JUNIO 2019

EVIDENCIAS ELECTRÓNICAS

MÁSTER UNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE TELECOMUNICACIONES

PROTOCOLOS Y APLICACIONES DE SEGURIDAD

Autora: Carmen Alés López
Consultor: Enric Hernández Jiménez
Profesor: Víctor García Font

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Evidencias electrónicas*
Nombre del autor:	*Carmen Alés López*
Nombre del consultor/a:	*Enric Hernández Jiménez*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2019
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*Protocolos y aplicaciones de seguridad*
Idioma del trabajo:	*Castellano*
Palabras clave	*Evidencias electrónicas, análisis forense, custodia digital*

Resumen del Trabajo

La evidencia electrónica puede ser frágil por naturaleza, es decir, puede ser alterada, manipulada o destruida a través del manejo o examen inadecuado. Por ello, es de vital importancia ser meticulosos durante el proceso de capturas de evidencias electrónicas, ya que, si no se manejan de la manera apropiada, éstas pueden resultar inválidas en un proceso judicial.

Toda evidencia digital tiene que ser veraz y auténtica, por ello no hay mejor manera para demostrarlo que capturándola tal y como es. El objetivo de este TFM es generar evidencias legalmente válidas sobre páginas web, cumpliendo con las normas vigentes y el buen hacer pericial sobre evidencias electrónicas, con el fin de demostrar que ciertos contenidos estaban publicados en un tiempo determinado, quedando demostrada su autenticidad.

En este TFM se han analizado los requisitos necesarios y se ha desarrollado un sistema para la captura de evidencias electrónicas de páginas web, con el propósito de poder aportarlas como pruebas en una investigación y asegurando en todo momento la integridad de éstas, haciendo uso del sellado de tiempo.

Abstract:

Digital evidence can be fragile in nature, it is means, it can be altered, manipulated or destroyed though the improper handling or examination. For that reason, it is of the vital importance being careful during capture of digital evidences process, because, if they are not handled properly, they can be invalid in a judicial process.

All digital evidence must be verified and authentic, so there is no better way to prove it than by capturing it as it is. The goal of this final project is the generation of evidences legally valid about websites, complying with digital evidence standards and the expert conduct on electronic evidences, in order to prove that some contents were published in a fixed moment, on this way is proved its authenticity.

For it, the necessary requirements have been analyzed, developing a system for website digital evidences capturing, with the purpose of provide them as evidences in an investigation, and assuring the integrity of those evidences always, making use of the timestamp.

Índice

Lista de figuras

1. Introducción

1.1. Contexto y justificación del trabajo

Hoy en día se presentan demandas sobre hechos relevantes de elementos registrados en soporte electrónico o digital para impugnar concursos publicados en una web, uso indebido de propiedad intelectual, publicaciones de información no autorizada, publicaciones ilícitas, etc.

Para que estos hechos se puedan aportar como pruebas judiciales, se tiene que probar su existencia, además de su autenticidad. En caso contrario estas pruebas no serán válidas.

Hace años se utilizaban las capturas de pantallas como pruebas judiciales, pero hoy en día los jueces normalmente las suelen considerar nulas porque las consideran manipulables. Para que las consideren válidas tienen que ser certificadas como evidencias electrónicas o digitales.

1.2. Objetivos del trabajo

El objetivo de este trabajo fin de máster es generar evidencias legalmente válidas sobre páginas web para demostrar que ciertos contenidos estaban publicados en un tiempo determinado.

Para ello se realizará un análisis previo legal y técnico del estado del arte sobre evidencias electrónicas para después implementar un prototipo de sistemas de capturas de evidencias sobre páginas web. En dichas evidencias se asegurará la integridad del contenido de las páginas web para evitar que sean manipuladas haciendo uso del sellado de tiempo (timestamp). De esta manera, pueden ser válidas en un procedimiento judicial.

1.3. Metodología

La metodología que se va a seguir en este TFM tiene modelo de cascada con las siguientes etapas que se cumplirán de forma sucesiva:

- Análisis: En esta etapa se analizarán los problemas que hay a la hora de generar y custodiar evidencias electrónicas, es decir, se especificarán los requisitos necesarios en la captura de evidencias digitales.
- Diseño: En esta etapa se diseñará los procedimientos y guías adecuadas para cumplir con los requisitos.
- Implementación: En esta etapa se implementarán los procedimientos para satisfacer los requisitos.
- Documentación: En esta etapa se desarrollará la documentación necesaria.

1.4. Tareas

Las tareas que se van a llevar a cabo en el desarrollo del TFM son las siguientes:

- Análisis del problema: En esta tarea se redactarán los requisitos para la captura de evidencias electrónicas.
- Revisión de la normativa y estándares aplicables: Esta tarea consiste en consultar las normativas y estándares que se aplican en la recopilación de evidencias electrónicas.
- Aplicación a la captura y custodia de evidencias para recursos web y correos electrónicos: Esta tarea consiste en aplicar la normativa consultada y cumplir con los requisitos analizados durante la recopilación y protección de las evidencias digitales.
- Desarrollo de documentación sobre la recolección y preservación de evidencias electrónicas en procesos de peritaje legal: En esta tarea se redactará toda la documentación necesaria durante el proceso de capturas de evidencias digitales y la documentación necesaria para aportar las pruebas necesarias en un peritaje judicial. Además, también se preparará el vídeo explicativo sobre el TFM.

1.5. Planificación del trabajo

A continuación, se muestra la planificación del TFM diferenciada por etapas y tareas:

Etapa	Tarea	Fecha inicio	Fecha fin	Duración
Análisis	Análisis de requisitos	06/03/2019	24/03/2019	15
Diseño	Revisión de la normativa y estándares aplicables	06/03/2019	24/03/2019	15
	Casos de uso	25/03/2019	14/04/2019	17
Implementación	Aplicación a la custodia de evidencias para recursos web y correos electrónicos	15/04/2019	15/05/2019	31
Documentación	Documentación sobre la recolección de capturas de evidencias electrónicas	25/03/2019	30/04/2019	37
	Documentación sobre la preservación de capturas de evidencias electrónicas	25/03/2019	30/04/2019	37
	Redacción memoria final TFM	01/05/2019	04/06/2019	35
	Preparación vídeo explicativo TFM	05/06/2019	11/06/2019	7

En la siguiente figura se muestra el diagrama de Gantt del TFM.

