iniciar la investigación. • Las órdenes judiciales y otras autorizaciones necesarias se obtienen antes de llegar al lugar.	Optimizado (Pts: 5)

Tabla 2: Procedimientos vinculados con el triage en el lugar del hecho.

3.4.2.2 Reconocimiento de evidencias electrónicas

Descripción de los procedimientos	Grado de Madurez Puntaje
• Los investigadores no tienen orientación o experiencia sobre lo que debe recolectarse y conservarse para la investigación. • No se realiza la identificación de ciertos dispositivos y los investigadores no están seguros de haber recolectado todo lo que podría estar dentro del alcance de la investigación.	Incompleto (Pts: 1)
• El investigador a menudo pasa por alto los dispositivos tecnológicos que deberían estar incluidos en el alcance de la investigación. • Los dispositivos pueden pasarse por alto si están ocultos o fuera de la vista. • Los investigadores generalmente se detienen cuando han recolectado computadoras portátiles o personales.	Realizado (Pts: 2)
• Los investigadores están capacitados y tienen procedimientos claros para identificar la tecnología que podría proporcionar evidencia. • Los investigadores recopilan todos los dispositivos que se han definido en los procedimientos.	Gestionado (Pts: 3)
• Los investigadores están capacitados y tienen procedimientos claros para identificar la tecnología que podría proporcionar evidencia. • Los investigadores recopilan todos los dispositivos que se han definido en los procedimientos. • El investigador busca otros dispositivos que podrían contener evidencia digital.	Definido (Pts: 4)
• Los investigadores están capacitados y tienen procedimientos claros para identificar la tecnología que podría proporcionar evidencia. • Se realiza una búsqueda sistemática en la escena del crimen para identificar todos los posibles dispositivos que podrían parecer irrelevantes a primera vista. • Los respondedores consideran la posibilidad de dispositivos ocultos y realizan búsquedas exhaustivas.	Optimizado (Pts: 5)

Tabla 3: Procedimientos vinculados con la identificación de evidencias electrónicas.

3.4.2.3 Documentación de la escena del hecho

Descripción de los procedimientos	Grado de Madurez Puntaje
• La documentación relevada en la escena es poca o nula. • Los investigadores no saben qué puede ser útil en la investigación cuando surjan futuros interrogantes.	Incompleto (Pts: 1)
• La documentación se crea de forma ad-hoc. • La calidad de la documentación se basa en el conocimiento de los investigadores.	Realizado (Pts: 2)
• Existen procedimientos para la documentación de la escena del crimen. • Los investigadores documentan adecuadamente la escena del crimen de acuerdo con los procedimientos aprobados.	Gestionado (Pts: 3)
• Las evidencias se encuentran definidas y contabilizadas con precisión. • Se recogen materiales de papel como facturas y embalajes. • Los periféricos, conectores, medios extraíbles, dispositivos móviles y pantallas se fotografían y guardan con el estuche.	Definido (Pts: 4)
• Las evidencias se encuentran definidas y contabilizadas con precisión. • Se recogen materiales de papel como facturas y embalajes. • Se fotografía el estado general de escena y ubicación original de los dispositivos electrónicos para ser aportador en caso que sean de utilidad en el futuro. • Los periféricos, conectores, medios extraíbles, dispositivos móviles y pantallas se fotografían y guardan con el estuche.	Optimizado (Pts: 5)

Tabla 4: Procedimientos vinculados con la documentación de la escena del hecho.

3.4.2.4 Resguardo de los medios físicos de almacenamiento

Descripción de los procedimientos	Grado de Madurez Puntaje
• Los dispositivos físicos no se recolectan o se hace al azar sin una comprensión clara sobre el alcance de la investigación. • No se utiliza fotografía y no se crea documentación complementaria sobre los dispositivos.	Incompleto (Pts: 1)
• Los dispositivos físicos se recopilan de acuerdo con la comprensión de cada investigador. • En ocasiones, la fotografía se utiliza para complementar la documentación.	Realizado (Pts: 2)
• Existen procedimientos para resguardar adecuadamente todos los dispositivos que pueden contener evidencia digital. • La fotografía se utiliza para complementar la documentación de los dispositivos.	Gestionado (Pts: 3)
• Una vez que se incauta un dispositivo, se coloca en el contenedor apropiado y se etiqueta de acuerdo con los estándares de la organización. • Se utiliza fotografía significativa para complementar detalles del caso. • Se sigue la cadena de custodia. El contenedor se transporta inmediatamente y se registra su ingreso en el depósito del laboratorio forense.	Definido (Pts: 4)
• Una vez que se incauta el dispositivo, se coloca en el contenedor apropiado y se etiqueta de acuerdo con los estándares de la organización. • Se utiliza fotografía significativa para complementar detalles del caso. • Se sigue la cadena de custodia. El contenedor se transporta inmediatamente y se registra su ingreso en el depósito del laboratorio forense. • Los dispositivos alimentados por batería que deben permanecer encendidos se identifican y se les proporciona la energía.	Optimizado (Pts: 5)

Tabla 5: Procedimientos vinculados con el resguardo de los medios físicos.

3.4.2.5 Aislamiento de los dispositivos incautados

Descripción de los procedimientos	Grado de Madurez Puntaje
• Los dispositivos no están protegidos de señales inalámbricas o conectividad remota externa. • Un bloqueo o borrado remoto de la memoria pueden tener un impacto grave sobre el dispositivo.	Incompleto (Pts: 1)
• El investigador puede tomar medidas para aislar el dispositivo. • El asilamiento se basa en la experiencia del investigador.	Realizado (Pts: 2)
• Existen procesos tipificados para el aislamiento de los dispositivos involucrados en una investigación. • Los investigadores están capacitados en procedimientos básicos y toman medidas para preservar el estado de los dispositivos incautados.	Gestionado (Pts: 3)
• Existen procesos tipificados para el aislamiento de los dispositivos involucrados en una investigación. • Los investigadores proporcionan indicaciones al equipo sobre nuevos dispositivos identificados y cómo podrían recolectados. • Los investigadores están capacitados en procedimientos básicos y toman medidas para preservar el estado de los dispositivos incautados.	Definido (Pts: 4)
• Los dispositivos se aíslan de otros elementos utilizados para la sincronización de datos, como una estación base, un cable USB o una computadora personal. • Los investigadores proporcionan indicaciones al equipo sobre nuevos dispositivos identificados y cómo podrían recolectados. • El dispositivo está aislado de todas las redes de comunicación, como WIFI, Celular y Bluetooth, para evitar modificaciones en su contenido. • Los dispositivos se colocan en modo avión o se preservan en bolsas de Faraday.	Optimizado (Pts: 5)

Tabla 6: Procedimientos vinculados con el aislamiento de los dispositivos incautados.

3.4.3 Etapa de preservación

La sección de adquisición y preservación puede ser desarrollada tanto en el lugar como en ambiente de laboratorio, ocupándose principalmente de la recopilación de pruebas. Esta fase se incluyen actividades como el aseguramiento de la cadena de custodia, la adquisición de unidades de almacenamiento, memoria, eventos de red y sistema, extracción forense sobre dispositivos móviles y cálculo de algoritmos de seguridad hash. La evaluación de esta etapa permitirá comprender las mejoras que se pueden realizar en la recopilación de evidencia digital de todas las fuentes posibles y pasos necesarios para la cadena de custodia.

3.4.3.1 Cadena de custodia

Descripción de los procedimientos	Grado de Madurez Puntaje
• No se implementa la cadena de custodia durante las investigaciones.	Incompleto (Pts: 1)
• La cadena de custodia es problemática, no existe trazabilidad de los registros. • La cadena de custodia solo se lleva a cabo para ciertos casos y según criterio del investigador.	Realizado (Pts: 2)
• Existen procedimientos formalizados para el registro de la cadena de custodia y se cumple con los mismos.	Gestionado (Pts: 3)
• Existen procedimientos formalizados para el registro de la cadena de custodia y se cumple con los mismos. • La cadena de custodia ingresa digitalmente en una plataforma de gestión de evidencias electrónicas.	Definido (Pts: 4)
• El procedimiento de cadena de custodia se encuentra documentado rigurosamente. • El proceso da cuenta de cada elemento de prueba desde la recolección hasta la presentación. • La cadena de custodia está claramente documentada, archivada electrónicamente en una plataforma de gestión de evidencias electrónicas y no puede modificarse.	Optimizado (Pts: 5)

Tabla 7: Procedimientos vinculados con la cadena de custodia.

3.4.3.2 Adquisición por medio de imágenes forenses

Descripción de los procedimientos	Grado de Madurez Puntaje
• No se considera obtener imágenes forenses. • Los examinadores recopilan dispositivos físicos con para realizar el análisis a partir de los mismos.	Incompleto (Pts: 1)
• No existe un estándar claro sobre cómo se obtendrán las imágenes forenses. • La obtención de imágenes se realiza según el criterio del examinador. • A menudo se generan evidencias lógicas. • Las imágenes pueden corromperse o manipularse incorrectamente durante el proceso de adquisición.	Realizado (Pts: 2)
• Las imágenes se obtienen de forma correcta y segura de acuerdo con procedimientos definidos. • Tanto la generación de evidencias lógicas como la creación de imágenes físicas se realizan cuando corresponde de acuerdo al caso investigado. • Las imágenes forenses se resguardan en un dispositivo de almacenamiento para que los investigadores accedan a las mismas.	Gestionado (Pts: 3)
• Las imágenes se obtienen de forma correcta y segura de acuerdo con procedimientos definidos. • Tanto la generación de evidencias lógicas como la creación de imágenes físicas se realizan cuando corresponde de acuerdo al caso investigado. • Se proporciona a los investigadores herramientas forenses portátiles con capacidad de almacenamiento suficiente para la obtención de imágenes forenses.	Definido (Pts: 4)
• Las imágenes se obtienen de forma correcta y segura de acuerdo con procedimientos definidos. • Tanto la generación de evidencias lógicas como la creación de imágenes físicas se realizan cuando corresponde de acuerdo al caso investigado. • Se proporciona a los investigadores herramientas forenses portátiles con capacidad de almacenamiento suficiente para la obtención de imágenes forenses. • Se tiene cuidado de no alterar el estado de los dispositivos incautados, los investigadores verificarán que la imagen forense se obtuvo correctamente.	Optimizado (Pts: 5)

Tabla 8: Procedimientos vinculados con adquisición de imágenes forenses.

3.4.3.3 Adquisición de memoria volátil

Descripción de los procedimientos	Grado de Madurez Puntaje
• La memoria volátil no se considera una fuente de evidencia que pueda ser de utilidad. • Los investigadores no están capacitados para realizar la adquisición de memoria.	Incompleto (Pts: 1)
• La adquisición de memoria se realiza de forma ad-hoc y solo por ciertos investigadores que entienden el procedimiento. • Las herramientas no están estandarizadas para la adquisición de memoria volátil. Las herramientas son elegidas por el investigador. • La adquisición de memoria volátil no tiene prioridad.	Realizado (Pts: 2)
• Existen procedimientos claros para la captura de memoria volátil. • Los investigadores han adoptado formalmente un conjunto de herramientas y se encuentran completamente capacitados. • Los investigadores recopilan memoria volátil de dispositivos comunes como computadoras portátiles o de escritorio.	Gestionado (Pts: 3)
• Existen procedimientos claros para la captura de memoria volátil. • Los investigadores han adoptado formalmente un conjunto de herramientas y se encuentran completamente capacitados. • Los investigadores se encuentran capacitados para obtener memoria volátil de varios tipos de dispositivos, como teléfonos, computadoras personales y otros dispositivos portátiles.	Definido (Pts: 4)
• Existen procedimientos claros para la captura de memoria volátil. • Los investigadores han adoptado formalmente un conjunto de herramientas y se encuentran completamente capacitados. • Los investigadores se encuentran capacitados para obtener memoria volátil de varios tipos de dispositivos, como teléfonos, computadoras personales y otros dispositivos portátiles. • Los registros obtenidos siguen los mismos lineamientos de seguridad que para el caso de las imágenes forenses.	Optimizado (Pts: 5)

Tabla 9: Procedimientos vinculados con adquisición de memoria volátil.

3.4.3.4 Recolección de eventos de red

Descripción de los procedimientos	Grado de Madurez Puntaje
• Los registros de eventos de red no se buscan ni se recolectan como evidencia. • Los investigadores no están capacitados para recolectar pruebas de equipos de seguridad o de red.	Incompleto (Pts: 1)
• Los registros de eventos de red no se recolectan de forma correcta. • Cuando se recolectan se hace de acuerdo al nivel de conocimiento del investigador y no se obtienen resultados consistentes.	Realizado (Pts: 2)
• Los investigadores están capacitados en la recolección y posible empleo de los registros eventos de red para la investigación. • Los registros de eventos de red se recolectan de los sistemas cuando resultan pertinentes para la investigación. • Existe un procedimiento escrito para realizar la recolección de los eventos de red.	Gestionado (Pts: 3)
• Los investigadores están capacitados en la recolección y posible empleo de los registros eventos de red para la investigación. • Los registros de eventos de red se recolectan de los sistemas cuando resultan pertinentes para la investigación. • Los registros se recolectan de manera coherente y se realiza la correlación de eventos. • Existe un procedimiento escrito para realizar la recolección de los eventos de red.	Definido (Pts: 4)
• Los investigadores buscan registro de eventos en diferentes fuentes como firewalls, filtros de contenido, sistemas para detección de intrusiones (ISD) y gestión de eventos de seguridad (SIEM). • Los registros relevantes se exportan y se agregan a las evidencias de la investigación. • Los registros se recolectan de manera coherente, realizándose la correlación de eventos y línea de tiempo correspondiente. • Se realiza una interconsulta con áreas de seguridad de la Información para interpretar completamente los eventos recolectados.	Optimizado (Pts: 5)

Tabla 10: Procedimientos vinculados con la recolección de eventos de red.

3.4.3.5 Recolección de dispositivos IoT

Descripción de los procedimientos	Grado de Madurez Puntaje
• Los dispositivos de IoT no se consideran fuentes de evidencia para la investigación.	Incompleto (Pts: 1)
• Los dispositivos de IoT no se consideran habitualmente como fuentes de evidencia para la investigación. • Cuando en la investigación se recolectan dispositivos IoT, el procedimiento se lleva a cabo según el criterio del investigador.	Realizado (Pts: 2)
• Los investigadores están capacitados para buscar evidencias en dispositivos de IoT. • Existe un procedimiento escrito para realizar la recolección de dispositivos IoT.	Gestionado (Pts: 3)
• Los investigadores están capacitados para buscar evidencias en dispositivos de IoT. • Existe un procedimiento escrito para realizar la recolección de dispositivos IoT. • Los dispositivos de IoT se preservan en un estado que garantice la integridad de sus datos.	Definido (Pts: 4)
• Los investigadores están capacitados para buscar evidencias en dispositivos de IoT. • Existe un procedimiento escrito para realizar la recolección de dispositivos IoT locales, redes y fuentes en la nube. • Los dispositivos de IoT se preservan en un estado que garantice la integridad de sus datos.	Optimizado (Pts: 5)

Tabla 11: Procedimientos vinculados con la recolección de dispositivos IoT.

3.4.3.6 Recolección de dispositivos móviles

Descripción de los procedimientos	Grado de Madurez Puntaje
• Los dispositivos móviles no se consideran fuentes de evidencias para la investigación. • Los investigadores no están capacitados en la extracción de evidencia de dispositivos móviles.	Incompleto (Pts: 1)
• Los dispositivos móviles se recolectan ocasionalmente como fuentes de evidencia. • El análisis forense de dispositivos móviles solo tiene éxito dependiendo del nivel de conocimiento del investigador. • Las extracciones lógicas se llevan a cabo desde el dispositivo conectado a una PC de forma rudimentaria mediante transferencia de archivos.	Realizado (Pts: 2)
• Existe un procedimiento escrito para realizar el análisis forense de dispositivos móviles. • Los investigadores están capacitados formalmente en el análisis de dispositivos móviles. • Los investigadores tienen la capacidad de recolectar registros de llamadas, listas de contactos, mensajes de texto, chats de aplicaciones de mensajería, historial de navegación e información almacenada en medios extraíbles desde un teléfono desbloqueado.	Gestionado (Pts: 3)
• Existe un procedimiento escrito para realizar el análisis forense de dispositivos móviles. • Los investigadores están capacitados formalmente en el análisis de dispositivos móviles. • Los investigadores tienen la capacidad de recolectar registros de llamadas, listas de contactos, mensajes de texto, chats de aplicaciones de mensajería, historial de navegación e información almacenada en medios extraíbles desde un teléfono desbloqueado o bloqueado. • Se consideran técnicas de extracción manual mediante técnicas alternativas.	Definido (Pts: 4)
• Existe un procedimiento escrito para realizar el análisis forense de dispositivos móviles. • Los investigadores están capacitados formalmente en el análisis de dispositivos móviles. • Los investigadores tienen la capacidad de recolectar registros de llamadas, listas de contactos, mensajes de texto, chats de aplicaciones de mensajería, historial de navegación e información almacenada en medios extraíbles desde un teléfono desbloqueado o bloqueado. • Los investigadores tienen la capacidad de extraer datos desde el nivel de la pantalla visual hasta el nivel	Optimizado (Pts: 5)

Descripción de los procedimientos	Grado de Madurez Puntaje
de chip off.	

Tabla 12: Procedimientos vinculados con la recolección de dispositivos móviles.

3.4.3.7 Hash de las evidencias

Descripción de los procedimientos	Grado de Madurez Puntaje
• Realizar el cálculo de hash sobre las evidencias no se considera necesario para la investigación.	Incompleto (Pts: 1)
• Los investigadores aseguran archivos específicos para ayudar en la investigación y garantizar la cadena de custodia. • El hash se utiliza de acuerdo con el nivel de conocimiento del investigador.	Realizado (Pts: 2)
• Existe un procedimiento formal escrito que describe cómo se procesará la evidencia para realizar el cálculo de hash. • Los investigadores aseguran archivos específicos para ayudar en la investigación y garantizar la cadena de custodia.	Gestionado (Pts: 3)
• Existe un procedimiento formal escrito que describe cómo se procesará la evidencia para realizar el cálculo de hash. • Los investigadores aseguran archivos específicos para ayudar en la investigación y garantizar la cadena de custodia. • Los investigadores utilizan hash para identificar archivos conocidos utilizados en otras investigaciones criminales.	Definido (Pts: 4)
• Existe un procedimiento formal escrito que describe cómo se procesará la evidencia para realizar el cálculo de hash. • Los investigadores aseguran archivos específicos para ayudar en la investigación y garantizar la cadena de custodia. • El hash se utiliza de acuerdo con el nivel de conocimiento del investigador. • Los investigadores utilizan bibliotecas de hash para reducir significativamente la cantidad de archivos que deben analizarse.	Optimizado (Pts: 5)

Tabla 13: Procedimientos vinculados con el hash de las evidencias.