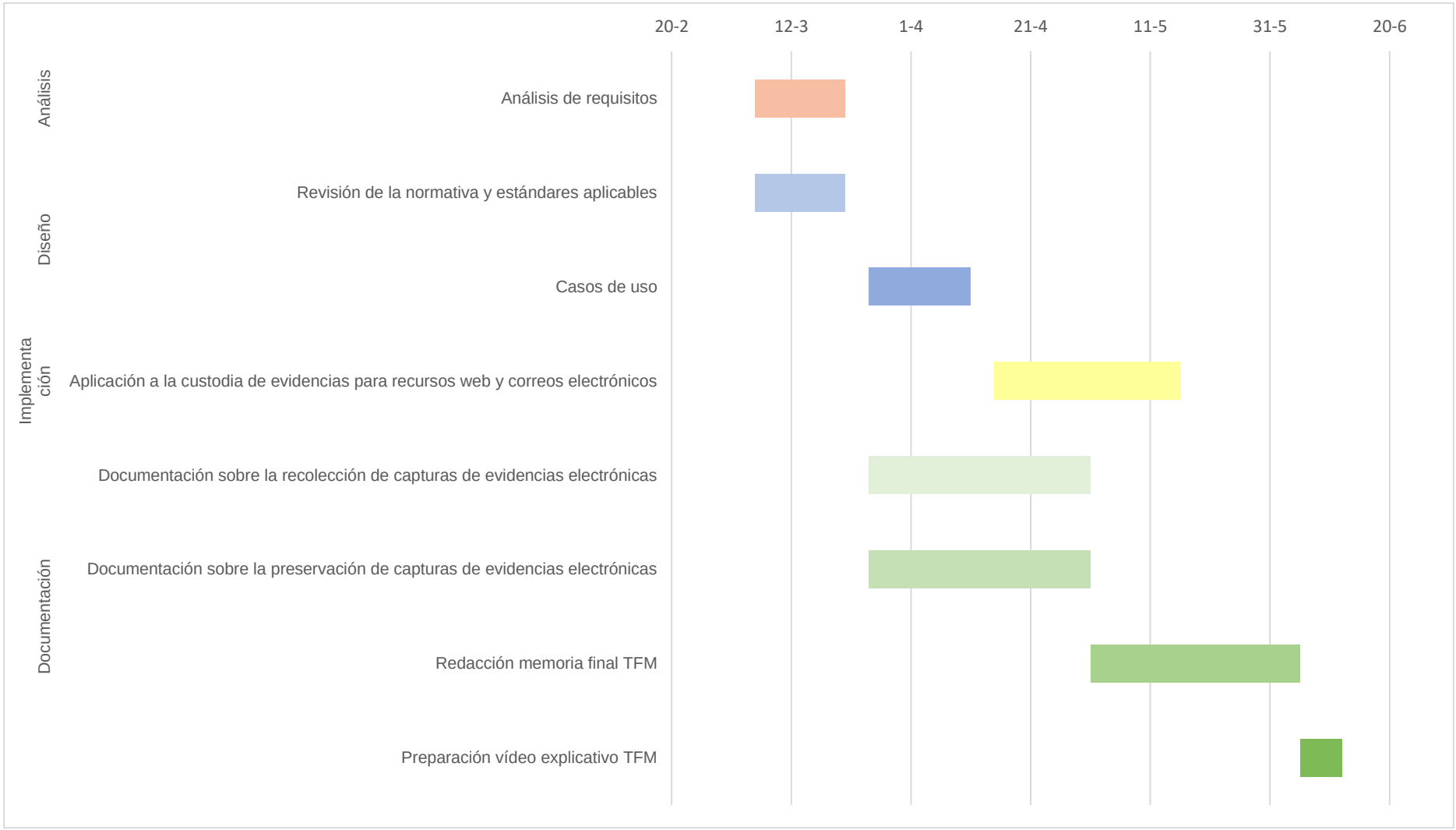

Figura 1 *– Diagrama de Gantt*

1.6. Breve sumario de productos obtenidos

El producto obtenido en el desarrollo de este TFM es un sistema para la generación de evidencias digitales de páginas web. El sistema desarrollado es capaz de demostrar que ciertos contenidos estaban publicados en el momento de dichas capturas.

1.7. Breve descripción de los otros capítulos de la memoria

A continuación, se muestra una breve descripción de los capítulos que componen el TFM veremos lo siguiente:

- **Capítulo 2 – Estado del arte**: En este capítulo pondremos en contexto el trabajo a desarrollar en este TFM.
- **Capítulo 3 – Recursos necesarios**: En este apartado veremos los recursos necesarios para el desarrollo de este TFM.
- **Capítulo 4 – Análisis de viabilidad**: En este capítulo se hablará de la viabilidad del trabajo que se va a desarrollar en este TFM.
- **Capítulo 5 – Normativa**: En este capítulo se verá la normativa aplicable a la captura de las evidencias digitales de contenidos de páginas web y correos electrónicos.
- **Capítulo 6 – Análisis de requisitos**: En este apartado analizaremos los requisitos aplicables de la normativa vista en el capítulo 5.
- **Capítulo 7 – Recopilación de capturas de evidencias electrónicas**: En este apartado hablaremos de cómo recopilar capturas de evidencias electrónicas en una investigación forense, según la normativa aplicable y los requisitos analizados.
- **Capítulo 8 – Preservación de capturas de evidencias electrónicas**: En este apartado hablaremos de cómo preservar capturas de evidencias electrónicas, según la normativa aplicable y los requisitos analizados, para que sean válidas en una investigación forense.
- **Capítulo 9 – Implementación de capturas de evidencias electrónicas**: En este capítulo desarrollaremos un sistema de capturas de evidencias electrónicas que cumpla con los requisitos analizados en el capítulo 5.
- **Capítulo 10 – Conclusiones**: En este capítulo se hablará de las conclusiones a las que se ha llegado después del desarrollo del TFM.

2. Estado del arte[1]

Durante el desarrollo de este TFM se llevarán a cabo una serie de directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas. Todo ello teniendo en cuenta en todo momento la seguridad en el almacenamiento, garantizando idoneidad y adecuación del método de investigación de incidentes. Cumpliendo siempre con la gobernanza del marco de riesgo de la investigación digital.

2.1. Requisitos para el manejo de evidencias electrónicas

Las evidencias electrónicas capturadas deben cumplir los siguientes requisitos:

- Relevancia: Se debe demostrar que el material adquirido es relevante para la investigación.
- Confiabilidad: Todos los procesos utilizados en el manejo de la evidencia electrónica potencial deben ser auditables y reproducibles.
- Suficiencia: En un proceso de capturas de evidencias electrónicas hay que tener en cuenta si se ha obtenido el material suficiente para permitir que se lleve a cabo una investigación adecuada.

2.2. Proceso de manejo de evidencias electrónicas

La evidencia digital puede ser frágil por naturaleza, es decir, puede ser alterada, manipulada o destruida a través del manejo o examen inadecuado.

Las personas que manejan evidencias electrónicas deben ser competentes para identificar y gestionar los riesgos y consecuencias de posibles cursos de acción cuando se trata de evidencia digital. Si no se manejan los dispositivos digitales de una manera apropiada, la evidencia digital potencial contenida en esos dispositivos digitales puede quedar inutilizable o inválida en un proceso judicial.

2.2.1. Identificación

Durante el proceso de identificación hay que priorizar la recopilación de evidencias durante su volatilidad. La volatilidad de los datos debe identificarse para garantizar el orden correcto de los procesos de recopilación y adquisición para minimizar el daño a la evidencia digital potencial y obtener la mejor evidencia. Además, el proceso debe identificar la posibilidad de evidencia digital potencial oculta.

2.2.2. Recopilación

Una vez que se han identificado las evidencias digitales, hay que decidir si se recopilan o adquieren dichas evidencias.

La recopilación es un proceso en el proceso de manejo de pruebas digitales en el que los dispositivos que pueden contener pruebas digitales potenciales cambian su ubicación original por un laboratorio u otro entorno controlado para su posterior adquisición y análisis. Los dispositivos que contienen evidencia digital potencial pueden estar en uno de dos estados: cuando el sistema está encendido o cuando el sistema está apagado. Se requieren diferentes enfoques y herramientas, dependiendo del estado del dispositivo.

Este proceso incluye la documentación de todo el enfoque, así como el empaquetado de estos dispositivos antes del transporte. La evidencia digital potencial puede perderse o dañarse si no se aplica un cuidado razonable.

[1] UNE-EN ISO/IEC 27037:2016

2.2.3. Adquisición

El proceso de adquisición implica producir una copia de evidencia digital y documentar los métodos utilizados y las actividades realizadas.

2.2.4. Preservación

Se debe preservar la evidencia digital potencial para garantizar su utilidad en la investigación. Es importante proteger la integridad de la evidencia. El proceso de preservación implica la protección de la evidencia digital potencial y los dispositivos digitales que pueden contener evidencia digital potencial de manipulación o despojo. El proceso de preservación debe iniciarse y mantenerse a lo largo de los procesos de manejo de la evidencia digital, a partir de la identificación de los dispositivos digitales que contienen evidencia digital potencial.

3. Recursos necesarios

Los recursos necesarios para el desarrollo del TFM son:

- Acceso a la biblioteca de la UOC para consultar la normativa y estándares aplicables como normativas AENOR.
- Paquete Office para el desarrollo de la documentación.
- VirtualBox con distribución Kali Linux para montar el laboratorio forense digital.
- Python 3.6 para el desarrollo del sistema de capturas digitales.

4. Análisis de viabilidad

Con el fin de analizar la viabilidad del desarrollo del TFM hay que analizar los requisitos necesarios para su desarrollo.

En los procesos de peritaje legal hay que asegurar que todas las capturas de evidencias electrónicas son auténticas y no han sido manipuladas para que sean aceptadas como pruebas válidas. Además, siempre hay que cumplir con la legalidad a la hora de interceptar las capturas.

Durante el proceso captura, se tienen que cumplir una serie de requisitos:

- Identificar las evidencias electrónicas.
- Analizar y capturar las evidencias digitales.
- Adquirir y recoger las evidencias electrónicas.
- Preservar y asegurar el almacenamiento de las pruebas.
- Garantizar la idoneidad y adecuación del método de investigación de incidentes.
- Cumplir con la normativa legal.
- Desarrollar la documentación necesaria en procesos de peritaje legal.

4.1. Proceso de desarrollo e implementación[2]

Antes de implementar un proceso para su uso en investigaciones, debe someterse a un proceso de desarrollo adecuado para garantizar que sea adecuado para su propósito. Las etapas típicas son las siguientes:

- Captura y análisis de requisitos.
- Diseño del proceso.
- Implementación de procesos.
- Verificación del proceso (opcional)
- Validación del proceso.
- Confirmación.
- Despliegue.
- Revisión y mantenimiento.