3.4.3.8 Copias de seguridad

Descripción de los procedimientos	Grado de Madurez Puntaje
• Las copias de seguridad no se consideran necesarias en la investigación. Se utilizan soportes originales.	Incompleto (Pts: 1)
• Hacer una copia de seguridad de la evidencia no es habitual en las investigaciones. • Las copias de seguridad se realizan según el criterio del investigador. • Las copias de seguridad de las pruebas no se encuentran disponibles frecuentemente.	Realizado (Pts: 2)
• Existen procedimientos formales para realizar copias de seguridad de las evidencias recolectadas. • Los investigadores realizan copias de seguridad para preservar la evidencia original. • Las copias tienen como finalidad ser empleadas durante la etapa de análisis forense en lugar de los ejemplares originales.	Gestionado (Pts: 3)
• Existen procedimientos formales para realizar copias de seguridad de las evidencias recolectadas. • Existen múltiples copias de seguridad de cada dispositivo disponibles para los investigadores. • Las copias tienen como finalidad ser empleadas durante la etapa de análisis forense en lugar de los ejemplares originales.	Definido (Pts: 4)
• Se utiliza una suite forense para almacenar los archivos de todos los investigadores del equipo en un mismo lugar. • Existen varias copias de seguridad de cada dispositivo analizado. • Los datos recabados se respaldan para ser utilizados durante el proceso de investigación. • Las copias de seguridad se almacenan en diferentes ubicaciones como plan de contingencia ante posibles desastres o incidentes de seguridad.	Optimizado (Pts: 5)

Tabla 14: Procedimientos vinculados con las copias de seguridad.

3.4.4 Etapa de análisis

Esta sección hace foco principalmente en examinar el contenido de la evidencia digital recopilada por el examinador forense. Esta fase incluye no solo el análisis de evidencia digital, sino también de otro tipo de elementos que puedan aportar información de interés, como por ejemplo documentación, anotaciones, elementos electrónicos y hardware, entre otros. Conocer la madurez de esta etapa indicará las mejoras que se pueden realizar al realizar el análisis técnico de diferentes fuentes de evidencias digitales, como así también otros subconjuntos de datos.

3.4.4.1 Entrenamiento formal

Descripción de los procedimientos	Grado de Madurez Puntaje
• No existe capacitación disponible para los recursos que realizan las investigaciones.	Incompleto (Pts: 1)
• El éxito de las investigaciones se basa en el conocimiento individual de los analistas forenses que se encuentran a cargo. • Rara vez se ofrece capacitación formal.	Realizado (Pts: 2)
• Los integrantes del equipo son capacitados por los proveedores sobre el conjunto de herramientas que utilizan. • Los integrantes con mayor conocimiento capacitan a los miembros más jóvenes del equipo.	Gestionado (Pts: 3)
• Los integrantes del equipo son capacitados por organismos oficiales o proveedores sobre el conjunto de herramientas que utilizan. • Un programa de mentores hace que los miembros senior capaciten a los miembros junior • Los analistas forenses obtienen certificaciones en el conjunto de herramientas que utilizan.	Definido (Pts: 4)
• Los equipos forenses obtienen formación formal e interna durante todo el año. • Los miembros del equipo asisten a las conferencias forenses. • Se solicita a los proveedores que mantengan actualizado al equipo al día respecto de nuevas funcionalidades en las herramientas. • Los integrantes con mayor conocimiento capacitan a los miembros más jóvenes del equipo. • Los investigadores obtienen certificaciones en sus conjuntos de herramientas.	Optimizado (Pts: 5)

Tabla 15: Procedimientos vinculados con el entrenamiento formal.

3.4.4.2 Repetitividad de los análisis practicados

Descripción de los procedimientos	Grado de Madurez Puntaje
• Los investigadores no prueban las herramientas forenses para asegurar que proporcionan resultados correctos.	Incompleto (Pts: 1)
• Las herramientas forenses se prueban una vez implementadas y de forma ad-hoc para actualizaciones futuras.	Realizado (Pts: 2)
• Las herramientas forenses se prueban una vez implementadas y de forma ad-hoc para actualizaciones futuras.	Gestionado (Pts: 3)
• La administración de la agencia realiza las pruebas internas. • Los examinadores participan en diferentes pruebas internas con evidencias y artefactos forenses cuyos resultados son pueden ser previamente conocidos o desconocidos.	Definido (Pts: 4)
• Todos los procesos se prueban para verificar su repetitividad. Los examinadores participan en diferentes pruebas internas con evidencias y artefactos forenses cuyos resultados son pueden ser previamente conocidos o desconocidos. • Todos los investigadores están capacitados utilizando los mismos procedimientos. • Un investigador independiente puede repetir el proceso para proporcionar resultados comparativos.	Optimizado (Pts: 5)

Tabla 16: Procedimientos vinculados con la repetitividad de los análisis practicados.

3.4.4.3 Conjunto de herramientas forenses

Descripción de los procedimientos	Grado de Madurez Puntaje
• El análisis consiste en un proceso manual de observación. • Los investigadores no cuentan con un conjunto de herramientas forenses.	Incompleto (Pts: 1)
• Los investigadores realizan análisis forenses con los conjuntos de herramientas de su preferencia personal. • Las herramientas utilizadas no se encuentran optimizadas para el análisis que se encuentra realizando. • Se utilizan herramientas código abierto o gratuitas.	Realizado (Pts: 2)
• Se proporcionan herramientas forenses y los investigadores reciben capacitación sobre las mismas. • Se compran y obtienen herramientas forenses para alinearse con las investigaciones que se llevan a cabo. • Se utilizan herramientas comerciales, de código abierto y gratuitas.	Gestionado (Pts: 3)
• Se proporcionan herramientas forenses de probada efectividad y los investigadores reciben capacitación sobre las mismas. • Se compran y obtienen herramientas forenses para alinearse con las investigaciones que se llevan a cabo. • Se pone a disposición de las investigaciones una combinación de herramientas empresariales y de código abierto.	Definido (Pts: 4)
• Se proporcionan herramientas forenses de probada efectividad y los investigadores reciben capacitación sobre las mismas. • Se compran y obtienen herramientas forenses para alinearse con las investigaciones que se llevan a cabo. • Los investigadores desarrollan herramientas personalizadas para las investigaciones. • Se pone a disposición de las investigaciones una combinación de herramientas empresariales y de código abierto.	Optimizado (Pts: 5)

Tabla 17: Procedimientos vinculados con el conjunto de herramientas forenses.

3.4.4.4 E-Discovery

Descripción de los procedimientos	Grado de Madurez Puntaje
• Los investigadores no realizan e-Discovery como parte de las investigaciones. • El e-Discovery no se lleva a cabo en esta fase.	Incompleto (Pts: 1)
• e-Discovery puede ser realizado por un investigador, pero el resultado no siempre es exitoso en la identificación de medios de prueba.	Realizado (Pts: 2)
• e-Discovery se lleva a cabo de acuerdo con un procedimiento escrito. • Los investigadores logran obtener documentación y vinculaciones cuando es necesario el e-Discovery.	Gestionado (Pts: 3)
• e-Discovery se lleva a cabo de acuerdo con un procedimiento escrito. • Los investigadores logran obtener documentación y vinculaciones cuando es necesario el e-Discovery. • Los resultados identificados se comparten con otros investigadores o personas de interés.	Definido (Pts: 4)
• e-Discovery se lleva a cabo de acuerdo con un procedimiento escrito. • Los investigadores logran obtener documentación y vinculaciones cuando es necesario el e-Discovery. • Los resultados identificados se comparten con otros investigadores o personas de interés. • Se pone a disposición de los investigadores una plataforma empresarial de e-Discovery.	Optimizado (Pts: 5)

Tabla 18: Procedimientos vinculados con E-Discovery.

3.4.5 Etapa de presentación

Tiene como finalidad presentar un documento escrito que contenga un pormenorizado detalle sobre los datos del caso, el investigador que participó, las evidencias analizadas, metodología aplicada, operaciones practicadas, resultados obtenidos y conclusiones arribadas respecto del interrogante pericial planteado. Esta fase incluye además la documentación de nuevas metodologías y lecciones aprendidas. Realizar una evaluación permitirá identificar oportunidades de mejora en la manera en que se presentan, categorizan y presentan los resultados fruto de una investigación forense.

3.4.5.1 Informes periciales

Descripción de los procedimientos	Grado de Madurez Puntaje
• El investigador no realiza ningún reporte formal después de concluir la investigación.	Incompleto (Pts: 1)
• Los reportes se realizan y se ajuntan ocasionalmente a la investigación. • Por lo general faltan informes y, a menudo, se encuentran incompletos.	Realizado (Pts: 2)
• Existen plantillas personalizadas que los investigadores utilizan para redactar un documento coherente. • Los informes se encuentran completos y detallados.	Gestionado (Pts: 3)
• Existen plantillas personalizadas que los investigadores utilizan para redactar un documento coherente. • Los investigadores redactan y siguen normas de presentación de informes acorde procedimientos establecidos. • Se envían materiales de apoyo adicional como copias de evidencia digital, cadena de custodia, notas de campo y otra evidencia física.	Definido (Pts: 4)
• Los investigadores redactan y siguen normas de presentación de informes acorde procedimientos establecidos. • El informe se encuentra elaborado pensando en la audiencia, evitándose caer en exceso de vocabulario técnico. • Se envían materiales de apoyo como copias de evidencia digital, cadena de custodia, notas de campo del investigador y otra evidencia física. • El informe consiste en un resumen claro y detallado de los pasos de la investigación, las herramientas utilizadas y las conclusiones arribadas.	Optimizado (Pts: 5)

Tabla 19: Procedimientos vinculados con los informes periciales.

3.4.5.2 Lecciones aprendidas

Descripción de los procedimientos	Grado de Madurez Puntaje
• Las lecciones aprendidas no se registran o son documentadas eventualmente por el investigador.	Incompleto (Pts: 1)
• Los investigadores registran y documentan periódicamente las lecciones aprendidas.	Realizado (Pts: 2)
• Existen procedimientos formales para documentar las lecciones aprendidas. • Las actividades de compartir las lecciones aprendidas se llevan a cabo después de cada investigación.	Gestionado (Pts: 3)
• Existen procedimientos formales para documentar las lecciones aprendidas. • Los investigadores se reúnen formalmente para revisar las fases de la investigación, los resultados e identificar oportunidades de mejora continua. • Las lecciones aprendidas se utilizan habitualmente para mejorar el proceso forense y capacitar a todos los investigadores.	Definido (Pts: 4)
• Existen procedimientos formales para documentar las lecciones aprendidas. • Los investigadores se reúnen formalmente para revisar las fases de la investigación, los resultados e identificar oportunidades de mejora continua. • Las lecciones aprendidas se utilizan habitualmente para mejorar el proceso forense y capacitar a todos los investigadores. • Los directivos y otras partes interesadas asisten a las reuniones para conocer las lecciones aprendidas.	Optimizado (Pts: 5)

Tabla 20: Procedimientos vinculados con las lecciones aprendidas.

4
Conclusiones

Acorde a las actividades realizadas durante el desarrollo del presente Trabajo Final de Maestría, basado en la investigación exploratoria y documental sobre reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de informática forense y evidencia digital, tanto nacionales y como del extranjero, resultó factible establecer una gran cantidad de información sobre los desafíos y problemas reales que enfrentan los laboratorios de análisis forense digital.

Del mismo modo, por medio del presente estudio, se diseñó y elaboró un marco de referencia para integrar el modelo de madurez de capacidades en laboratorios de análisis forense digital, promoviendo una mejora significativa en la gestión de sus recursos y alcanzar sus objetivos a través de un sistema de evaluaciones y herramientas de planificación, orientadas a medir el cumplimiento y estadio de tres dominios organizativos clave: personas, procesos y herramientas tecnológicas, y sus interrelaciones, lo que permite:

- Brindar un marco de referencia integral y estratégico, facilitando su interpretación práctica e implementación en diferentes organizaciones, independientemente de su actividad o envergadura, permitiéndoles conocer su grado de madurez actual mediante un sistema de autoevaluación.
- Incrementar la eficacia y eficiencia de los procesos llevados a cabo en los laboratorios forenses digitales, logrando comprender cuáles son las capacidades actuales y qué pasos se pueden tomar para madurar su programa al siguiente nivel, garantizando la calidad de los servicios prestados, en pos de una mejora continua.
- Además, surge que las normas y estándares existentes en materia de informática forense y evidencia digital existentes, resultan demasiado

generales o demasiado técnicos y específicos, y no proporcionaban un esquema holístico para abordar la mayoría de los desafíos más críticos y significativos que enfrentan los laboratorios de análisis forense digital en los tres dominios organizativos clave: personas, procesos y herramientas tecnológicas, de forma integral.

Los resultados del presente trabajo, sientan las bases para tomar como posible línea de investigación, desarrollo e innovación, el diseño y elaboración de una herramienta para automatizar el sistema de autoevaluación e integración del modelo de madurez de capacidades en los laboratorios de informática forense, a fin que una organización o una parte interesada comprenda mejor cuáles son las capacidades actuales y establecer cuáles serán aquellos desafíos que deba enfrentar para evolucionar hasta lograr la excelencia de sus servicios forenses.

5
Bibliografía específica

[1] M. C. PAULK, «A Comparison of ISO 9001 and the Capability Maturity Model for Software,» Carnegie Mellon University, Pittsburgh, Pennsylvania, 1994.

[2] A. L. TANNER y D. A. DAMPIER, «An Approach for Managing Knowledge in Digital Forensics,» International Journal for Computer Science Security, Mississippi, 2010.

[3] T. LINDSEY, «Challenges in Digital Forensics,» Digital Forensic Research Workshop, New York, 2006.

[4] I. S. Organization, *General requirements for the competence of testing and calibration laboratories,* USA, 2017.

[5] N. W. Group, «www.ietf.org,» Febrero 2002. [En línea]. Available: https://www.ietf.org/rfc/rfc3227.txt. [Último acceso: 10 Octubre 2021].

[6] S. Australia, «https://www.saiglobal.com,» Marzo 2003. [En línea]. Available: https://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB171.PDF. [Último acceso: 10 Octubre 2021].

[7] N. I. o. S. a. Technology, «https://nvlpubs.nist.gov,» Agosto 2006. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. [Último acceso: 10 Octubre 2021].

[8] U. D. o. Justice, «https://www.ncjrs.gov,» Abril 2008. [En línea]. Available: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf. [Último acceso: 10 Octubre 2021].

[9] I. S. a. F. Society, «http://www.isfs.org.hk,» Agosto 2009. [En línea]. Available: http://www.isfs.org.hk/publications/ISFS_ComputerForensics_part2_20090806.pdf. [Último acceso: 10 Octubre 2021].

[10] A. o. C. P. Officers, «http://www.digital-detective.net,» Marzo 2012. [En línea]. Available: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. [Último acceso: 10 Octubre 2021].

[11] E. U. A. f. N. a. I. S. (ENISA), «https://www.enisa.europa.eu,» 2014. [En línea]. Available: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders/at_download/fullReport. [Último acceso: 10 Octubre

2021].

[12] I. S. Organization, *ISO/IEC 27037/2016 "Guidelines for identification, collection, acquisition, and preservation of digital evidence",* USA, 2016.

[13] P. G. d. l. Nación, «https://www.fiscales.gob.ar,» Marzo 2016. [En línea]. Available: https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf. [Último acceso: 10 Octubre 2021].

[14] M. d. S. d. l. Nación, «http://servicios.infoleg.gob.ar,» 07 Junio 2016. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/262787/norma.htm. [Último acceso: 10 Octubre 2021].

[15] C. Gispert, Enciclopedia Autodidactica Interactiva, México: Océano, 2002.

[16] C. N. d. I. C. y. Técnicas, «https://www.conicet.gov.ar,» Abril 2016. [En línea]. Available: https://www.conicet.gov.ar/programas/ciencia-y-justicia/ciencia-forense/. [Último acceso: 10 Octubre 2021].

[17] M. G. Noblett, «https://archives.fbi.gov,» Octubre 2000. [En línea]. Available: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm. [Último acceso: 10 Octubre 2021].

[18] R. C. &. Associates, «https://www.tech4law.co.za/,» 02 Marzo 2015. [En línea]. Available: https://www.tech4law.co.za/tech-advisor/107-digital-foren-sics/1528-what-is-digital-forensics/. [Último acceso: 10 Octubre 2021].

[19] R. Salgado, «https://federalevidence.com,» 02 Febrero 2013. [En línea]. Available: https://federalevidence.com/pdf/2013/02Feb/EE-4thAmSearch-Power%20of%20Hash.pdf. [Último acceso: 01 Abril 2019].

[20] N. I. o. S. a. Technology, «https://csrc.nist.gov,» 01 Agosto 2002. [En línea]. Available: https://csrc.nist.gov/csrc/media/publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf. [Último acceso: 01 Abril 2019].

[21] E. E. Torales, Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen, Buenos Aires: Ediciones Infojus, 2014.

[22] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3ra ed., San Diego (CA): Academic Press, 2011.

[23] J. J. C. Martínez, «Admisibilidad de la Evidencia Digital: Algunos Elementos de Revisión y Análisis,» *Revista Electrónica de Derecho Informático,* nº 61, 2003.

[24] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 26 Septiembre 1933. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/norma.htm. [Último acceso: 10 Octubre 2021].

[25] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 26 Diciembre 1980. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/18803/texact.htm. [Último acceso: 10 Octubre 2021].

[26] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 04 Octubre 20. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm. [Último acceso: 10 Octubre 2021].

[27] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 18 Diciembre 1996. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41094/norma.htm. [Último acceso: 10 Octubre 2021].

[28] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 19 Diciembre 1996. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41379/norma.htm. [Último acceso: 10 Octubre 2021].

[29] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 03 Agosto 1988. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20465/texact.htm. [Último acceso: 10 Octubre 2021].

[30] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 04 Junio 2008. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm. [Último acceso: 10 Octubre 2021].

[31] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 13 Noviembre 2013. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm. [Último acceso: 10 Octubre 2021].

[32] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar,» 28 Julio 2011. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm. [Último acceso: 10 Octubre 2021].

[33] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar,» 16 Septiembre 2011. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/187698/norma.htm. [Último acceso: 10 Octubre 2021].

[34] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar,» 08 Agosto 2013. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219212/norma.htm. [Último acceso: 10 Octubre 2021].

[35] A. P. NACIONAL, «http://servicios.infoleg.gob.ar,» 10 Junio 2015. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247971/norma.htm. [Último acceso: 10 Octubre 2021].

[36] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar,» 10 Noviembre 2015. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/255201/norma.htm. [Último acceso: 10 Octubre 2021].

[37] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar,» 20 Agosto 2015. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/250000-254999/251022/norma.htm. [Último acceso: 10 Octubre 2021].