[2] UNE-EN ISO/IEC 27041:2016

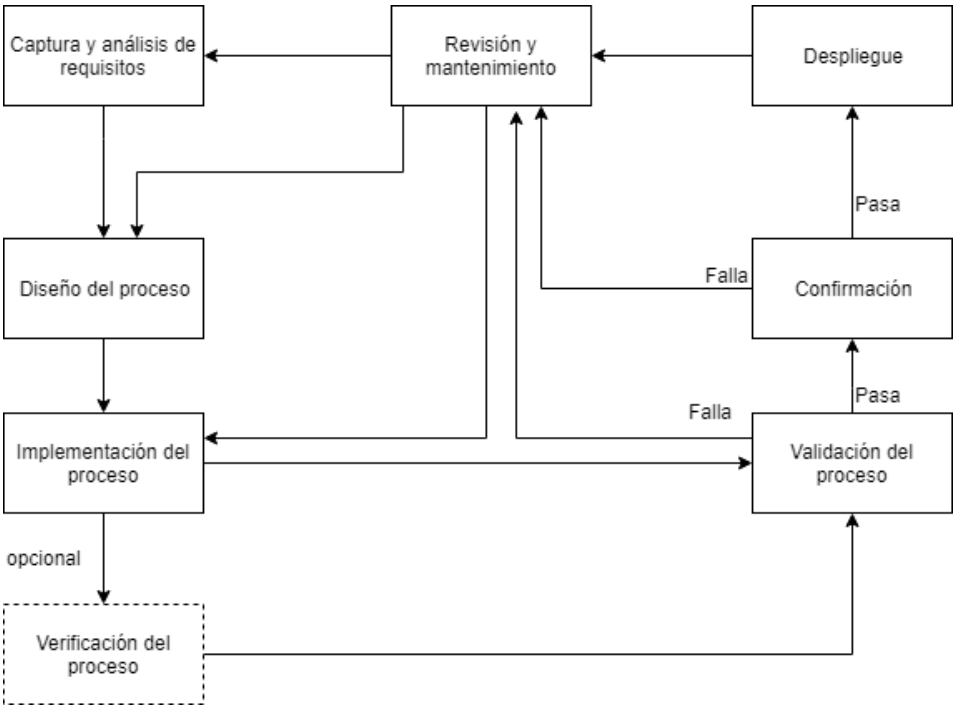

Figura 2 *– Proceso de desarrollo e implementación*

5. Normativa

En este apartado se hablará de la normativa aplicable a la captura de las evidencias digitales de contenidos de páginas web y correos electrónicos.

5.1. UNE-EN ISO/IEC 27037:2016

Esta norma refleja las directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas. En ella se proporcionan una serie de pautas para la identificación, recopilación, adquisición y preservación de evidencias digitales.

5.2. UNE-EN ISO/IEC 27038:2016[3]

Esta norma especifica los requisitos necesarios para la redacción digital de evidencias digitales, para eliminar permanentemente información de una copia de un documento antes de que se divulgue a personas no autorizadas

5.3. UNE-EN ISO/IEC 27040:2016[4]

Esta norma estableces las técnicas de seguridad en el almacenamiento de evidencias digitales.

5.4. UNE-EN ISO/IEC 27041:2016

Esta norma marca las directrices para garantizar la idoneidad y adecuación del método de investigación de incidentes.

5.5. UNE-EN ISO/IEC 27042:2016[5]

Esta norma refleja las directrices para el análisis e interpretación de las evidencias electrónicas.

5.6. UNE-EN ISO/IEC 27043:2016[6]

Esta norma establece los principios y procesos de investigación de incidentes.

5.7. UNE-EN ISO/IEC 30121:2016[7]

Esta norma trata sobre el marco de riesgo de la investigación digital.

[3] UNE-EN ISO/IEC 27038:2016
[4] UNE-EN ISO/IEC 27040:2016
[5] UNE-EN ISO/IEC 27042:2016
[6] UNE-EN ISO/IEC 27043:2016
[7] UNE-EN ISO/IEC 30121:2016

6. Análisis de requisitos

En este apartado se especificarán los requisitos aplicables a las evidencias digitales en base a la normativa consultada.

6.1. Requisitos funcionales

FR01 - Generales	
FR01.01	Los dispositivos digitales se deben manejar de manera apropiada para que las evidencias digitales potenciales que contengan sean utilizables.
FR01.02	En el proceso de planificación de la recopilación, el almacenamiento y el manejo de datos previos al incidente, se deben definir las actividades para la recopilación, el almacenamiento y el manejo de los incidentes previos a los incidentes que representan posibles pruebas digitales. El resultado de este proceso debe incluir las actividades definidas para la recopilación, el almacenamiento y el manejo de incidentes previos a los incidentes que representan posibles pruebas digitales.
FR01.03	El DEFR debe poder justificar todas las acciones y métodos utilizados en el manejo de la evidencia digital potencial.
FR01.04	En el proceso de planificación del proceso de detección de incidentes, se debe definir las acciones a realizar y luego se detecta un incidente. La salida de este proceso debe incluir acciones definidas que se realizarán una vez que se detecte un incidente. La información también debe incluir entradas del sistema preconocidas, resultados de todos los procesos de clase de preparación, así como datos recopilados y generados durante los procesos de grupo de procesos de implementación.

FR02 - Auditabilidad	
FR02.01	Todos los procesos utilizados en el manejo de la evidencia digital potencial deben ser auditables.
FR02.02	El DEFR debe indicar cuánto material se ha considerado y los procedimientos utilizados a través de la auditoría y justificación
FR02.03	Un asesor independiente u otras partes interesadas autorizadas deben poder evaluar las actividades realizadas por un DEFR y por un DES.
FR02.04	Los procesos realizados por un DEFR y un DES deben estar disponibles para una evaluación independiente para determinar si se siguió la técnica o el procedimiento del método científico apropiado.
FR02.05	El DEFR y el DES deben poder justificar la toma de decisiones.

FR03 - Repetitividad	
FR03.01	Todos los procesos utilizados en el manejo de la evidencia digital potencial deben ser repetibles.
FR03.02	El DEFR poder realizar todos los procesos descritos en la documentación y llegar a los mismos resultados sin orientación ni interpretación.
FR03.03	El DEFR debe ser consciente de que puede haber circunstancias en las que no sea posible repetir la prueba.

FR03.04	Cuando no es posible repetir la prueba, el DEFR debe garantizar que el proceso de adquisición es fiable.

FR04 - Reproducibilidad	
FR04.01	Todos los procesos utilizados en el manejo de la evidencia digital potencial deben ser reproducibles.
FR04.02	El DEFR o la persona que realiza la reproducción deberán estar informados sobre las condiciones aplicables.

FR05 - Identificación	
FR05.01	La identificación y la evaluación de evidencias digitales deben llevarse a cabo en presencia de suficiente información contextual para que el investigador pueda tomar decisiones sobre cada elemento en consideración.
FR05.02	La volatilidad de los datos debe identificarse para garantizar el orden correcto de los procesos de recopilación y adquisición para minimizar el daño a la evidencia digital potencial y obtener la mejor evidencia.
FR05.03	Se debe priorizar la recopilación de evidencias en función de su volatilidad, además se deben identificar las posibles evidencias digitales ocultas.
FR05.04	Algunas de las fuentes potenciales identificadas podrían no estar disponibles. En ese caso, se deben explorar los controles para que la fuente identificada esté disponible.

FR06 - Recopilación	
FR06.01	EL DEFR debe tener en cuenta la recopilación del material suficiente para permitir que se lleve a cabo una investigación adecuada.
FR06.02	El material adquirido durante la recopilación de evidencias digitales debe ser relevante para la investigación.
FR06.03	Otro DEFR o DES debe poder demostrar que la decisión tomada en la recopilación de la evidencia digital fue la mejor.
FR06.04	El DEFR y el DES deben adoptar el mejor método de recopilación posible basado en la situación, coste y tiempo, y documentar la decisión de usar un método en particular.
FR06.05	El DEFR debe asegurarse de que es competente para extraer los medios de almacenamiento, y reconocer cuándo es apropiado y se puede hacer.
FR06.06	De acuerdo con los requisitos de la jurisdicción aplicable, los detalles sobre evidencias digitales no recopiladas deben documentarse con justificación para su exclusión.
FR06.07	El DEFR también puede necesitar recopilar alguna evidencia hablando con personas que puedan tener información útil o relevante sobre la posible evidencia digital. Cualquier respuesta debe ser documentada con precisión. Estas personas pueden ser el administrador del sistema, el propietario de la página web y los usuarios. Durante esta recopilación de pruebas verbales, el DEFR puede solicitar información como la configuración del sistema y la contraseña de administrador / root. Estas conversaciones deben documentarse para garantizar que los detalles

	sean precisos y que la declaración documentada no se pueda cambiar. El DEFR debe estar familiarizado con los requisitos jurisdiccionales relevantes relacionados con la recopilación de pruebas no digitales.
FR06.08	Al recopilar un dispositivo digital o adquirir evidencia digital potencial, se deben considerar varios factores que incluyen, entre otros, los siguientes: • Volatilidad de la evidencia digital potencial. • Existencia de encriptación. • Criticidad del sistema. • Requisitos legales de una jurisdicción. • Recursos tales como el tamaño del almacenamiento requerido, disponibilidad de personal, limitaciones de tiempo.

FR07 - Adquisición	
FR07.01	El método de adquisición utilizado debe ser una copia de evidencia digital potencial que puedan contener evidencia digital potencial.
FR07.02	El DEFR debe poder describir los procedimientos seguidos y explicar cómo se tomó la decisión de la adquisición de cada elemento de las evidencias digitales.
FR07.03	El DEFR debe decidir cuánto y qué material es necesario adquirir.
FR07.04	El DEFR debe adoptar un método de adquisición adecuado en función de la situación, coste y tiempo, y documentar la decisión de utilizar un método o herramienta en particular de manera apropiada.
FR07.05	Los métodos utilizados para adquirir evidencia digital potencial deben documentarse detalladamente y deben ser reproducibles o verificables por un DEFR competente.
FR07.06	Un DEFR o un DES deben adquirir la evidencia digital potencial de la manera menos intrusiva para evitar introducir cambios cuando sea posible.
FR07.07	Si el proceso de adquisición de la evidencia digital va a alterar la evidencia dejándola inoperable, las acciones realizadas deben documentarse para tener en cuenta los cambios en los datos.
FR07.08	Tanto la fuente original como la copia de evidencia digital deben verificarse con una función de verificación probada y debe ser aceptable para la persona que usará la evidencia.
FR07.09	La fuente original y cada copia de evidencia digital deben procesar la misma salida de la función de verificación.
FR07.10	En circunstancias donde el proceso de verificación no se puede realizar, el DEFR debe usar el mejor método posible disponible y ser capaz de justificar y defender la selección del método.

FR08 - Análisis	
FR08.01	En el proceso de planificación del análisis de datos de la evidencia digital potencial previo al incidente, se debe definir procedimientos para el análisis previo a incidentes de datos que representan evidencia digital potencial. La entrada a este proceso debe incluir los escenarios definidos en el proceso de definición de escenario, así como la salida del proceso de recopilación previa al incidente. La entrada también debe incluir los objetivos para los procesos de preparación. El

	resultado de este proceso debe incluir las actividades definidas para el análisis previo a incidentes de los datos que representan evidencia digital potencial. Las actividades definidas en este proceso deben incluir información exacta sobre cómo se detecta el incidente y qué comportamiento constituye e incide.
FR08.02	El análisis debe hacer uso de los procesos validados por personal competente y documentarse escrupulosamente para establecer una procedencia rastreable y defendible de la información.
FR08.03	Los procesos utilizados para llevar a cabo el análisis de elementos de evidencia digital potencial deben validarse por completo para sus roles en la investigación.
FR08.04	El procesamiento utilizado no debe cambiar el contenido de ninguna fuente de evidencia digital potencial que se esté analizando. Cuando exista la posibilidad de dañar la evidencia digital potencial, se deben tomar las medidas adecuadas para minimizar la probabilidad o los efectos de dicho daño. En el caso de que el daño sea inevitable o estrictamente necesario, el equipo de investigación debe ser competente para explicar los efectos de cualquier acción tomada que pueda haber resultado en daño, así como las razones de tales acciones y daño.
FR08.05	A lo largo del análisis, cada persona que lleve a cabo cualquier proceso debe mantener notas precisas y detalladas de sus acciones y de los resultados de esas acciones, además del registro de la cadena de custodia. Las notas deben ser lo suficientemente detalladas para permitir que otra persona igualmente competente repita los pasos y logre los mismos resultados. Las notas deben incluir detalles de la información relevante recibida y las decisiones tomadas, incluidas las razones de la decisión.
FR08.06	El análisis estático se debe realizar en una copia de la evidencia digital potencial original para evitar la supresión u ofuscación accidental de la evidencia digital.
FR08.07	En algunas circunstancias, se debe analizar una versión en vivo de la evidencia digital potencial para obtener una comprensión adecuada.
FR08.08	Cuando la evidencia digital se analice en vivo pero no sea posible seguir los pasos recomendados en la norma UNE-EN ISO/IEC 27037, los investigadores deben tener mucho cuidado de minimizar el riesgo de daños a la posible evidencia digital y deben asegurarse de que tengan un registro completo y detallado de todos los procesos realizados. Los prospectos de investigación deben garantizar que cualquier persona que deba realizar un análisis en vivo sea plenamente competente para hacerlo y pueda explicar sus procesos y cualquier alteración de los datos, evidencia digital potencial o sistemas que puedan haber ocurrido como resultado de sus acciones.