[38] P. G. d. l. Nación, «http://www.mpf.gov.ar,» 18 Noviembre 2015. [En línea]. Available: http://www.mpf.gov.ar/resoluciones/pgn/2015/PGN-3743-2015-001.pdf. [Último acceso: 10 Octubre 2021].

[39] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 25 Febrero 2015. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm. [Último acceso: 10 Octubre 2021].

[40] M. d. S. d. l. Nación, «https://www.argentina.gob.ar/,» 16 Abril 2018. [En línea]. Available: https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-564-2018-308989. [Último acceso: 10 Octubre 2021].

[41] J. d. G. d. Ministros, «https://www.boletinoficial.gob.ar,» 25 Junio 2021. [En línea]. Available: https://www.boletinoficial.gob.ar/detalleAviso/primera/246104/20210628. [Último acceso: 10 Octubre 2021].

[42] I. S. Organization, *Quality management systems — Fundamentals and vocabulary,* USA, 2015.

[43] I. S. Organization, *Quality management systems — Requirements,* USA, 2015.

[44] W. S. HUMPHREY, «Characterizing the Software Process - A Maturity Framework,» Software Engineering Institute, USA, 1987.

[45] N. I. o. S. a. Technology, «https://www.nist.gov,» 09 05 2017. [En línea]. Available: https://www.nist.gov/sites/default/files/documents/2017/05/09/wb-spec-jan-07-1.pdf. [Último acceso: 10 Octubre 2021].

6

Anexos

6.1 Tabla 21: Modelo simplificado - Etapa preparativa.

Actividades / Documentación Técnica	Recepción del requerimiento	Revisión de capacidades	Definición del alcance	Equipamiento básico[30]	Planificación y diseño
RFC 3227/2002			●		●
SAI HB 171/2003		●	●		●
NIST 800-86-2006		●	●	●	●
US DoJ NCJ 219941/2008			●	●	●
ISFS/2009		●	●	●	●
ACPO/2012			●		●
ENISA/2014			●	●	
ISO/IEC 27037/2016	●	●	●		●
PGN 756/2016			●	●	●
MINSEG RES 234/2016			●		●

[30] Ver Anexo “Equipamiento básico para el primer interviniente”.

6.1.1 Equipamiento básico para el primer interviniente

6.1.1.1 Elementos para resguardo

El primer interviniente en el manejo de evidencia digital debe contar con un conjunto de herramientas que les permita arribar a la escena y recopilar la mayor cantidad de evidencia disponible, asegurando su integridad para una investigación posterior. Dicho equipamiento básico de herramientas debe incluir, entre otros, los siguientes elementos:

- Cámaras de fotografía y video: para capturar imágenes de la escena y registrar el estado de los elementos electrónicos.
- Un reloj digital: para utilizar como referencia, de modo que las marcas de tiempo sean visibles también como imagen y no solo como metadatos.
- Cajas de cartón o bolsas seguras de evidencia: aptas para recolectar, preservar la evidencia y su posterior transporte al laboratorio.
- Registros de inventario de evidencia, cinta de evidencia, bolsas, rótulos o etiquetas: crucial para garantizar la integridad y continuidad de la evidencia encontrada en la escena.
- Guantes: para protegerse contra los contaminantes presentes en la escena.
- Bolsas y equipos antiestáticos y kit de herramientas no magnéticas: para permitir la recolección segura de evidencia, protegiendo su integridad.

6.1.1.2 Equipamiento específico

Del mismo modo, en aquellos casos donde la adquisición de evidencias (físicas/lógicas) sea en la escena o exista una alta probabilidad de ello, es necesario que algunos equipos adicionales formen parte del equipamiento básico de herramientas, a saber:

- Computadora portátil con herramientas forenses que permita la adquisición en escena.
- Herramientas para obtener un volcado de memoria.
- Dispositivo de protección contra escritura forense para proteger evidencias digitales.

- Dispositivos para interceptar el tráfico de red puede ser necesario (hub/ switch).
- Cables de conexión necesarios.
- Medios desinfectados para almacenar imágenes de cualquier evidencia digital.

Como regla general, el equipamiento básico de herramientas de los primeros intervinientes en el manejo de evidencia digital, debe permitir recopilar evidencia digital de dispositivos estándar de PC / laptop, teléfonos móviles, tabletas, televisores inteligentes, consolas de juegos y todos los demás dispositivos modernos que contengan medios de almacenamiento digital. Cuando se trata de teléfonos móviles, se debe considerar usar bolsas de Faraday[31] para aislarlos y garantizar su preservación.

Cabe destacar que todo el equipo utilizado durante el trabajo forense debe ser apropiado para tal propósito y mantenido periódica y adecuadamente por consideraciones operativas, donde solo las herramientas, técnicas y procedimientos evaluados adecuadamente deben utilizarse para un examen forense, además que todos los medios utilizados para hacer copias forenses deben ser estériles.

[31] Elementos de resguardo especialmente diseñados para la recolección, preservación, transporte y análisis de dispositivos móviles e inalámbricos, para aislarlos de la red de comunicaciones y protegerlos contra descargas electrostáticas.

6.2 Tabla 22: Modelo simplificado - Etapa de identificación.

Actividades / Documentación Técnica	Tipos de infraestructura	Tipos de dispositivos	Categorización de posibles evidencias	Otras evidencias físicas	Requisitos previos a la adquisición
RFC 3227/2002		●	●		
SAI HB 171/2003	●	●			
NIST 800-86-2006	●	●	●		●
US DoJ NCJ 219941/2008	●	●	●		●
ISFS/2009	●	●	●	●	●
ACPO/2012	●	●			●
ENISA/2014	●	●	●		
ISO/IEC 27037/2016	●	●	●	●	●
PGN 756/2016		●	●		●
MINSEG RES 234/2016		●		●	●

6.3 Tabla 23: Modelo simplificado - Etapa de preservación[32].

Actividades / Documentación Técnica	Orden de volatilidad	Tipos Evidencia (Física/Lógica)	Algoritmos de seguridad	Consideraciones legales	Cadena de custodia[33]
RFC 3227/2002	●	●		●	●
SAI HB 171/2003	●	●			●
NIST 800-86-2006	●	●	●	●	●
US DoJ NCJ 219941/2008				●	●
ISFS/2009	●	●	●	●	●
ACPO/2012	●	●		●	
ENISA/2014	●		●	●	●
ISO/IEC 27037/2016	●	●	●	●	●
PGN 756/2016	●	●	●	●	●
MINSEG RES 234/2016			●	●	●

[32] Ver Anexo “Adquisición de imágenes Forenses”.

[33] Ver Anexo “Cadena de custodia”.

6.3.1 Adquisición de imágenes Forenses

6.3.2 Consideraciones generales

A continuación, se presenta la metodología general, independiente del sistema operativo empleado, con la finalidad de obtener este tipo de evidencias lógicas. Se recomienda preservar en todo momento la integridad y la autenticidad de información recolectada.

- Uso de herramientas forenses: los kits de herramientas forenses son herramientas especializadas, diseñadas para cumplir con los criterios de las investigaciones forenses. Permiten acceder y adquirir datos de manera que los cambios en los medios de origen son mínimos. Entre las diferentes opciones se encuentran desde aplicaciones de distribución libre y sistemas operativos de arranque de LiveCD en medios extraíbles, hasta aplicaciones comerciales de nivel empresarial.
- No realizar modificaciones: durante el proceso de preservación y recolección de evidencias lógicas, en la medida de lo posible, no se debe modificar, eliminar ni agregar datos en los medios de origen. Como ya se hubiera indicado, el empleo de herramientas forenses reducirá el impacto de esta actividad, dado que están diseñadas para acceder a los medios en un estado de solo lectura y no crearán ni modificarán archivos en los sistemas de origen, a menos que sea absolutamente necesario. Estas herramientas suelen publicar una lista que contiene los archivos que se modifican en caso de ser empleadas en un sistema "en vivo".
- Realizar el hash criptográfico: el uso de hash garantizará la autenticidad e integridad de las evidencias lógicas recolectadas a lo largo de la investigación forense. Todas estas deben ser hasheadas al momento de su recolección, transferencia y montaje para análisis. Los valores de hash deben registrarse en múltiples ubicaciones, como el registro del investigador forense y formularios de cadena de custodia.
- Documentar lo actuado: los investigadores forenses deben mantener registros detallados de las acciones que realizan durante el proceso de adquisición y recopilación. Si bien los registros se pueden crear y mantener,

ya sea en papel o en formato electrónico según la preferencia del investigador forense, cada opción tendrá un impacto en el proceso. Los registros de papel son menos susceptibles de ser manipulados o alterados, aun cuando es menos probable que contengan información técnica detallada, ya que debería ingresarse a mano. Los registros electrónicos pueden contener información técnica detallada, pero son menos tangibles, susceptibles de ser alterados, por lo cual resultan menos fiables. Sin embargo, la integridad de los registros electrónicos debe garantizarse mediante el cálculo hash correspondiente.

- Registrar y preservar la cadena de custodia: la cadena de custodia, en combinación con hash, resulta esencial para garantizar la autenticidad e integridad de la evidencia lógica recolectada. La cadena de custodia debe comenzar con la recolección de datos y mantenerse hasta su aceptación como evidencia.
- Realizar copias: una vez que la evidencia lógica es recolectada, la misma debe duplicarse y almacenarse en medios limpios, preferiblemente inalterables, como soportes ópticos en formato CD-R o DVD-R. A tal efecto, cada archivo de evidencia lógica debe ser hasheado de forma individual, para garantizar que dichas copias sean idénticas al original y se reflejen en la cadena de custodia. Se debe contar con al menos dos copias de la evidencia lógica recolectada, una para resguardo y otra para el análisis.

6.3.3 Bloqueadores de escritura

Existen una serie de requisitos generales que deben cumplir estos dispositivos, por ejemplo, la herramienta no debe permitir cambios en la unidad protegida, tampoco impedirá obtener información de o sobre cualquier unidad, ni ejecutar operaciones en las unidades que no estén protegidas [45].

6.3.3.1 Bloqueadores por hardware

Se tratan de dispositivos que permiten conectar una unidad de disco a un sistema informático mediante diferentes puertos (USB/E-SATA/FIREWARE), para obtener imágenes forenses del disco y garantizar que todas las operaciones de escritura en el disco se encuentren bloqueadas.

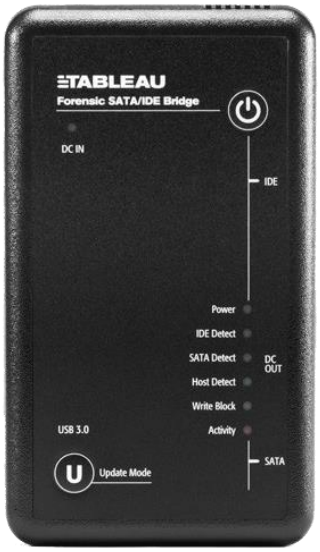

Ilustración 10: Bloqueador de escritura Tableau T35u (SATA/IDE)[34].

6.3.3.2 Bloqueadores por software

Básicamente, los bloqueadores por software permiten conectar una unidad de disco a un sistema informático mediante un puerto USB configurado en modo "solo lectura", para obtener de esta manera imágenes forenses del disco y garantizar que las operaciones de escritura en el disco se encuentren bloqueadas.

Si bien los puertos USB pueden configurarse de forma manual, por ejemplo mediante la herramienta Regedit[35], existen diferentes soluciones que realizan esta maniobra de forma automática.

Ilustración 11: Bloqueador de escritura Phrozen Safe USB v1.0[36].

[34] Bloqueador de escritura por hardware desarrollado por la firma Guidance Software.
[35] Regedit es el nombre de la herramienta que permite editar el registro del sistema operativo Windows. Este registro es la base de datos donde se guardan las preferencias del usuario en materia de configuraciones.
[36] Bloqueador de escritura por software freeare desarrollado por la firma Phrozen.

Cabe destacar que los bloqueadores de escritura de software y hardware realizan el mismo trabajo. Evitan escrituras en dispositivos de almacenamiento. La principal diferencia entre ambos es que los bloqueadores de escritura de software se instalan en una estación de trabajo informática forense, mientras que los bloqueadores de escritura de hardware tienen un software de bloqueo de escritura instalado en un chip controlador dentro de un dispositivo físico portátil. A continuación, se detallan ventajas y desventajas de las dos variantes planteadas.

BLOQUEADORES DE ESCRITURA POR HARDWARE	VENTAJAS	• No depende del sistema operativo subyacente. • Resulta más fácil de explicar a personas que no son técnicas. • Posee indicaciones visuales de la función a través de luces e interruptores físicos. • Por lo general proporciona interfaces para diferentes dispositivos de almacenamiento (IDE, SATA, etc.). • Parece ser más aceptado en la comunidad forense general.
	DESVENTAJAS	• Constituye un dispositivo adicional para transportar. • Requiere cierto mantenimiento. • Se encuentra limitado a las interfaces integradas en el dispositivo.

Tabla 24: Ventajas y desventajas de los bloqueadores de escritura por hardware.

BLOQUEADORES DE ESCRITURA POR SOFTWARE	VENTAJAS	• Se instala directamente en su estación de trabajo del investigador. • Utiliza las interfaces disponibles en la estación de trabajo del investigador, lo que evita gastos adicionales.
	DESVENTAJAS	• Podría necesitar adaptadores externos para interfaces nuevas. • Puede ser más difícil de explicar a personas no técnicas. • Siempre se debe comprobar su funcionalidad antes de conectar un dispositivo para análisis.

Tabla 25: Ventajas y desventajas de los bloqueadores de escritura por software.

6.3.4 Adquisición bajo entornos Windows y Linux

Como ya se hubiera indicado, la plataforma de trabajo se encontrará ligada a cada escenario posible, al igual que la experiencia del investigador forense, quien al final de cuentas definirá el entorno de trabajo de acuerdo a las necesidades imperantes, familiaridad con la herramienta forense empleada e incluso factores tales como la optimización de tiempo de trabajo.

6.3.4.1 Entorno Windows y uso de FTK Imager[37]

Posee una interfaz gráfica amigable. Se pueden obtener imágenes forenses en formato (DD, SMART, E01 y AFF).

Para realizar una imagen forense a partir de FTK Imager se deben seguir los siguientes pasos:

- Iniciar la aplicación, seleccionar la opción Archivo y luego, Crear Imagen de Disco.
- Seleccionar la unidad de origen (Disco físico/Disco lógico/Archivo de imagen/Contenido de una carpeta/Unidades ópticas tipo CD/DVD).
- Escoger el formato de la imagen forense (DD/SMART/E01/AFF).
- Completar datos relacionados al caso, evidencia e investigador.
- Acto seguido, se debe escoger la ruta de destino de la imagen forense, nombre de la misma, si se obtendrá un archivo único o la misma será spliteada en segmentos de determinado tamaño.
- A continuación, se debe chequear el origen y destino de la imagen forense, como así también seleccionar la verificación de la misma, para luego iniciar su obtención.
- Finalizado el proceso de obtención y comprobación, se aprecia un reporte con los algoritmos de seguridad hash (MD5/SHA1).
- Como resultado, en la ruta de destino se aprecian los archivos correspondientes a la imagen forense obtenida y su respectivo reporte.

[37] FTK Imager es una herramienta forense desarrollada por AccessData empleada, entre otras actividades, para la adquisición imágenes forenses.

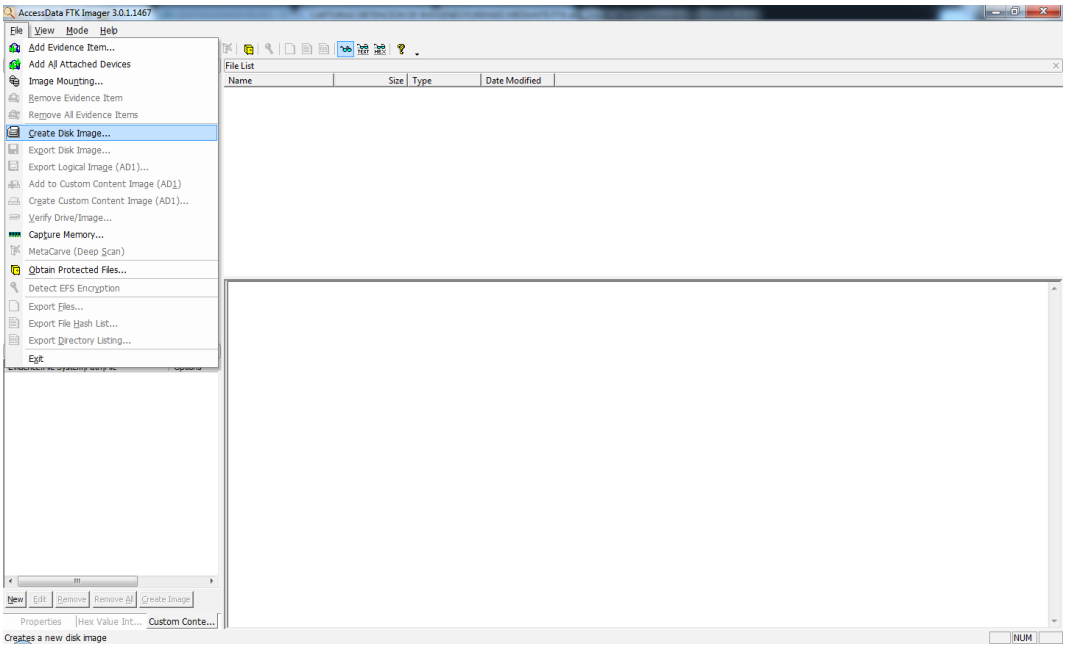

Ilustración 12: FTK Imager - Creación de imagen de disco.

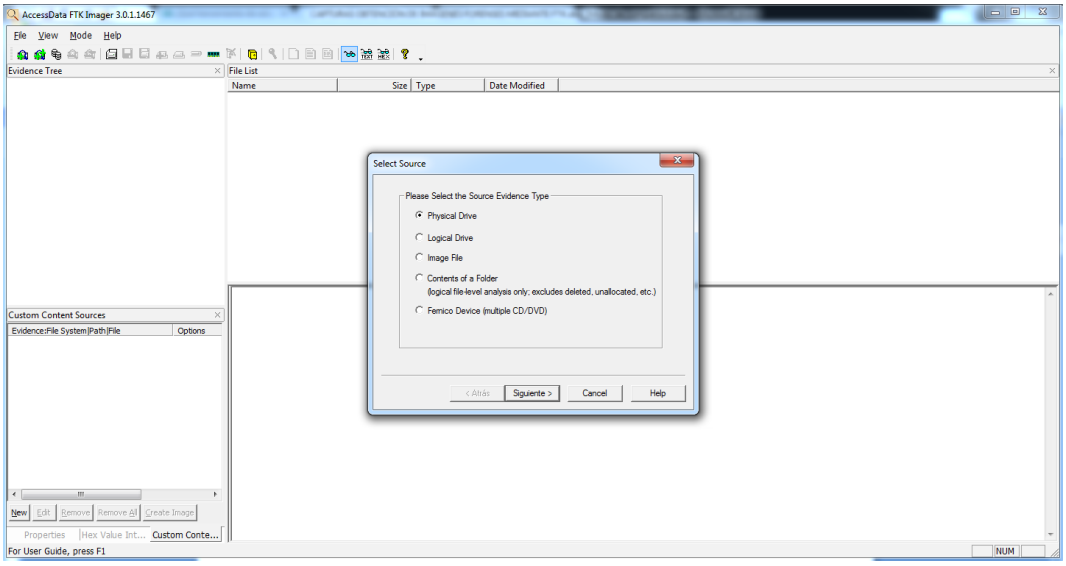

Ilustración 13: FTK Imager - Selección de tipo de origen.

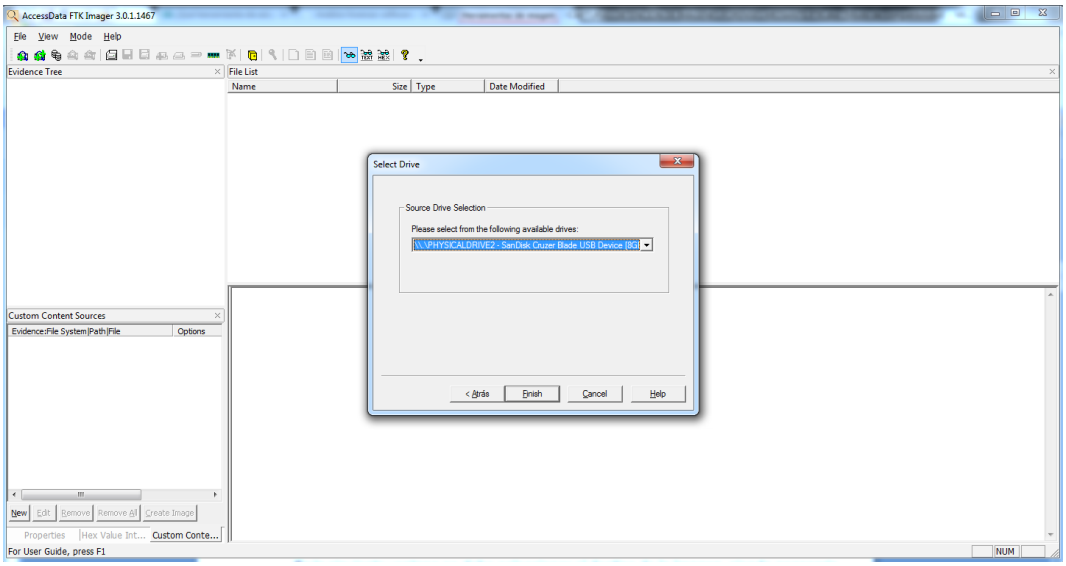

Ilustración 14: FTK Imager - Selección de disco de origen.

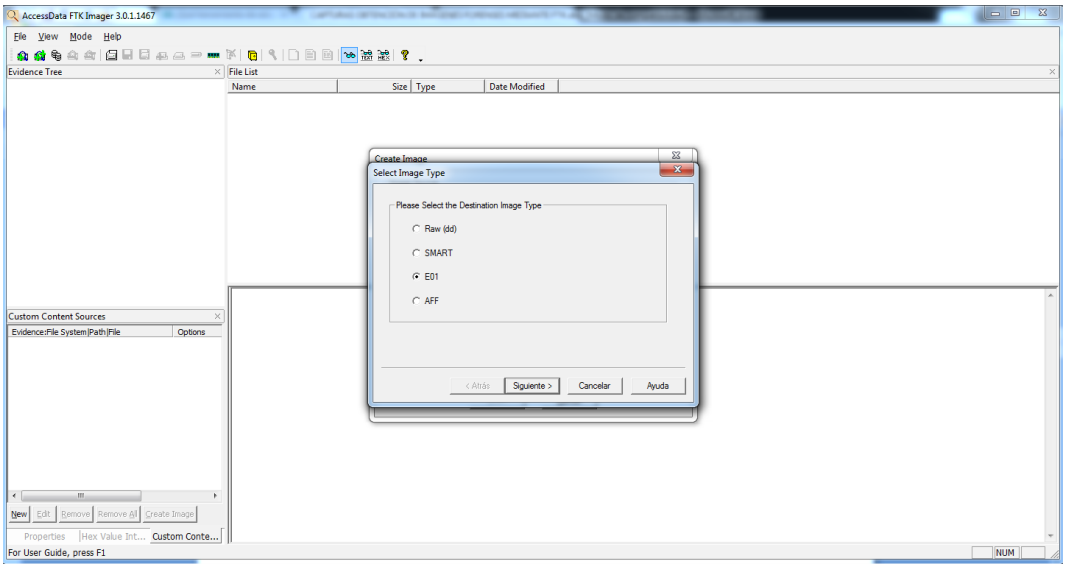

Ilustración 15: FTK Imager - Selección de formato de imagen.

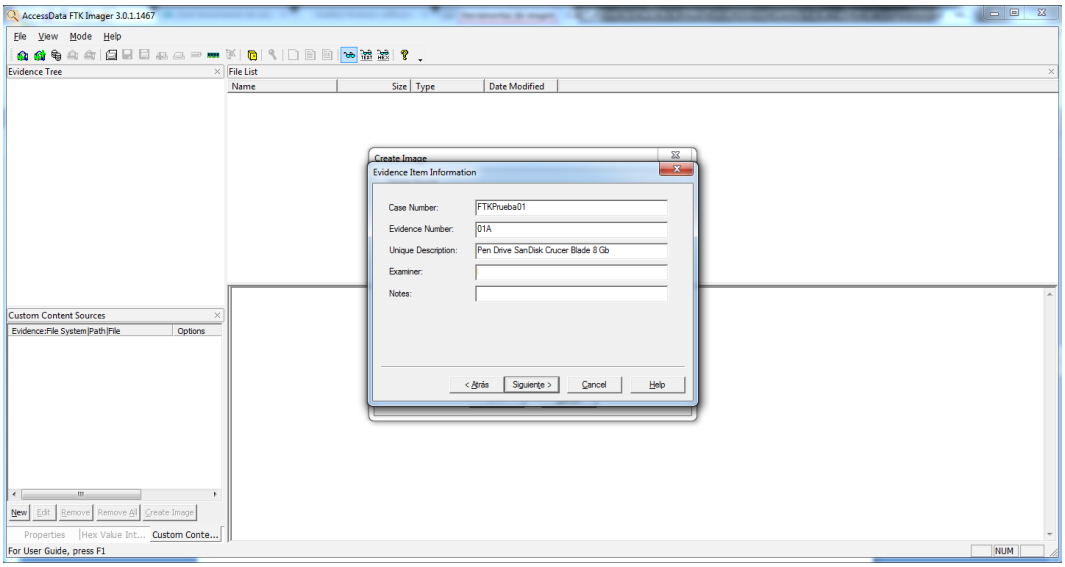

Ilustración 16: FTK Imager - Información de la evidencia.

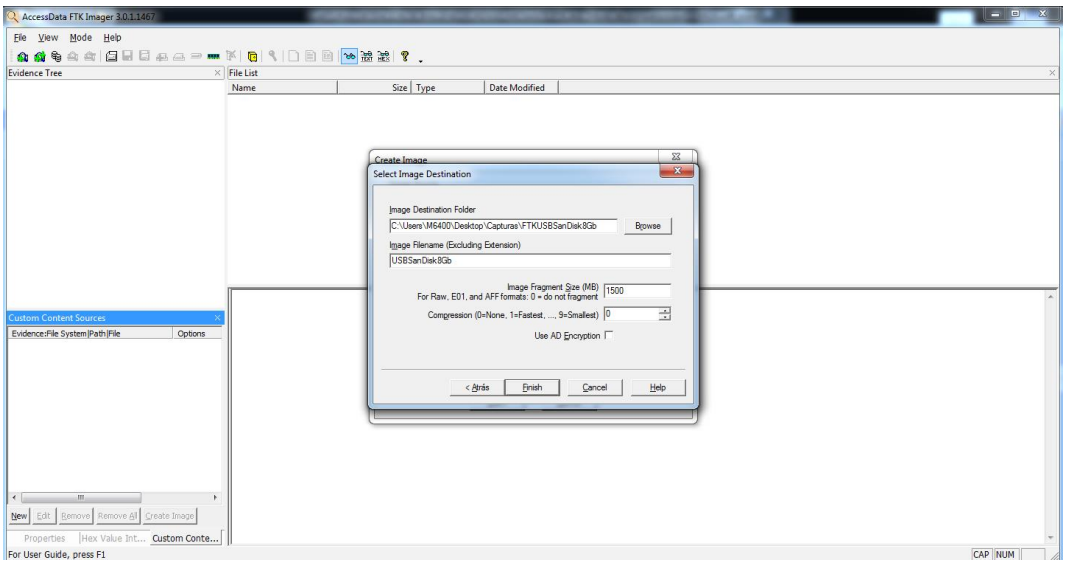

Ilustración 17: FTK Imager - Selección de ruta de destino.

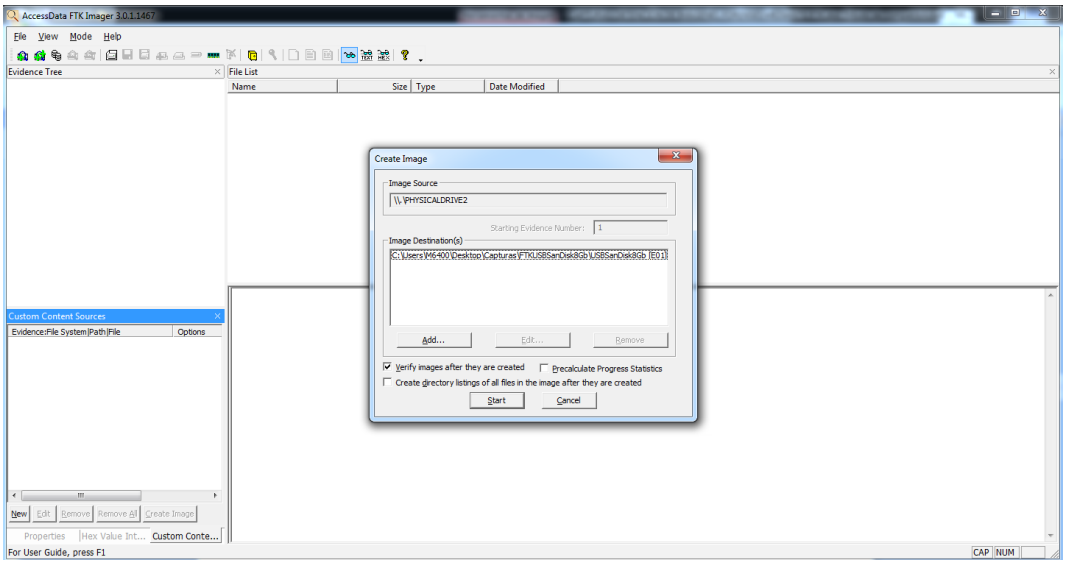

Ilustración 18: FTK Imager - Chequeo de parámetros y selección de verificación de la imagen.

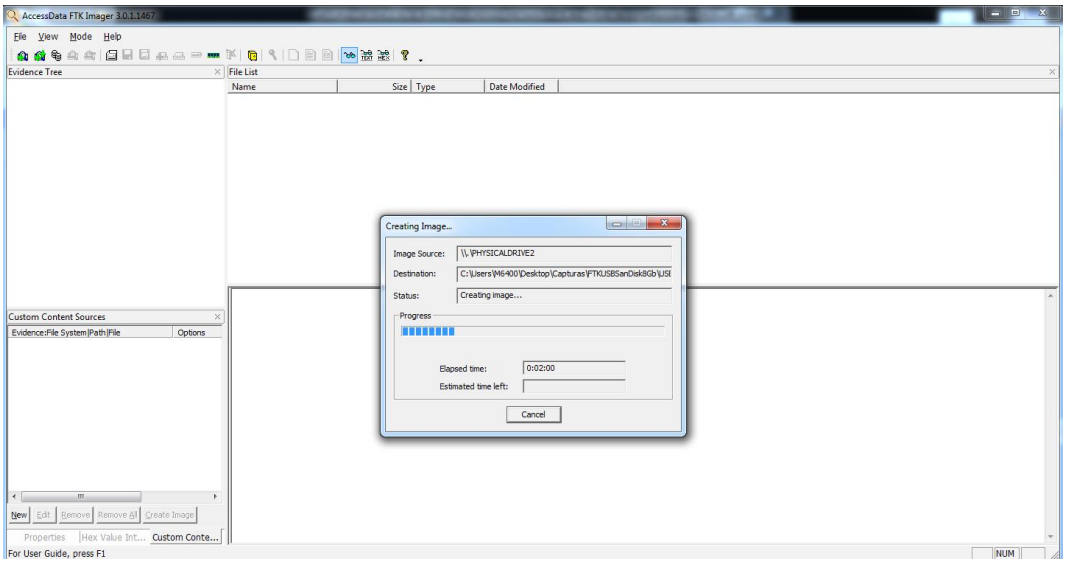

Ilustración 19: FTK Imager – Obtención de la imagen.

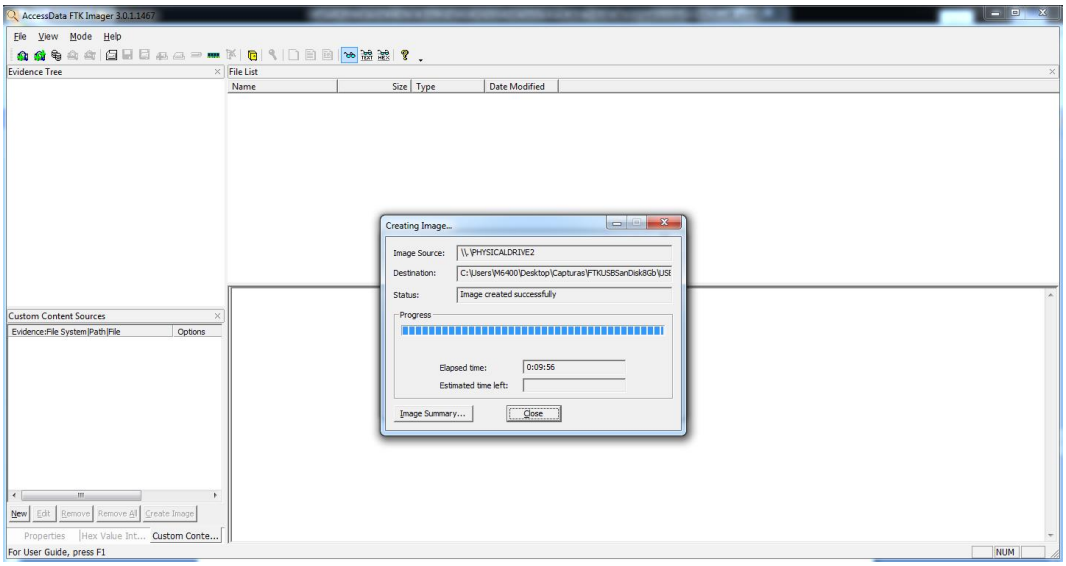

Ilustración 20: FTK Imager – Verificación de la imagen.

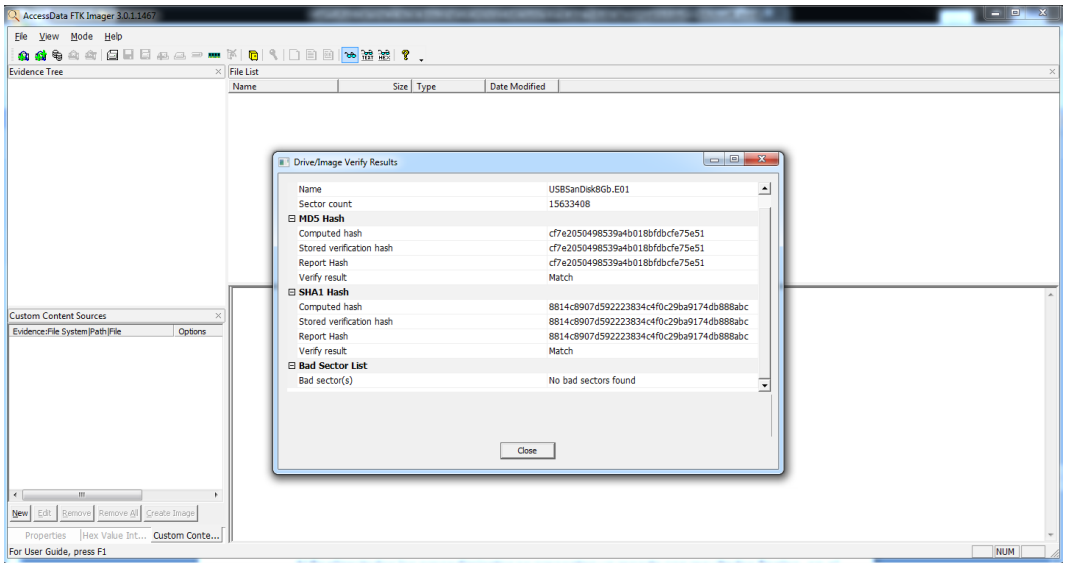

Ilustración 21: FTK Imager – Finalización del proceso.

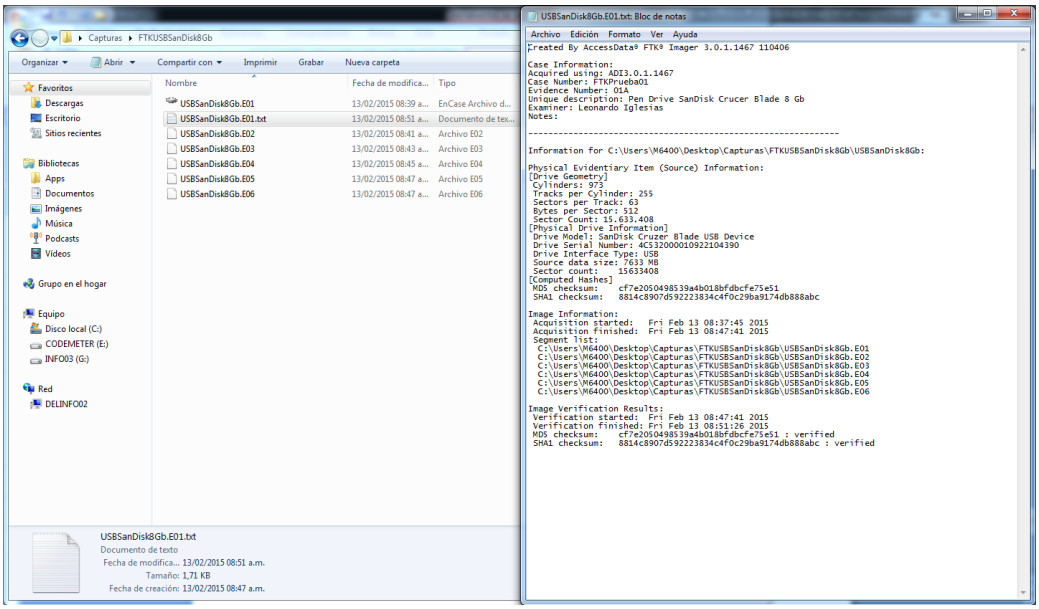

Ilustración 22: FTK Imager – Reporte correspondiente.