FR09 - Preservación	
FR09.01	Se debe preservar la evidencia digital potencial para garantizar su utilidad en la investigación.
FR09.02	Se deben seguir todos los procedimientos estrictamente desde el momento en el que se detecta el incidente hasta que se cierra la investigación para preservar la evidencia digital. Estos procedimientos deben garantizar que la evidencia original no se cambie y, lo que es más importante, deben garantizar que no surja ninguna oportunidad durante la cual la evidencia original pueda ser cambiada, perdida, robada, destruida, etc.

FR09.03	El proceso de preservación debe iniciarse y mantenerse a lo largo de los procesos de manejo de la evidencia digital, a partir de la identificación de los dispositivos digitales que contienen evidencia digital potencial.
FR09.04	El DEFR debe poder demostrar que la evidencia no ha sido modificada desde que fue recopilada o adquirida, o proporcionar la justificación y las acciones documentadas si se realizaron cambios inevitables.
FR09.05	Las evidencias digitales potenciales se deben asegurar de manera que se evite el despojo y la manipulación.
FR09.06	EL DEFR debe estar familiarizado con el embalaje específico de la jurisdicción relevante con el fin de preservar las evidencias digitales.
FR09.07	Toda evidencia digital potencial adquirida debe protegerse lo más lejos posible de la pérdida, manipulación o expoliación.
FR09.08	En el proceso de preservación se debe mantener la integridad y autenticidad de la evidencia digital potencial y su cadena de custodia.
FR09.09	La evidencia digital potencial adquirida debe almacenarse en una instalación de preservación de evidencia que aplique controles de seguridad físicos como sistemas de control de acceso, sistemas de vigilancia o detección de intrusos u otro entorno controlado para la preservación de evidencia digital.
FR09.10	Una vez completado el proceso de adquisición, el DEFR debe sellar los datos adquiridos mediante funciones de verificación o firmas digitales para determinar que las copias de pruebas digitales son equivalentes a las originales.
FR09.11	El DEFR debe asegurar lo siguiente: • Utilizar una función de verificación apropiada para proporcionar evidencia de que los archivos copiados son equivalentes a los originales. • Puede ser apropiado asociar el DEFR con la evidencia digital potencial adquirida, utilizando firmas digitales, biométrica y fotografía.

FR10 - Cadena de custodia	
FR10.01	En cualquier investigación, el DEFR debe poder explicar todos los datos y dispositivos adquiridos en el momento en que se encuentre bajo la custodia del DEFR.
FR10.02	El registro de la cadena de custodia debe contener la siguiente información como mínimo: • Identificador único de la evidencia. • Quién accedió a la evidencia y la hora y ubicación en que se llevó a cabo. • Quién verificó la evidencia dentro y fuera de la instalación de preservación de evidencia y cuándo sucedió • Por qué se verificó la evidencia (en qué caso y con qué propósito) y la autoridad pertinente, si corresponde. • Cualquier cambio inevitable en la evidencia digital potencial, así como el nombre del responsable individual y la justificación para la introducción del cambio.
FR10.03	La cadena de custodia debe mantenerse durante toda la vida útil de la evidencia y conservarse durante un cierto período de tiempo después del final de la vida útil de la evidencia.

FR11 - Priorización	
FR11.01	El DEFR debe intentar maximizar la cantidad de datos preservados por las acciones de recopilación y adquisición.
FR11.02	Cuando no está claro qué elementos son más relevantes que otros, se deben examinar antes de la recopilación mediante un proceso para determinar la prioridad.
FR11.03	El DEFR debe poseer un conocimiento sólido para priorizar de acuerdo a la volatilidad.
FR11.04	Tras la identificación, el DEFR debe ser rápido en la recolección y adquisición de datos con métodos validados.
FR11.05	En circunstancias en las que el tiempo puede ser un factor limitante durante una investigación, se debe dar preferencia a la evidencia digital potencial identificada como relevante para el incidente específico.

FR12 - Investigación	
FR12.01	Las investigaciones digitales se deben aplicar en la práctica siempre que sea necesario investigar una evidencia digital.
FR12.02	El investigador debe usar métodos adecuados para los fines de la investigación que no conduzcan a errores inaceptables o incertidumbre.
FR12.03	Se debe asegurar la idoneidad de los métodos de investigación de incidentes, siguiendo un modelo adecuado para garantizar que todos los procesos estén sujetos a revisión.
FR12.04	La investigación de un incidente se debe planificar con antelación cuando sea posible.
FR12.05	El incidente bajo investigación debe estar claramente identificado y definido, incluidas las limitaciones al alcance de la investigación. Se deben identificar las fuentes de evidencia digital potencial y las preguntas que deben responderse. Las fuentes de riesgo y sus efectos potenciales en la investigación, el personal y los sistemas también deben identificarse.
FR12.06	La investigación debe llevarse a cabo de manera que sea intrínsecamente fiable y que produzca evidencias digitales de procedencias fiables.
FR12.07	Los investigadores deben asegurar que cada elemento de la evidencia digital pueda rastrearse hasta la fuente de la que deriva.
FR12.08	Si un miembro del equipo de investigación cree que ha encontrado evidencia de otro incidente, debe informar al responsable de la investigación de este hecho y esperar instrucciones adicionales. Los líderes de la investigación deben consultar con las autoridades apropiadas antes de permitir que la investigación continúe. Si se produce algún daño observado en la evidencia digital potencial, debe indicarse en el informe.
FR12.09	Los miembros del equipo de investigación deben tener en cuenta sus obligaciones exigidas con respecto a la imparcialidad. Donde exista tal obligación y si, durante el curso de la investigación de una premisa, el equipo de investigación encuentra pruebas que refutan la premisa, o que apoya o sugiere una contrapremisa, debe ser reportado junto con la evidencia de respaldo.

FR12.10	Un investigador independiente, desconectado del análisis e interpretación, debe poder examinar los procesos y las decisiones tomadas por el equipo de investigación original y lograr los mismos resultados.
FR12.11	En el proceso de definición de escenario, se deben examinar todos los escenarios probables donde se requiera evidencia digital. El resultado de este proceso debe incluir los escenarios definidos.
FR12.12	En el proceso de identificación de posibles fuentes de evidencia digital, se debe identificar fuentes potenciales de evidencia digital dentro de una organización. El resultado de este proceso debe incluir las fuentes potenciales definidas de evidencia digital.