6.3.4.2 Entorno Linux - Uso de Guymager[38]

Posee una intuitiva interfaz gráfica y gran velocidad de copiado, debido a su diseño y eficaz uso de tecnología multiprocesador. Se pueden obtener imágenes forenses en formato DD y EWF (E01), además cuenta con la opción de duplicar discos. Para realizar una imagen forense a partir de Guymager se deben realizar los siguientes pasos:

- Iniciar la aplicación, seleccionar la unidad de origen y a partir del menú desplegable indicar la opción deseada (adquirir imagen o duplicar disco).
- Definir parámetros tales como formato de la imagen (DD/EWF), datos relacionados a la evidencia y caso de análisis, ruta de destino de la imagen forense, nombre de la misma, si se obtendrá un archivo único o la misma será spliteada[39] en segmentos de determinado tamaño. Asimismo, se puede seleccionar la habilitación para comprobación y cálculo de algoritmos de seguridad hash (MD5/SHA1/SHA256).
- Realizada esta configuración previa, se inicia el proceso de obtención de la imagen y se muestra en pantalla que se encuentra en ejecución.

[38] Guymager es una herramienta forense de fuente abierta para adquisición de imágenes forenses.
[39] Divisiones según capacidades preconfigurables por el usuario y generadas de forma automática por la herramienta forense.

- Finalizado el proceso, dicha actividad se visualiza en pantalla y como resultado, en la ruta de destino se aprecian los archivos correspondientes a la imagen forense obtenida y su respectivo reporte.

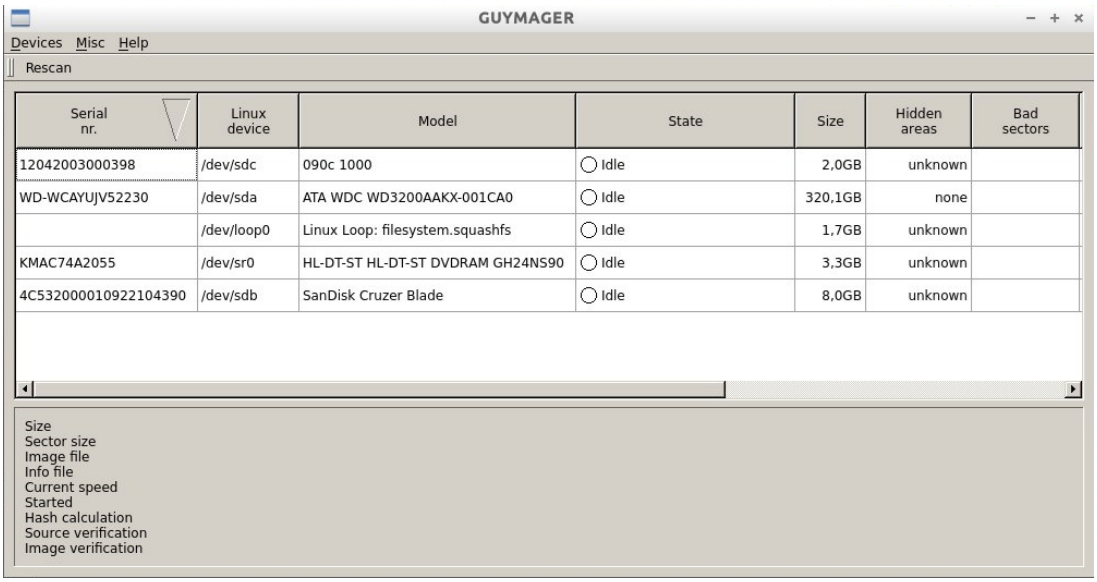

Ilustración 23: Guymager - Ventana de inicio.

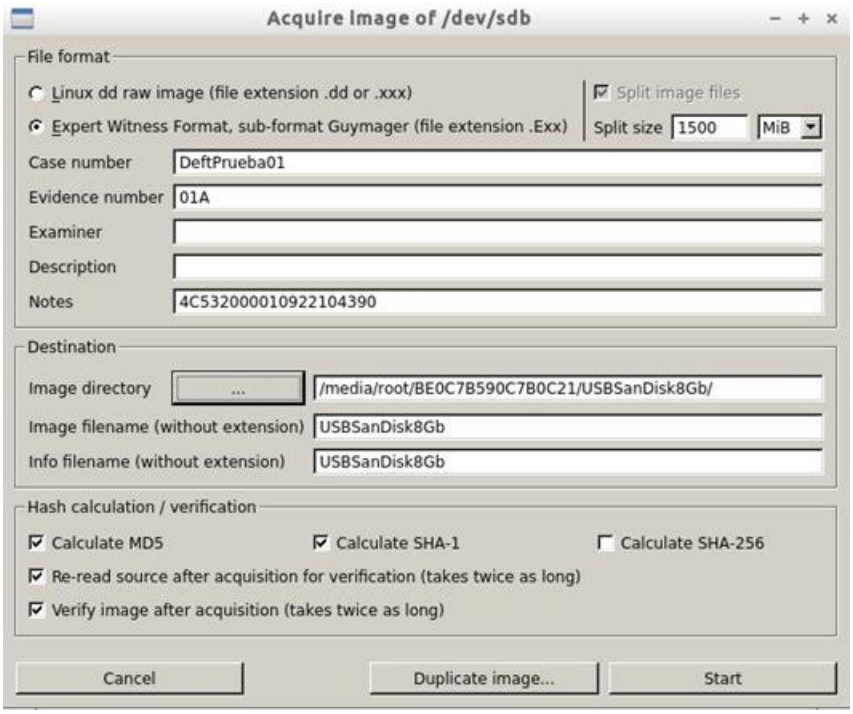

Ilustración 24: Guymager - Configuración de la Imagen.

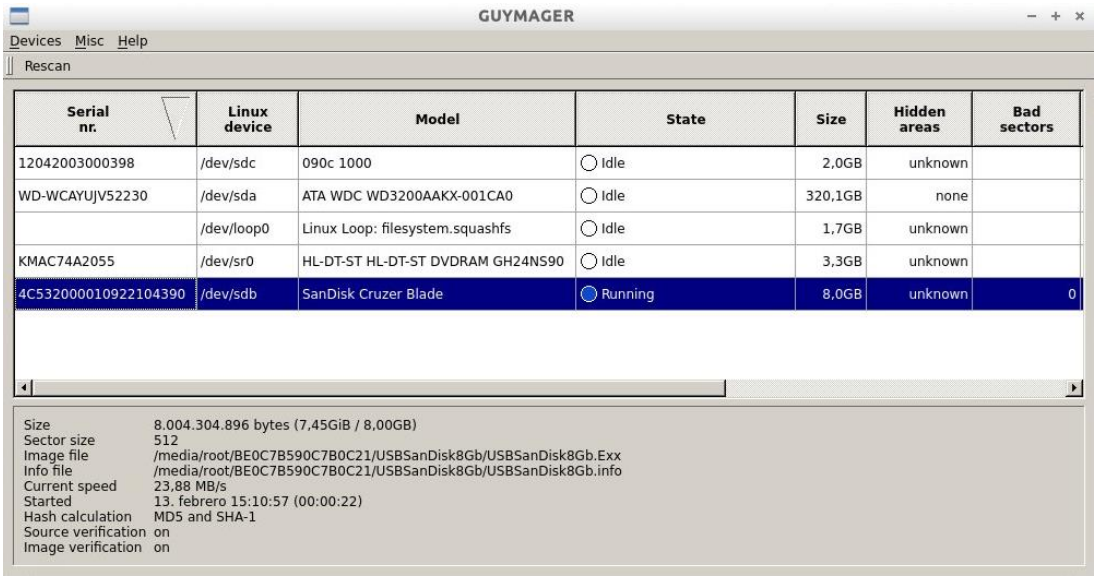

Ilustración 25: Guymager - Inicio de la adquisición.

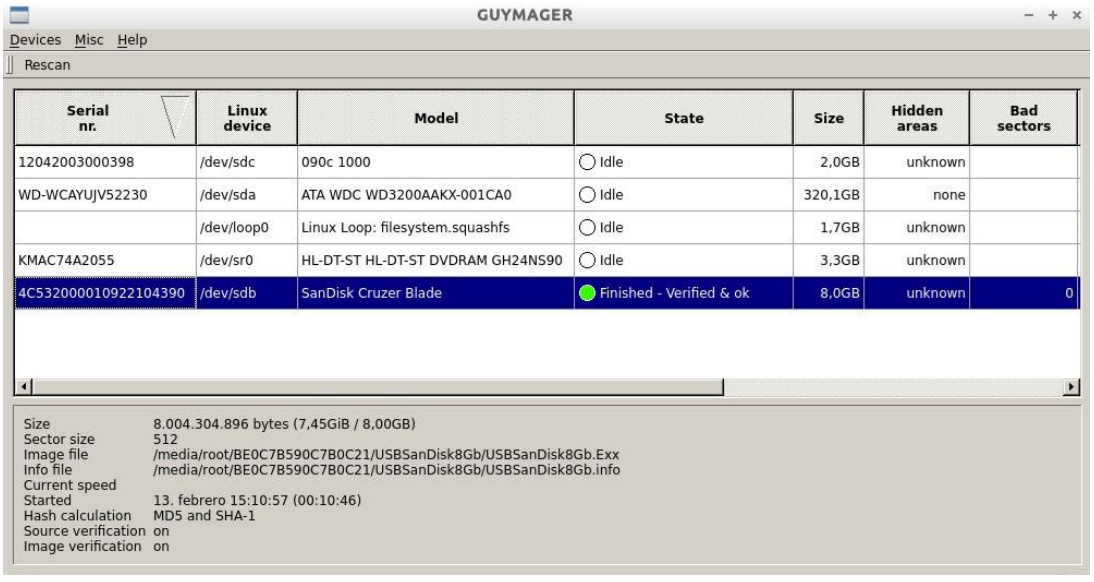

Ilustración 26: Guymager - Finalización de la adquisición.

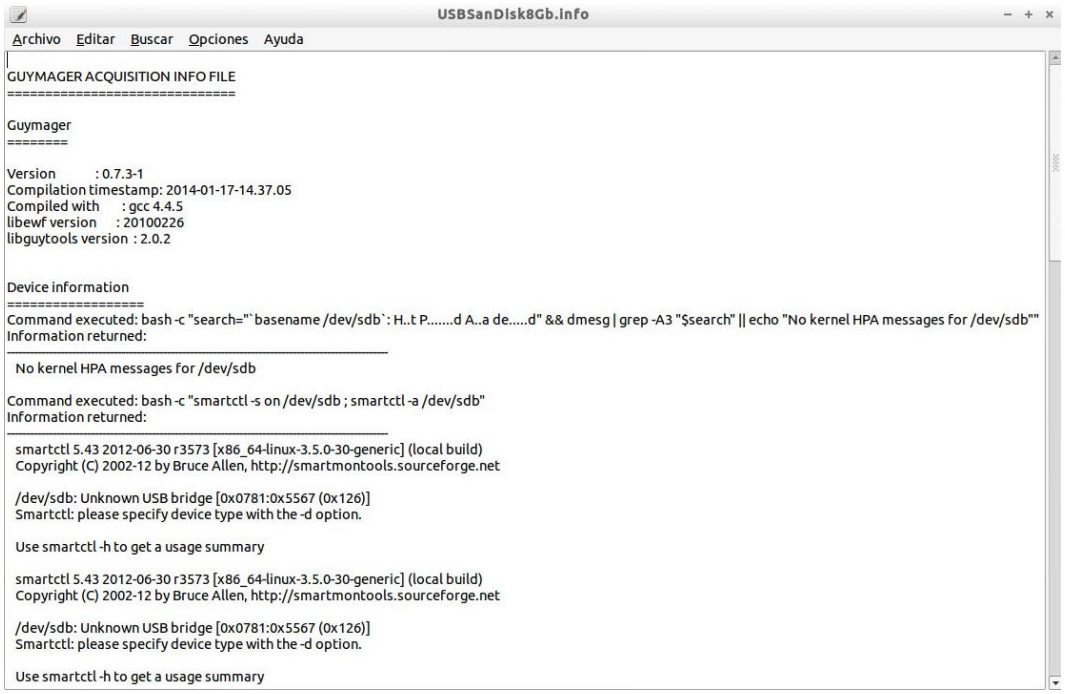

Ilustración 27: Guymager - Reporte de la imagen forense.

6.3.4.3 Entorno Linux - Comando DD[40]

Para ello, se ingresa código mediante consola. Se pueden obtener imágenes forenses en formato ISO, RAW (DD), la realización de imágenes forenses a partir del comando DD consta de los siguientes pasos:

- Abrir una consola de comando.
- Identificar el dispositivo de origen y sus respectivas tablas de partición mediante el comando “fdisk-l”.
- Calcular el algoritmo de seguridad hash del medio de origen (sdX) mediante el comando “sudo sha1sum /dev/sdc > /tmp/hash_sdc.sha1” y chequearlo mediante el comando “cat /hash_sdc.sha1”.
- Abrir una nueva consola y obtener la imagen del medio de origen mediante la herramienta “dd”, utilizar el comando “sudo dd if=/dev/sdX of=/tmp/sdZ.dd conv=noerror,sync”. Donde “if” indica la unidad de origen (sdX) y “of” la de destino (sdZ). Asimismo, el parámetro “conv” convierte el archivo de acuerdo a la lista de símbolos delimitados por comas, el parámetro “noerror”

[40] El comando DD, acrónimo de (Dataset Definition) es una herramienta provista por distribuciones Linux que, entre otras actividades, puede ser empleada para la adquisición imágenes forenses.

garantiza la continuidad de la operación aun cuando existan errores de lectura y por último “sync” se emplea para rellenar bloques con ceros en caso de error.

- Finalizado el proceso se aprecia un resumen con información de la actividad, como por ejemplo registros de ingreso y salida, bytes copiados, tiempo transcurrido para la obtención y promedio de la velocidad de copiado.
- A fin de realizar la comprobación de la imagen forense obtenida, se procede a calcular su algoritmo de seguridad hash mediante el comando “sha1sum /dev/sdZ.dd”.

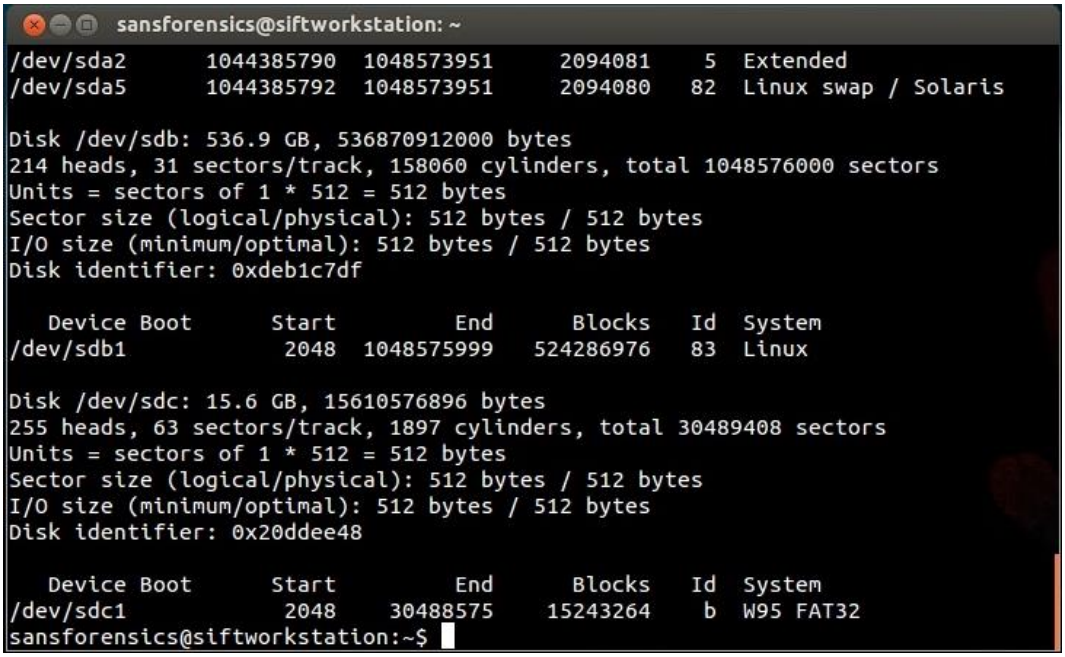

Ilustración 28: Comando DD - Identificación del medio de origen.

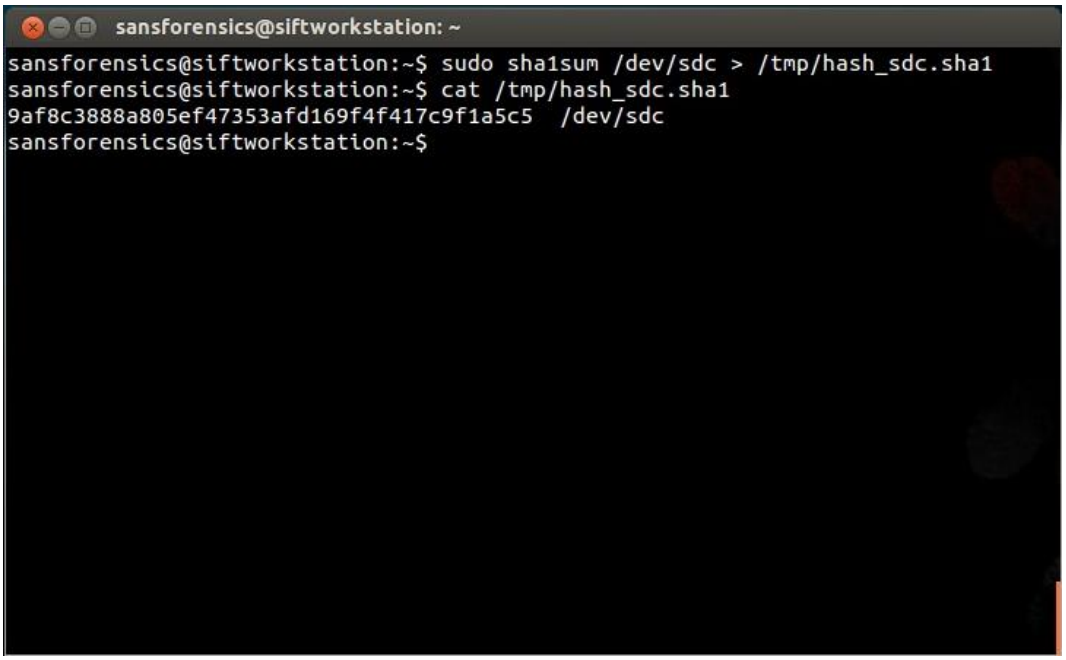

Ilustración 29: Comando DD - Hash SHA1 del medio de origen.

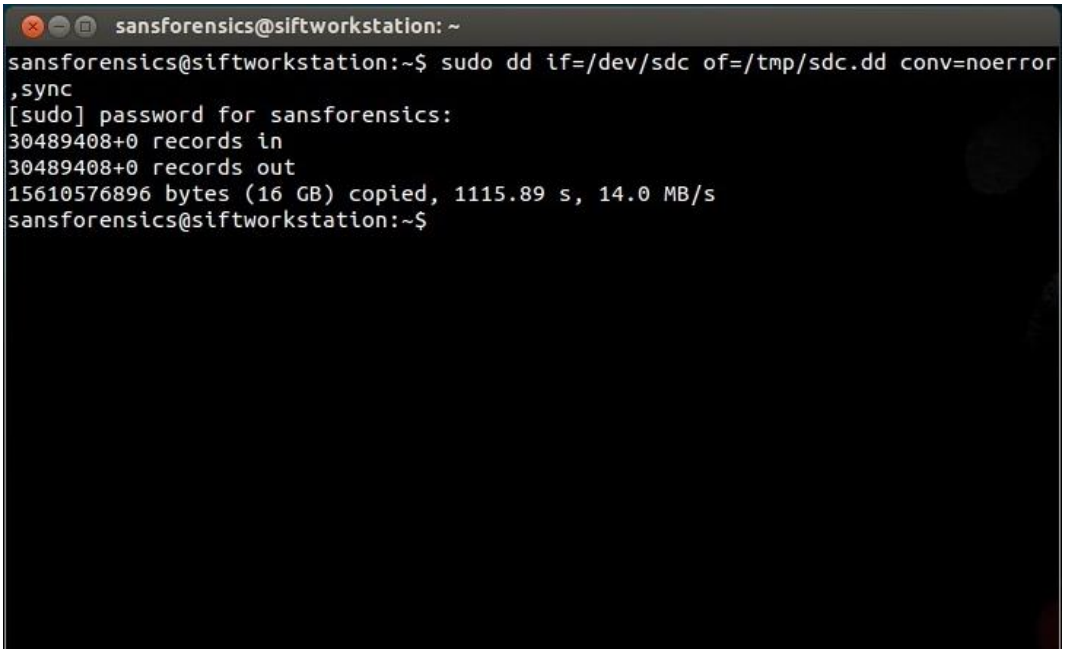

Ilustración 30: Comando DD - Obtención de la imagen forense y resumen.

```
sansforensics@siftworkstation: ~
sansforensics@siftworkstation:~$ sudo dd if=/dev/sdc of=/tmp/sdc.dd conv=noerror
,sync
[sudo] password for sansforensics:
30489408+0 records in
30489408+0 records out
15610576896 bytes (16 GB) copied, 1115.89 s, 14.0 MB/s
sansforensics@siftworkstation:~$ sha1sum /tmp/sdc.dd
9af8c3888a805ef47353afd169f4f417c9f1a5c5  /tmp/sdc.dd
sansforensics@siftworkstation:~$
```

Ilustración 31: Comando DD – Hash de la imagen forense.

```
sansforensics@siftworkstation: ~
sansforensics@siftworkstation:~$ sudo sha1sum /dev/sdc > /tmp/hash_sdc.sha1
sansforensics@siftworkstation:~$ cat /tmp/hash_sdc.sha1
9af8c3888a805ef47353afd169f4f417c9f1a5c5  /dev/sdc
sansforensics@siftworkstation:~$

sansforensics@siftworkstation: ~
sansforensics@siftworkstation:~$ sudo dd if=/dev/sdc of=/tmp/sdc.dd conv=noerror
,sync
[sudo] password for sansforensics:
30489408+0 records in
30489408+0 records out
15610576896 bytes (16 GB) copied, 1115.89 s, 14.0 MB/s
sansforensics@siftworkstation:~$ sha1sum /tmp/sdc.dd
9af8c3888a805ef47353afd169f4f417c9f1a5c5  /tmp/sdc.dd
sansforensics@siftworkstation:~$
```

Ilustración 32: Comando DD – Comprobación de la imagen forense.

6.3.5 Adquisición de dispositivos móviles

El contenido de la memoria de un dispositivo móvil a menudo contiene información, como datos eliminados, cuya accesibilidad dependerá del tipo de adquisición realizada por parte del investigador forense.

Podría decirse que existe un orden jerárquico en función de la complejidad del tipo de técnica empleada para la adquisición de evidencias móviles.

6.3.5.1 Evidencia Lógica en móviles

Dicha técnica copia los objetos almacenados en la memoria del dispositivo móvil, sincronizando la terminal con una estación de trabajo mediante mecanismos dispuestos originalmente por el fabricante.

La conexión puede ser realizada por un medio físico (Cable USB) o inalámbrico (WiFi), solicitando al sistema operativo del dispositivo móvil que envíe la información requerida por el examinador.

Como ventaja podemos indicar la sencillez de dicho proceso, aunque por el otro lado ofrece una cantidad acotada de información.

6.3.5.2 Evidencia Física en móviles

Este método es el todo analista forense prefiere a la hora de iniciar el análisis forense de un dispositivo móvil, dado que permite efectuar una imagen forense idéntica del original, preservando la totalidad evidencias que podrían encontrarse almacenadas en memoria.

Como ventaja podríamos citar que a partir de esta técnica resulta factible recuperar elementos eliminados, pero en contrapartida es un procedimiento complejo en relación con otros métodos, al igual que su procesamiento conlleva una mayor inversión de tiempo.

6.3.5.3 Chip-OFF[41]

Esta extracción requiere remover físicamente la memoria flash, proporcionando a los examinadores forenses la capacidad de crear una imagen binaria del chip removido, que una vez completada puede ser analizada.

Este tipo de adquisición es el que se podría asemejar a los métodos de adquisición directa relacionado con las imágenes físicas de unidades de disco duro como en el análisis forense digital tradicional.

Asimismo, este tipo de técnicas requieren una amplia capacitación para realizar operaciones exitosas, constituyendo un desafío por la amplia variedad de

[41] Los métodos de chip-off se refieren a la adquisición de datos directamente desde la memoria flash de un dispositivo móvil.

tipos de chips, formatos de datos sin procesar y el riesgo de causar daño físico al chip durante el proceso de extracción.

6.3.5.4 JTAG[42]

Por medio de esta interfaz los examinadores forenses pueden comunicarse con un componente compatible con JTAG utilizando dispositivos programadores independientes diseñados especialmente para testear puntos de prueba definidos.

JTAG ofrece a los especialistas otra vía para obtener la imagen de dispositivos bloqueados, con daños menores o que no pueden interconectarse adecuadamente de otra manera.

El método consiste en conectar una interfaz física o arnés de cableado desde una estación de trabajo a la interfaz JTAG del dispositivo móvil y acceder a la memoria a través de su microprocesador para obtener una imagen forense.

Las extracciones de JTAG son invasivas, dado que para su acceso y conexiones de cableado se requiere desmontar parte de un dispositivo móvil.

Las denominadas Flasher Box son dispositivos diseñados originalmente para actividades de reparación o actualización de dispositivos móviles, las que en la actualidad son utilizadas para realizar adquisiciones físicas, acompañadas de software para facilitar al acceso de datos. Entre sus limitaciones podemos señalar:

- Se requiere con frecuencia el reinicio del dispositivo móvil para comenzar el proceso de extracción, lo que incrementa las posibilidades de activar mecanismos de autenticación impidiendo un análisis más profundo.
- Muchas Flash Box recuperan datos en formato encriptado, requiriendo que el examinador forense deba utilizar software provisto por el fabricante de la caja para descifrar la información o incluso utilizar técnicas de ingeniería inversa por parte del analista.
- Muchos modelos de teléfonos no proporcionan la adquisición de todo el rango de memoria, encontrándose disponibles solo ciertas porciones lo que implica un volcado parcial de información.

[42] La mayoría de los fabricantes admiten el estándar JTAG (Joint Test Action Group), que define una interfaz de prueba común para procesadores, memorias y otros tipos de chips semiconductores.

- La falta de documentación sobre el uso de estas herramientas es común, por cuanto los métodos de extracción se comparten de manera informal, por ejemplo, mediante foros moderados por usuarios más experimentados.

A pesar de estas limitaciones, el uso de Flash Boxs es una opción viable para muchos casos forenses, donde la capacitación adecuada, experiencia y comprensión de su funcionamiento son claves de éxito.

El uso de esta técnica requiere una amplia gama de experiencia y una capacitación adecuada para extraer y analizar imágenes binarias con estos métodos, que incluyen la ubicación y la conexión a puertos JTAG, la creación de cargadores de arranque personalizados y la recreación de sistemas de archivos.

6.3.6 Cadena de custodia

6.3.6.1 Anverso

PLANILLA DE CADENA DE CUSTODIA			
DATOS DEL LUGAR	LUGAR: FECHA: HORA:		
	UNIDAD INTERVINIENTE:		
	JUZGADO/FISCALÍA:		
	SECRETARIA:		
	CARÁTULA:		
	SUMARIO/CAUSA NRO:		
	OBSERVACIONES:		
ELEMENTOS	**ELEMENTOS SECUESTRADOS**		
	DESCRIPCIÓN:		
	LUGAR DE RECOLECCIÓN:		
	MODO DE CONSERVACIÓN: SOBRE DE PAPEL CAJA CARTÓN BOLSA PLÁSTICA OTROS:		
	MODO DE TRASLADO:		
	DESTINO:		
TESTIGOS	**NOMBRES Y APELLIDO**	**D. N. I.**	**FIRMA**
1			
2			
PRIMER INTERVINIENTE			
COLECTADO POR	NOMBRES Y APELLIDO	HORA Y FECHA	FIRMA
	CARGO:		

6.3.6.2 Reverso

ENTREGA	NOMBRES Y APELLIDO	GRADO - CE- LP - DNI	FIRMA
RECIBE			
MOTIVO DE ENTREGA: CUSTODI☐	TRASL☐DO	P☐RITAJE	D☐STRUCCIÓN
FECHA / HORA: OBSERVACIONES:			
ENTREGA	NOMBRES Y APELLIDO	GRADO - CE- LP - DNI	FIRMA
RECIBE			
MOTIVO DE ENTREGA: CUSTODI☐	TRASL☐DO	P☐RITAJE	D☐STRUCCIÓN
FECHA / HORA: OBSERVACIONES:			
ENTREGA	NOMBRES Y APELLIDO	GRADO - CE- LP - DNI	FIRMA
RECIBE			
MOTIVO DE ENTREGA: CUSTODI☐	TRASL☐DO	P☐RITAJE	D☐STRUCCIÓN
FECHA / HORA: OBSERVACIONES:			
ENTREGA	NOMBRES Y APELLIDO	GRADO - CE- LP - DNI	FIRMA
RECIBE			
MOTIVO DE ENTREGA: CUSTODI☐	TRASL☐DO	P☐RITAJE	D☐STRUCCIÓN
FECHA / HORA: OBSERVACIONES:			
ENTREGA	NOMBRES Y APELLIDO	GRADO - CE- LP - DNI	FIRMA
RECIBE			
MOTIVO DE ENTREGA: CUSTODI☐	TRASL☐DO	P☐RITAJE	D☐STRUCCIÓN
FECHA / HORA: OBSERVACIONES:			

6.4 Tabla 26: Modelo simplificado - Etapa de análisis.

Actividades / Documentación Técnica	Lista de artefactos forenses	Línea de tiempo	Firmas de archivo	Palabras clave	Técnicas y herramientas para procesamiento
RFC 3227/2002					
SAI HB 171/2003					
NIST 800-86-2006	●	●	●	●	●
US DoJ NCJ 219941/2008	●		●		
ISFS/2009	●	●			
ACPO/2012	●			●	
ENISA/2014	●	●	●	●	
ISO/IEC 27037/2016					
PGN 756/2016					●
MINSEG RES 234/2016	●			●	

6.4.1 Herramientas Forenses

Una vez efectuada la obtención de imágenes forenses, acompañadas de sus respectivos algoritmos de seguridad hash y cadenas de custodia, se da paso al análisis de la información contenida en las evidencias recolectadas.

En tal sentido, el análisis forense digital debe cumplimentar los requisitos periciales objeto de la investigación e identificar aquellos artefactos forenses de interés, para su posterior presentación mediante los informes correspondientes.

Existen diferentes herramientas informáticas de amplio reconocimiento en la comunidad científica, las cuáles desempeñan funciones específicas.

6.4.1.1 Autopsy

Plataforma forense digital con interfaz gráfica de la firma The Sleuth Kit. Es utilizado por los encargados de hacer cumplir la ley, militares e investigadores forenses corporativos, cuyas principales características se listan a continuación:

- Múltiples sistemas operativos: posee versiones tanto para Windows como para Linux.
- Casos multiusuario: posibilidad de colaborar con otros investigadores forenses en casos con gran volumen de información.
- Análisis de línea de tiempo: muestra los eventos del sistema mediante una interfaz gráfica que facilita la identificación de actividad en disco.
- Búsqueda de palabras clave: permite la búsqueda mediante términos específicos, indexación e incluso patrones de expresiones regulares.
- Artefactos web: recolecta actividad web de los navegadores y permite identificar la actividad de cada usuario.
- Análisis del registro: utiliza RegRipper para identificar los documentos y dispositivos USB a los que se accedió recientemente.
- Análisis de archivos LNK: identifica accesos directos y documentos accedidos recientemente.
- Análisis de correo electrónico: soporta el formato MBOX, como por ejemplo Thunderbird.

- EXIF: permite extraer la ubicación geográfica e información de la cámara mediante archivos JPEG.
- Clasificación de tipo de archivo: permite agrupar los archivos por tipo para separar rápidamente imágenes o documentos.
- Reproducción de medios: videos e imágenes se reproducen en la aplicación sin la necesidad de un visor externo.
- Visor de miniaturas: muestra miniaturas de las imágenes para una visualización rápida.
- Análisis del sistema de archivos robusto: soporte para sistemas de archivo comunes, incluyendo NTFS, FAT12 / FAT16 / FAT32 / ExFAT, HFS +, ISO9660 (CD-ROM), Ext2 / Ext3 / Ext4, yaffs2 y UFS del kit de detective.
- Filtro de conjunto de hash: permite eliminar los archivos buenos conocidos. Utiliza NSRL y marca archivos maliciosos conocidos. Para ello usa hashsets personalizados en los formatos HashKeeper, md5sum y EnCase.
- Etiquetas: facilita el etiquetado de archivos con nombres arbitrarios, como 'favoritos' o 'sospechosos', y agregar comentarios.
- Extracción de cadenas Unicode: permite extraer cadenas de espacios no asignados y tipos de archivos desconocidos en diferentes idiomas (árabe, chino, japonés, etc.).
- Soporta la detección de tipos de archivo mediante firmas digitales y detección de desajuste de extensión.
- Compatibilidad con Android: extrae datos de SMS, registros de llamadas, contactos, diccionario y más.

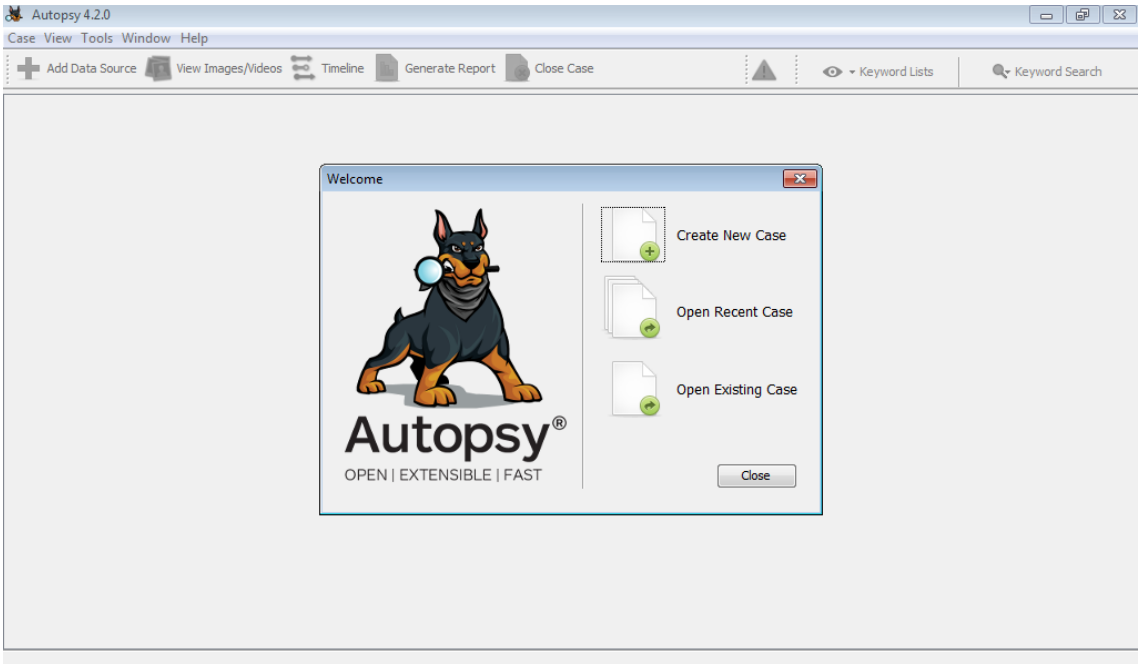

Ilustración 33: Herramienta forense Autopsy.

6.4.1.2 Digital Forensics Framework (DFF)

Framework forense empleado por investigadores forenses corporativos, examinadores encargados de hacer cumplir la ley, estudiantes forenses digitales y profesionales de la seguridad en todo el mundo. Escrito en Python y C ++. DFF combina una interfaz de usuario intuitiva con un diseño modular y multiplataforma. A continuación, se enumeran sus principales características:

- Interfaz de usuario: explorador de archivos, marcadores, ventanas acoplables, entorno de desarrollo integrado e intérprete (Python), línea de comando, multilenguaje, administrador de tareas.
- Visores: imágenes, videos, texto, web, estadísticas de sistemas de archivos.
- Análisis de línea de tiempo: vista gráfica, extracción virtual y reducción, filtros de metadatos.
- Visor hexadecimal: compatibilidad con archivos grandes, navegación de página, navegación y visualización de píxeles, búsqueda, etc.
- Volúmenes: particiones, VMDK (VMware).
- Manipulación de ficheros: corte, fusión, extracción, reducción de repuestos.

- Metadatos: EXIF, día y fecha, estructuras de datos, etc.
- Memoria volátil: Windows XP (Volatility).
- Sistemas de archivos: FAT 12/16/32, NTFS, EXTFS 2/3/4.
- Recuperación de datos: algoritmos de sistemas de archivos, tallado de archivos.
- Registro de Windows: reconstrucción y análisis.
- Otro: dispositivos locales, hash (md5, sha *), zip, unxor.