FR13 - Interpretación	
FR13.01	El equipo de investigación debe recordar que su responsabilidad principal es proporcionar una interpretación justa y precisa de los hechos a medida que los determinan.
FR13.02	Al evaluar la evidencia, se debe tener cuidado para distinguir los hechos encontrados y la información deducida.
FR13.03	Las distinciones entre los hechos y la información deducida deben tenerse en cuenta y tener cuidado de que todos los hechos necesarios para respaldar cualquier inferencia estén en su lugar y se verifiquen a sí mismos. Al informar hechos e información inferida, la distinción entre los dos debe establecerse y el proceso lógico que ha ocurrido en cualquier deducción debe ser claro y repetible.
FR13.04	La interpretación de cualquier evidencia digital depende de la información disponible sobre el contexto de creación de ese elemento de evidencia digital. Se debe tener cuidado para probar la confiabilidad de la información proporcionada y para garantizar que el valor probatorio asignado refleje esa confiabilidad.
FR13.05	Durante el análisis y la interpretación, el equipo de investigación debe tener en cuenta la calidad de la evidencia digital potencial disponible.
FR13.06	El objetivo de la etapa de interpretación es producir una explicación de los hechos encontrados durante el análisis, dentro del contexto proporcionado al equipo de investigación. Si hay más de una explicación razonable, también se deben informar explicaciones alternativas. Si los hechos se prestan a más de una interpretación, todos deben presentarse como resultado del análisis, indicando, si es posible, sus respectivas probabilidades.

6.2. Análisis de requisitos

AR01 - Captura y análisis de requisitos	
AR01.01	Antes de diseñar un proceso para su uso en un análisis, se deben especificar los requisitos y el cliente los debe aceptar. Este conjunto de requisitos debe derivarse de los requisitos identificados para la investigación completa y puede incluir tanto requisitos funcionales como no funcionales.
AR01.02	Se debe especificar cada requisito de forma individual, sin implementación, sin ambigüedades, completa, singular y coherente con el resto de los requisitos del conjunto.

AR01.03	La lista de requisitos producidos también debe incluir definiciones claras de los límites de operación asociados con la evidencia digital potencial anticipada y los procesos de investigación relacionados.
AR01.04	Es posible que deba formularse una nueva lista de requisitos para cada investigación realizada para garantizar que el examen cumpla correctamente con los requisitos especificados del caso.
AR01.05	Una vez que se han identificado los requisitos para la investigación, el equipo de investigación debe desarrollar los requisitos para los exámenes, análisis y procesos que conformarán la investigación.

AR02 - Requisitos funcionales	
AR02.01	Se deben especificar los requisitos funcionales derivados directamente de las necesidades de la investigación.
AR02.02	Los requisitos funcionales deben incluir las entradas y salidas esperadas.
AR02.03	Todos los requisitos funcionales deben ser satisfechos por la investigación.

AR03 - Verificación	
AR03.01	Los requisitos se deben verificar para garantizar que los requisitos especificados cumplen con las necesidades del método de investigación por el que se ha optado.
AR03.02	El proceso de verificación de los requisitos debe implicar un análisis de los requisitos registrados para identificar problemas. Cualquier problema identificado debe resolverse antes de pasar a las siguientes etapas.
AR03.03	La verificación de los requisitos que son similares a aquellos para el uso previsto debe tratarse como un indicador inicial de que la herramienta o el proceso pueden ser adecuados para el despliegue en el contexto de una investigación, pero no una garantía completa de que cumplirá con los requisitos para el uso previsto. La verificación debe considerarse como parte opcional de la garantía, pero potencialmente útil.

6.3. Metodología

ME01 - Procedimientos y metodología	
LJ01.01	Los procedimientos que se van a seguir deben incluir el manejo de pautas para fuentes de evidencias digitales potenciales.
LJ01.02	Los procedimientos llevados a cabo en el manejo de evidencias digitales deben tener en cuenta los cambios y documentar las medidas adoptadas.
LJ01.03	Los procedimientos en el manejo de evidencias digitales deben cumplir con las normas locales de evidencia.
LJ01.04	Debe existir un flujo de información definido entre cada uno de los procesos y entre las diferentes partes interesadas. Este flujo de información debe ser definido para cada tipo de investigación.

ME02 - Diseño metodología	
ME02.01	Durante la fase de diseño, todas las herramientas que puedan participar en el proceso deben identificarse.
ME02.02	El proceso documentado debe definir el grupo de herramientas que deben considerarse para su uso, junto con los riesgos identificados y, cuando sea posible, cuantificados.
ME02.03	Se deben diseñar procesos robustos proporcionales y superpuestos para garantizar que refuercen la procedencia de toda la evidencia digital encontrada.

ME03 - Implementación	
ME03.01	Una vez que se haya completado el diseño, se debe implementar en forma de instrucción de trabajo detallado y documentado, proporcionando instrucciones paso a paso para el funcionamiento correcto de cada paso del proceso.
ME03.02	Cuando el diseño del proceso incluye una lista de herramientas que pueden usarse para realizar las mismas funciones o funciones similares, la instrucción de trabajo debe proporcionar una guía sobre cómo el investigador debe elegir la herramienta adecuada para las condiciones encontradas durante el análisis.

ME04 - Verificación	
ME04.01	La verificación del proceso debe proporcionar un nivel de seguridad.
ME04.02	Cuando el diseño del proceso incluye una lista de herramientas que pueden usarse para realizar las mismas funciones o funciones similares, la instrucción de trabajo debe proporcionar una guía sobre cómo el investigador debe elegir la herramienta adecuada para las condiciones encontradas durante el análisis.
ME04.03	Después del desarrollo de la instrucción de trabajo, debe compararse con el diseño y la evidencia producida, para mostrar cómo la instrucción de trabajo cumple con el diseño.