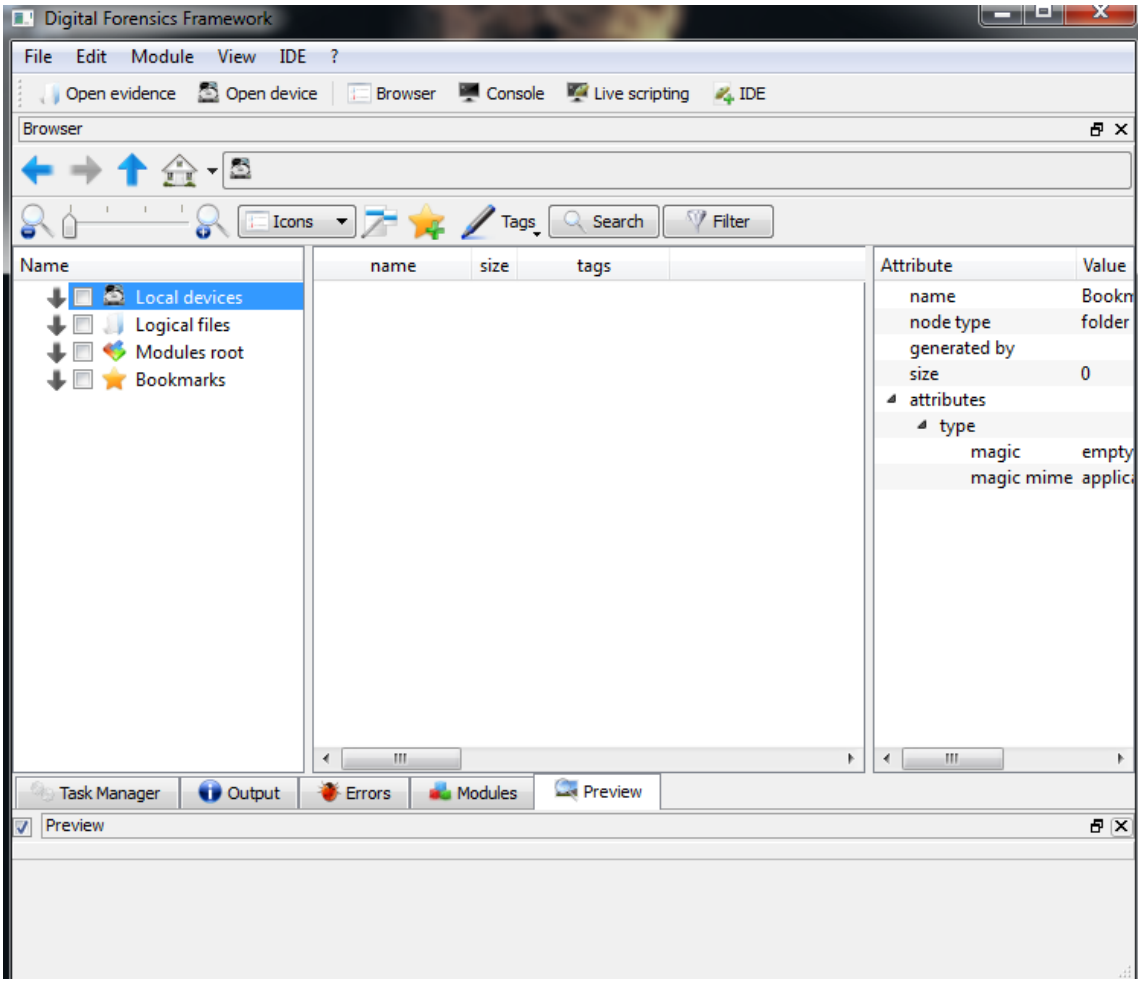

Ilustración 34: Herramienta forense Digital Forensics Framework.

6.4.1.3 Bulk Extractor

Software forense que extrae funciones tales como direcciones de correo electrónico, números de tarjetas de crédito, URL y otros tipos de información de archivos de pruebas digitales. A continuación, se listan sus principales características:

- Permite el análisis de direcciones de correo electrónico, URL y números de tarjetas de crédito.
- Puede manejar datos comprimidos (como archivos ZIP, PDF y GZIP), así como datos incompletos o parcialmente corruptos, relevar archivos JPEG, documentos de ofimática y otros tipos de archivos a partir de fragmentos de datos comprimidos. Puede detectar y extraer automáticamente archivos RAR encriptados.
- Soporta la creación de listas de palabras basadas en todas las palabras encontradas en los datos, incluso archivos comprimidos que no tienen espacio asignado. Estas listas de palabras se pueden usar para descifrar contraseñas.
- Permite multiproceso para optimizar el tiempo de análisis.
- Después del análisis, crea un histograma con la información relevada.
- Soporta el análisis de imágenes de disco, archivos o directorios de archivos y recolección de información sin analizar el sistema de archivos o la estructura del sistema de archivos.
- Posee un visualizador con funciones de exploración e interfaz gráfica.
- Contiene una suite de programas en Python para análisis adicional.

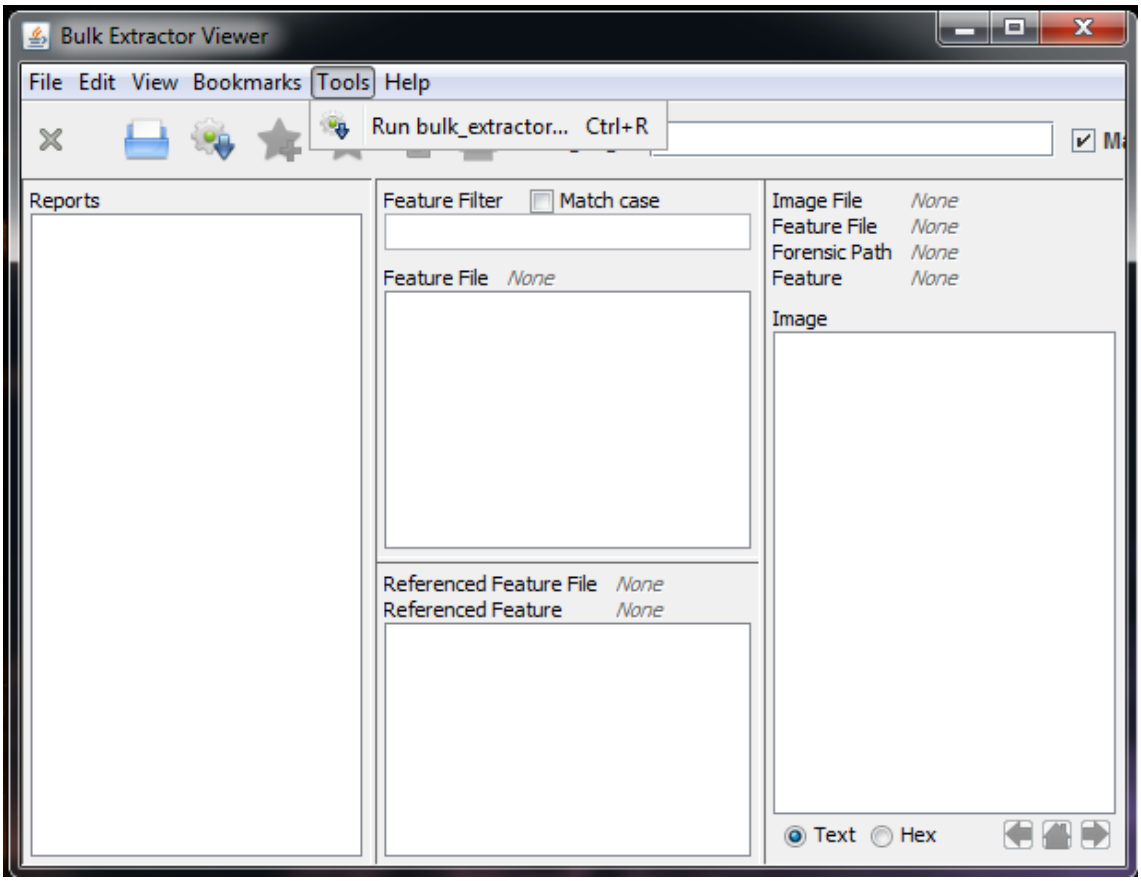

Ilustración 35: Herramienta forense Bulk Extractor.

6.4.1.4 DEFT

Acrónimo de Digital Evidence and Forensics Toolkit, es una distribución Linux basada en Ubuntu. Desarrollada para el análisis forense digital, con el propósito de analizar sistemas en vivo sin alterar o contaminar los dispositivos de almacenamiento conectados a la PC donde se lleva a cabo el proceso de arranque. Actualmente es utilizado por personal militar, oficiales del gobierno, fuerzas del orden, investigadores forenses corporativos, auditores de TI, universidades, entre otros. Sus principales capacidades se detallan a continuación:

- Multiplataforma: puede ejecutarse en vivo (mediante DVD-R o pendrive USB), instalarse o ejecutarse como un dispositivo virtual en VMware o Virtualbox.
- Soporta herramientas de análisis de ficheros de diferentes tipos.
- Contiene antimalware para búsqueda de rootkits, virus, malware.

- Posee software para la recuperación de ficheros.
- Permite la realización de cálculo de hashes de diferentes formatos: SHA1, SHA256, MD5.
- Contiene aplicaciones para realizar clonados y adquisición de imágenes de discos duros u otros orígenes.
- Permite el análisis forense de dispositivos móviles.

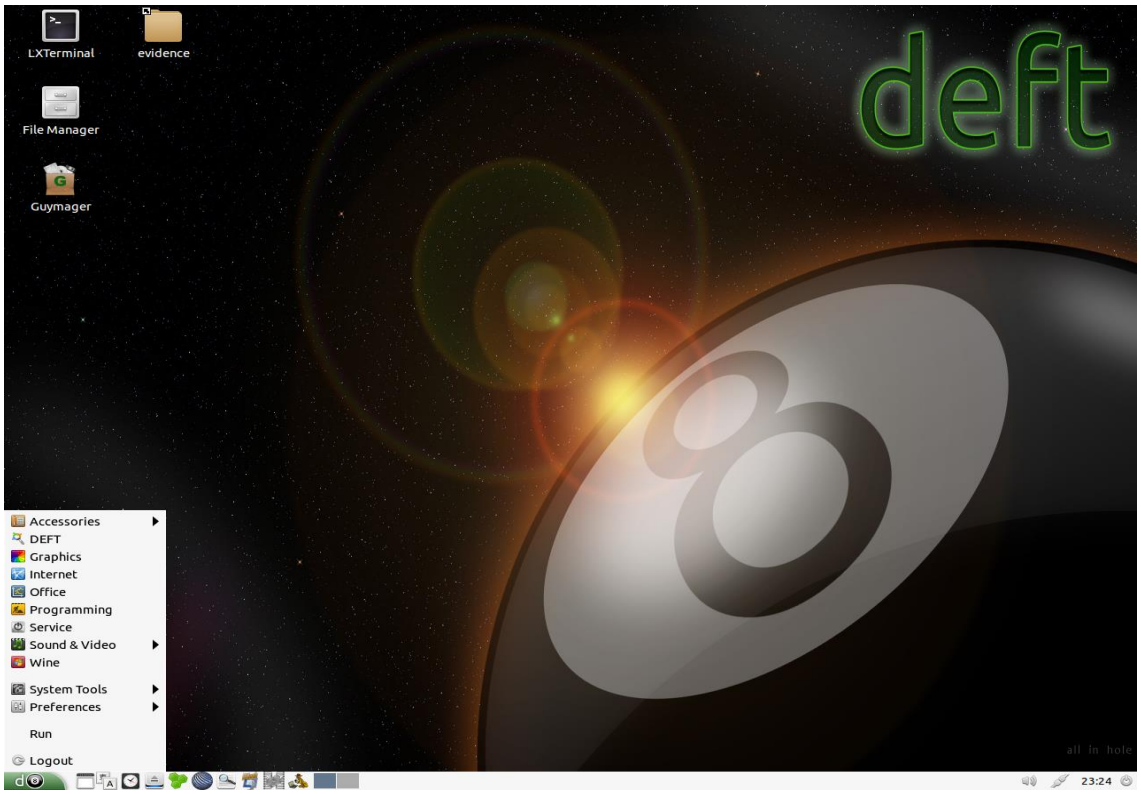

Ilustración 36: Herramienta forense DEFT.

6.4.1.5 CAINE

Acrónimo de Computer Aided Investigative Environment, es una distribución Linux basada en Ubuntu, desarrollada para el análisis forense digital con el propósito de ofrecer un entorno forense completo y organizado para integrar herramientas y módulos de software. Proporciona una interfaz gráfica amigable. Actualmente es utilizado por personal militar, fuerzas del orden, investigadores forenses corporativos, auditores de TI, entre otros. A continuación, se listan sus principales características:

- Multiplataforma: puede ejecutarse en vivo (mediante DVD-R o pendrive USB), instalarse o ejecutarse como un dispositivo virtual en VMware o Virtualbox, tanto en Linux como Windows.
- Permite el apoyo a las investigaciones mediante un entorno que ayuda al investigador en las cuatro fases del cómputo forense.
- Se encuentra provista de una interfaz gráfica amigable.
- Posee un kit de herramientas forenses cuyo empleo no resulta dificultoso.
- Entre tales herramientas se encuentran: Nirsoft suite, WinAudit, MWSnap, Arsenal Image Mounter, FTK Imager, Hex Editor, JpegView, herramientas de red, NTFS Journal viewer, Photorec y TestDisk, QuickHash, NBTempoW, USB Write Protector, VLC, Windows File Analyzer, entre otras.

Ilustración 37: Herramienta forense CAINE.

6.4.1.6 FTK Imager

Acrónimo de Forensic Toolkit Imager, es un software informático forense desarrollado por AccessData, cuyas principales capacidades se detallan a continuación:

- Multiplataforma: puede ejecutarse en vivo (mediante DVD-R o pendrive USB), instalarse o ejecutarse en el equipo del investigador, tanto en Linux como Windows.
- Permite la adquisición de imágenes forenses de discos físicos, lógicos, archivos de imagen, contenidos de carpetas e incluso unidades ópticas, en diferentes formatos (RAW, SMART, E01, AFF).
- Posee herramientas para volcado de memoria RAM.
- Permite la visualización y navegación por la estructura de directorios.
- Posee herramientas para la visualización en formato hexadecimal, vistas previas de documentos y ANSI latino.
- Permite la búsqueda mediante palabras clave.

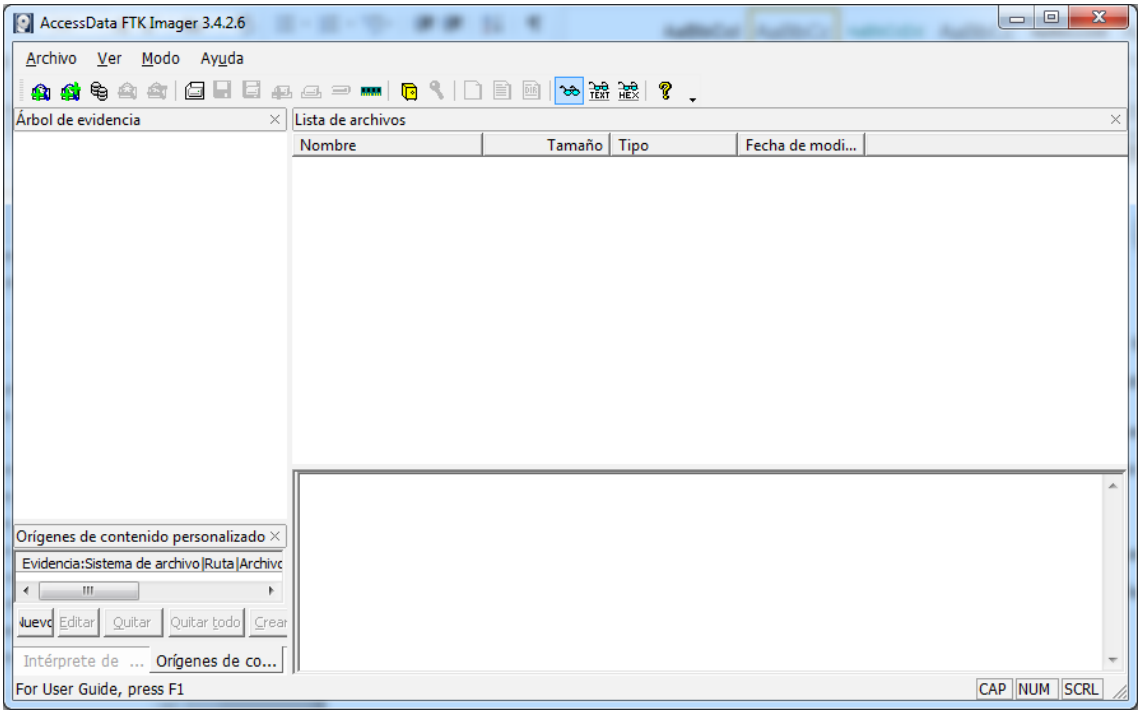

Ilustración 38: Herramienta forense FTK Imager.

6.4.1.7 EnCase

Respecto de EnCase, resulta oportuno destacar que se trata de uno de los productos líderes en el mercado, en gran parte gracias a las diferentes

herramientas que provee y a un poderoso motor de búsqueda, entre sus principales características se encuentran:

- Vista de los datos en línea de tiempo.
- Soporte para múltiples sistemas de archivos para el trabajo con evidencia digital.
- Motor de búsqueda y relacionamiento de datos propio.
- Soporte para múltiples arreglos de discos dinámicos y recuperación de archivos de sistemas de archivos ext 2/3,
- Trabajo sobre teléfonos inteligentes y tabletas de forma integrada, al igual que sobre discos rígidos, así como memorias y/o dispositivos extraíbles y portables.
- Generar base de datos de hash y búsqueda por palabras clave.
- Integración con otros softwares de análisis forense.
- Recolección de evidencia de forma remota, permitiendo la conexión a equipos y la extracción de evidencia digital a nivel de unidades de almacenamiento como de memoria.
- Posee dos métodos de búsqueda, indexado y palabras clave.
- Permite recuperar particiones reconstruyendo la estructura de volúmenes.
- Soporta el análisis del historial navegador web, artefactos de internet.
- Es compatible con diferentes formatos de correo electrónico (Pst/Ost de Outlook, Dbx de Outlook Express, Edb de Microsoft Exchange, Lotus Notes Versión 6.0.3, 6.5.4 y 7, Pfc de AOL 6.0, 7.0, 8.0 y 9.0, Yahoo, Hotmail, Netscape mail, archivos Mbox).
- Interpreta y analiza formatos de imágenes de VMware, Microsoft Virtual PC, DD y Safeback Versión 2.
- Permite realizar reportes en Html o texto enriquecido.

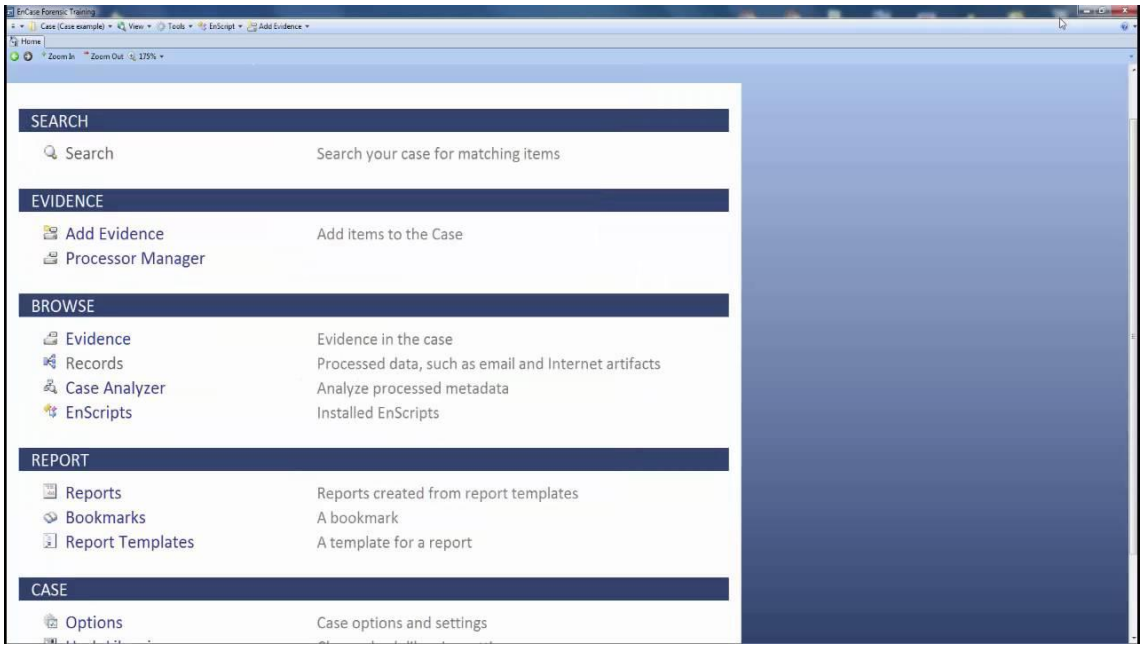

Ilustración 39: Herramienta forense EnCase.

6.4.1.8 Magnet AXIOM

Magnet AXIOM es considerada como una plataforma de investigación digital bastante completa, permitiendo investigadores forenses adquirir y analizar evidencias forenses de forma transparente, dentro de sus capacidades se pueden señalar:

- Vista de los datos en línea de tiempo.
- Compatible con equipos de computación Windows y Mac, al igual que teléfonos celulares y dispositivos tipo Tablets del mercado.
- Obtención y análisis forense de artefactos de internet, espacio asignado y no asignado, tales como redes sociales y sus aplicaciones, Webmail, aplicaciones de chat, servicios de almacenamiento en la nube y actividad de navegadores de internet.
- Imágenes y videos con metadatos exif.
- Copias de respaldo de dispositivos móviles.
- Búsqueda de palabras clave.
- Aplicar filtros, generar marcadores y crear notas.

- Visualizar línea de tiempo.
- Visualizar ubicaciones en mapa.

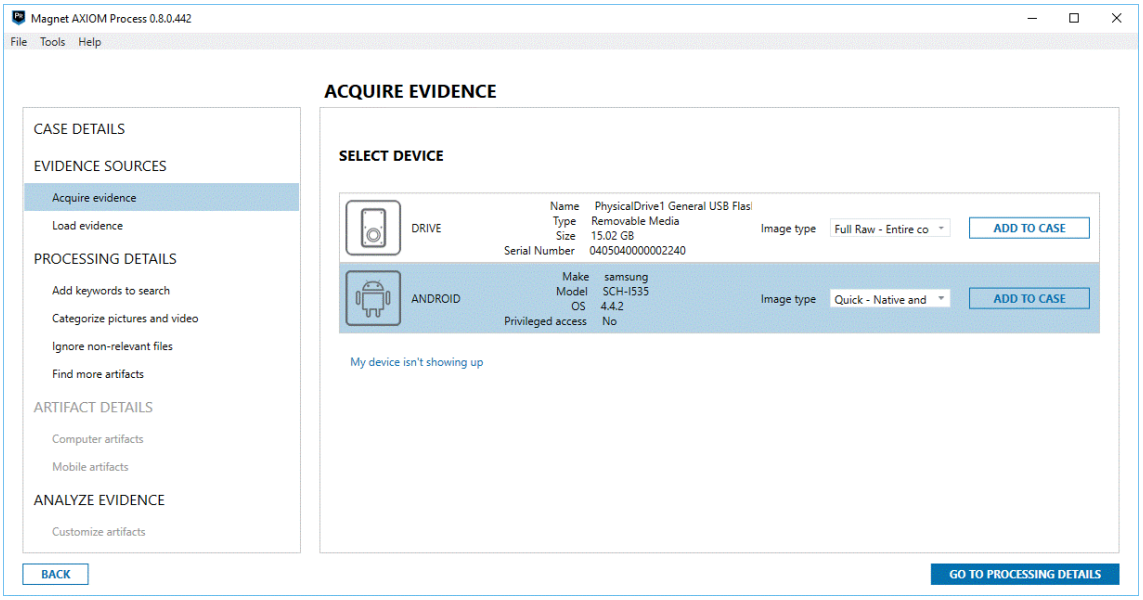

Ilustración 40: Herramienta forense Magnet AXIOM.

6.4.1.9 UFED 4 PC

Respecto de UFED 4 PC, cabe destacar que es un producto de análisis forense de dispositivos móviles con gran renombre en el mercado, en gran parte gracias a las prestaciones que posee, entre las que se encuentran:

- Compatibilidad con gran cantidad de teléfonos celulares y dispositivos móviles del mercado con sistemas operativos Symbian, Microsoft Mobile, BlackBerry, Palm y Apple iPhone.
- Uso para la extracción en tiempo real de información y datos procesables de teléfonos celulares, teléfonos y dispositivos inteligentes, dispositivos de posicionamiento global (gps).
- Capacidad para recolectar información sobre agenda de contactos, registro de llamadas (marcadas, recibidas y perdidas), imágenes, audios, videos, calendario, correo electrónico, mensajes de texto, aplicaciones de mensajería y chat, archivos multimedia, etiquetas geográficas, información

de ubicación (WiFi, celda y aplicaciones de navegación), posiciones GPS, audio.

- Relevar información el dispositivo tal como marca, modelo, IMEI, ESN.
- Colectar sistemas de archivos completos (volcado de memoria).
- Extracción de contraseñas de usuarios y de archivos.
- Exportar la información y presentarla mediante informes claros y concisos.

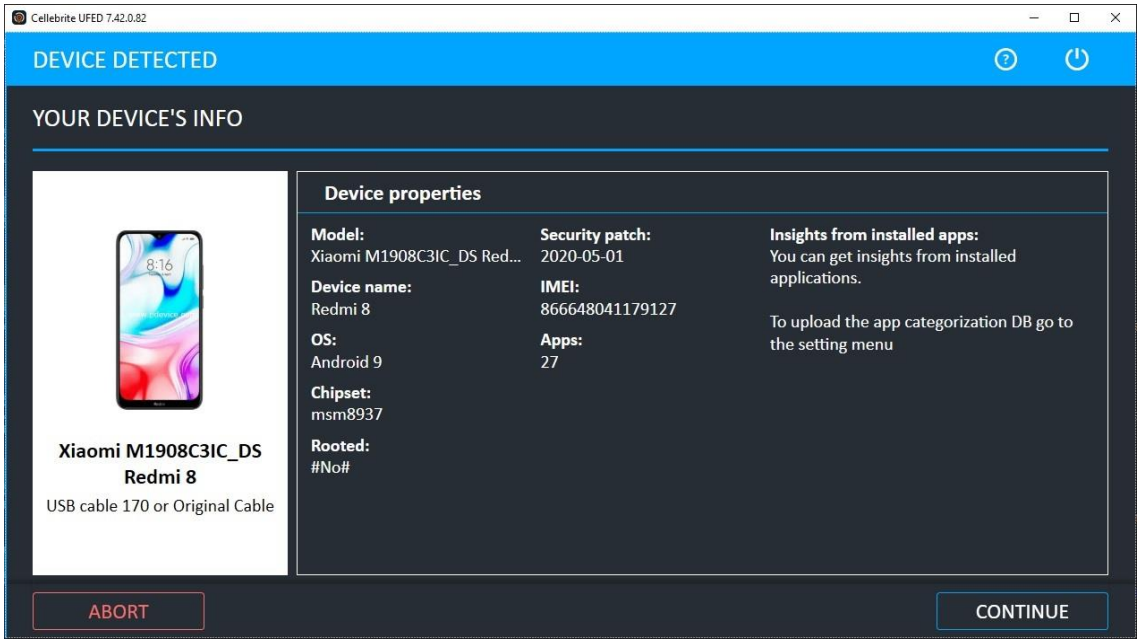

Ilustración 41: Herramienta forense UFED 4 PC.

6.4.1.10 Oxygen Forensic

Respecto de Oxygen Forensic, esta herramienta se trata de uno de los productos líderes en el mercado respecto de análisis forense para dispositivos móviles, en gran parte gracias a la cantidad de dispositivos que soporta, incluyendo unidades GPS y Drones, como así también las múltiples herramientas que provee, entre las que podemos destacar:

- Compatibilidad con gran cantidad de teléfonos celulares y dispositivos móviles del mercado con sistemas operativos Symbian, Microsoft Mobile, BlackBerry, Palm y Apple iPhone.

- Uso para la extracción en tiempo real de información y datos procesables de teléfonos celulares, teléfonos y dispositivos inteligentes, dispositivos de posicionamiento global (gps).
- Capacidad para recolectar información sobre agenda de contactos, registro de llamadas (marcadas, recibidas y perdidas), imágenes, audios, videos, calendario, correo electrónico, mensajes de texto, aplicaciones de mensajería y chat, archivos multimedia, etiquetas geográficas, información de ubicación (WiFi, celda y aplicaciones de navegación), posiciones GPS, audio.
- Relevar información el dispositivo tal como marca, modelo, IMEI, ESN.
- Colectar sistemas de archivos completos (volcado de memoria).
- Realizar extracción de información almacenada de diferentes fuentes en la nube.
- Extracción de contraseñas de usuarios y de archivos.
- Posicionamiento geográfico de eventos.
- Línea de tiempo.
- Estadísticas de comunicación.
- Marcar evidencias clave.
- Grafo de análisis de actividades.
- Exportar la información y presentarla mediante informes claros y concisos.

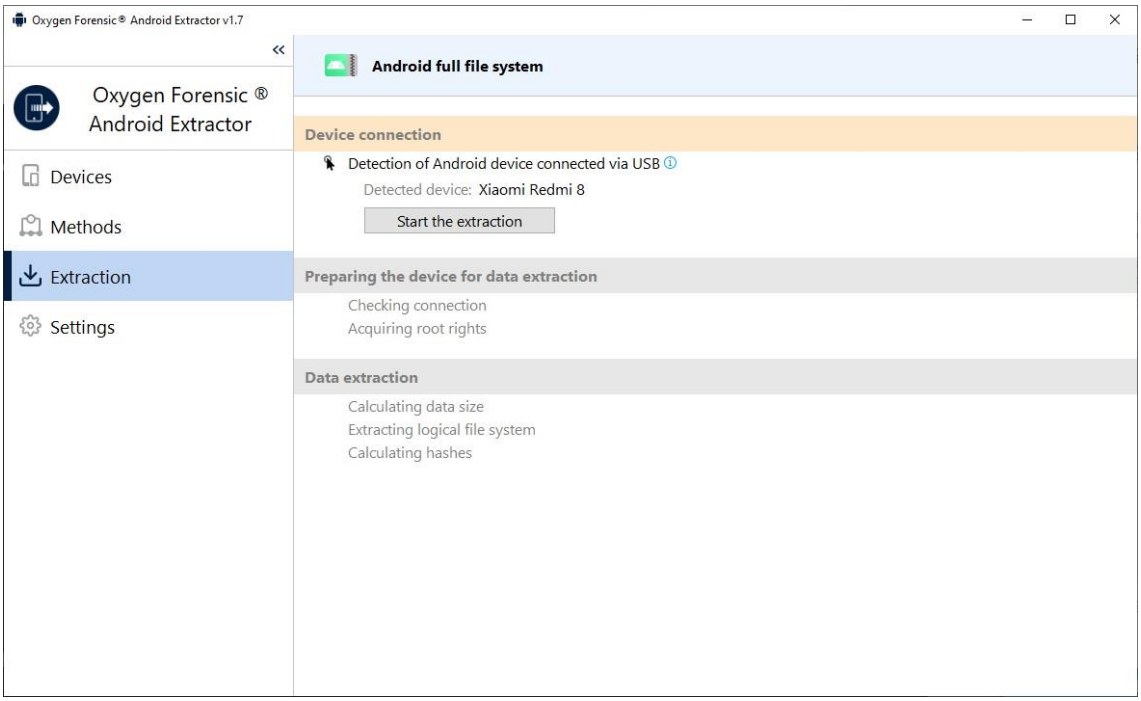

Ilustración 42: Herramienta forense Oxygen Forensic.

6.5 Tabla 27: Modelo simplificado - Etapa de presentación.

Actividades / Documentación Técnica	Reporte de resultados	Remisión de hallazgos	Mecanismos para su preservación	Modelos de trabajo	Recomendaciones
RFC 3227/2002					
SAI HB 171/2003					
NIST 800-86-2006	●				●
US DoJ NCJ 219941/2008					
ISFS/2009	●				●
ACPO/2012	●				●
ENISA/2014	●				●
ISO/IEC 27037/2016					
PGN 756/2016					
MINSEG RES 234/2016					

6.6 Tabla 28: Modelo simplificado - Etapa de evaluación.

Actividades / Documentación Técnica	Análisis de los resultados obtenidos	Ponderación de los resultados obtenidos	Revisión de metodologías aplicadas	Identificación de interrogantes adicionales	Reformulación del alcance
RFC 3227/2002					
SAI HB 171/2003					
NIST 800-86-2006	●	●			
US DoJ NCJ 219941/2008					
ISFS/2009					
ACPO/2012					
ENISA/2014					
ISO/IEC 27037/2016					
PGN 756/2016					
MINSEG RES 234/2016					

6.7 Tabla 29: Roles y responsabilidades - Investigador.

DESCRIPCIÓN
Es aquella persona encargada de planificar y organizar todo el proceso de investigación digital, coordinando diferentes actividades a desarrollarse. Por lo general, este rol puede ser desempeñado por un individuo designado por la organización involucrada o autoridad judicial competente, a fin de velar por el cumplimiento de aquellos objetivos planteados para el desarrollo de la investigación.

ACTIVIDADES
• Solicitar el inicio de la investigación. • Señalar el escenario del incidente. • Aportar detalles sobre los eventos investigados. • Establecer el alcance de la investigación. • Estudiar las conclusiones aportadas. • Ponderar los hallazgos identificados. • Realizar nuevos requerimientos.

COMPETENCIAS REQUERIDAS	EXPERIENCIA	• Usuario general de tecnología de la información. • Conceptos fundamentales básicos de análisis forense. • Alcance y limitaciones de herramientas forenses.
	CONOCIMIENTO	• Trabajo en equipo. • Comunicación. • Resolución de problemas.
	HABILIDAD	• Marco legal y normativo. • Procedimientos de investigación. • Análisis de información.

6.8 Tabla 30: Roles y responsabilidades - Primer interviniente.

DESCRIPCIÓN
Es aquella persona involucrada en la identificación, recolección y preservación de la evidencia digital en la escena del incidente. Este rol lo desempeñan profesionales que poseen amplia experiencia, habilidad y conocimientos en el manejo de evidencia digital, lo que será crucial para su preservación en virtud de la fragilidad que presenta.

ACTIVIDADES
• Evaluar el escenario del incidente. • Planificar, diseñar y ejecutar sus actividades de forma eficiente. • Identificar aquellos dispositivos y registros digitales de interés para la investigación. • Preservar evidencias digitales según diferentes grados de volatilidad. • Establecer requisitos para recolectar evidencia digital de forma lógica y/o física. • Seleccionar herramientas forenses adecuadas para obtener evidencias digitales. • Evaluar riesgos que pudieran modificar, alterar o eliminar tales indicios. • Documentar los procedimientos implementados. • Velar por la cadena de custodia de los elementos recolectados y remitirlos al laboratorio de análisis forense.

COMPETENCIAS REQUERIDAS	EXPERIENCIA	• Administración de tecnología de la información. • Cadena de custodia. • Marco legal y normativo.
	CONOCIMIENTO	• Identificación de dispositivos y equipos informáticos. • Procedimientos investigativos en la escena del hecho. • Planificación y ejecución de actividades operativas.
	HABILIDAD	• Utilización de herramientas forenses para adquisición. • Optimización de procesos para recolección de evidencia digital. • Preservación de evidencias digitales.

6.9 Tabla 31: Roles y responsabilidades - Especialista en análisis de evidencia digital.

DESCRIPCIÓN
Es aquella persona que lleva adelante el análisis y procesamiento de las evidencias digitales recolectadas, para luego elaborar el informe pericial correspondiente. Este rol corresponde a profesionales que poseen experiencia, conocimientos y habilidades con alto grado de especificidad en el análisis de evidencia digital, además pueden ejecutar aquellas actividades correspondientes a los primeros intervinientes.

ACTIVIDADES
• Verificar la integridad de la evidencia digital remitida para análisis. • Realizar copias de respaldo de aquellas evidencias remitidas para análisis y verificar su integridad. • Seleccionar herramientas forenses adecuadas de análisis. • Realizar análisis integral de las evidencias digitales y artefactos forenses. • Clasificar los hallazgos identificados en función de los requerimientos planteados. • Exportar hallazgos identificados, garantizando su disponibilidad e integridad. • Correlacionar hallazgos identificados mediante una línea de tiempo. • Documentar los procedimientos realizados mediante la confección del informe correspondiente. • Velar por la cadena de custodia de los elementos recolectados originalmente, las copias de respaldo obtenidas y hallazgos identificados.

COMPETENCIAS REQUERIDAS	EXPERIENCIA	• Administración avanzada de tecnología de la información. • Confección de reportes de forma clara y concisa. • Aseguramiento de la cadena de custodia.
	CONOCIMIENTO	• Artefactos forenses. • Técnicas antiforenses. • Metodologías de trabajo y reglas de buena práctica.
	HABILIDAD	• Utilización de herramientas forenses para análisis. • Correlación de eventos. • Presentación de reportes.