ME05 - Validación	
ME05.01	La validación del proceso debe demostrar que el proceso definido en la instrucción de trabajo cumple con los requisitos acordados con el cliente.
ME05.02	Antes de que se lleve a cabo la validación, se debe realizar un plan de validación.
ME05.03	La validación debe ser realizada por una parte no involucrada en el diseño, la implementación y la verificación del proceso. Si esto no es posible, el proceso utilizado para la validación debe documentarse de manera clara y coherente para que pueda ser revisado por una parte independiente para evaluar la imparcialidad.
ME05.04	La validación debe someterse a una verificación final para garantizar que sea suficiente y adecuada para satisfacer los requisitos establecidos. Esta verificación no debe ser realizada únicamente por un tercero, sino que debe ser supervisada por la organización la cual será responsable de tratar los resultados de cualquier investigación.
ME05.05	Cuando sea posible, el proceso de validación también debe determinar las condiciones de contorno y las tasas de error.

ME05.06	Se debe desarrollar un plan de validación y datos asociados independientemente de las fases de diseño e implementación y deben basarse únicamente en los requisitos acordados.
ME05.07	Un proceso no debe emplearse hasta que se haya validado por completo.
ME05.08	Si un proceso no pasa la validación, se deben revisar los requisitos, el diseño y la implementación y deben modificarse adecuadamente. Después se debe validar de nuevo el proceso.
ME05.09	Una vez que se haya confirmado la validación, el proceso debe llevarse a cabo, según las instrucciones de trabajo, para cada prueba definida en el conjunto de validación, utilizando las muestras de validación correspondientes. Se debe mantener un registro del resultado de cada prueba con detalles de cualquier problema encontrado o cambios requeridos como resultado del proceso de validación. Este registro debe incluir detalles del conjunto de validación utilizado y constituye la evidencia de validación.

ME06 - Confirmación	
ME06.01	Para que la confirmación se lleve a cabo, las pruebas de validación del proceso deben verificarse con los requisitos acordados para el uso previsto del proceso. Un proceso solo debe ser confirmado si está completamente validado.

ME07 - Implementación	
ME07.01	La implementación del proceso se debe llevar a cabo después de la confirmación. Todas y cada una de las desviaciones de los resultados o comportamientos esperados deben registrarse y deben tomarse medidas correctivas.

ME08 - Revisión y mantenimiento	
ME08.01	Tras la implementación de un proceso, se debe revisar su rendimiento para identificar los requisitos que faltan o los cambios que pueden ser necesarios para hacer frente a los cambios en las herramientas utilizadas.
ME08.02	La validación debe someterse a revisiones periódicas para garantizar que sigue siendo adecuada para los usos previstos de los procesos asociados. Los procesos deben ser auditados para asegurar que su evidencia de validación sigue siendo correcta y que sigan siendo validados adecuadamente.
ME08.03	Un proceso que ya no se valida apropiadamente o ya no tiene evidencia actual de validación se debe considerar no validado hasta que se vuelva a validar.
ME08.04	Si un conjunto de validación se modifica/actualiza, todos los procesos validados utilizando el conjunto deben verificarse para determinar si el conjunto de validación revisado se aplica a ellos. Si la validación revisada no es aplicable, los procesos pueden permanecer validados mediante el uso del conjunto de validación original. Si el conjunto de validación revisado es aplicable a los procesos existentes, deben volver a validarse utilizando el conjunto de validación revisado.

6.4. Documentación

D01 - Informes	
D01.01	El DEFR debe desarrollar un informe de recopilación y adquisición.
D01.02	En el caso de que se realizaran cambios inevitables en las evidencias digitales, todas las acciones y sus justificaciones deben documentarse.
D01.03	Antes de comenzar la investigación, el responsable de la investigación debe determinar la naturaleza y el propósito del informe final. Esto debe usarse para guiar el proceso de investigación y puede consistir en un conjunto de preguntas que deben responderse, una indicación de los posibles lectores del informe y detalles de las restricciones y limitaciones que se aplican a la investigación. El líder de investigación debe preparar un documento con la estrategia o plan de investigación para ayudar en la determinación de los recursos, la selección de procesos y herramientas y para brindar orientación al equipo de investigación.
D01.04	Los informes deben contener toda la información requerida por la legislación local aplicable.
D01.05	Cuando un informe contiene una o más opiniones, el que escribe el informe debe distinguir claramente entre hechos y opiniones, y justificar las opiniones expresadas.
D01.06	Cada proceso realizado debe documentarse para asegurar la repetibilidad y reproducibilidad, preservar la cadena de custodia, pero también para mejorar la eficiencia y una mayor probabilidad de una investigación digital exitosa.
D01.07	Durante el proceso de presentación de una evidencia digital se debe demostrar la documentación apropiada.

D02 - Redacción digital	
D02.01	La redacción digital se lleva a cabo para eliminar permanentemente información particular de una copia de un fichero. Se debe utilizar cuando, por ejemplo, una o dos palabras de un individuo, una oración o un párrafo, una imagen, un nombre, una dirección y / o una firma deben eliminarse de un fichero antes de que se divulgue a personas que no están autorizadas a hacerlo.
D02.02	Las organizaciones deben tener la capacidad de identificar los documentos que deben redactarse antes de su publicación o divulgación.
D02.03	La redacción debe ser realizada o supervisada por revisores que tengan conocimiento sobre los documentos y puedan determinar qué información se debe redactar. Si los revisores que identifican dicha información no realizan la redacción ellos mismos, sus instrucciones deben ser específicas.
D02.04	La redacción se realizará sobre copias del documento digital. El proceso de redacción debe dar como resultado la creación de un nuevo documento digital donde se logre la eliminación completa e irreversible de la información redactada. Este nuevo documento digital se debe administrar y eliminar de la misma manera que el documento original.
D02.05	Cuando se identifique información que debe ser eliminada antes de la publicación, no se deben identificar oraciones completas o párrafos si solo se van a redactar una o dos palabras en esa oración o párrafo, a menos que la divulgación permita la identificación de la información redactada por contexto.

D02.06	Cuando sea necesario, la información relacionada con el efecto de la redacción de un documento digital se debe vincular con el documento digital.
D02.07	Cuando la redacción se realiza en un documento digital, todos los metadatos incluidos en el documento digital deben revisarse para los requisitos de redacción y se deben realizar las redacciones apropiadas.
D02.08	Cuando la redacción se realiza en un documento digital que contiene imágenes, video e información de voz, se deben utilizar técnicas de redacción que eliminen la información necesaria.
D02.09	La redacción de documentos digitales se debe llevar a cabo de acuerdo con los siguientes principios: • Retención de documento digital. • Eliminación completa de la información redactada. • Redacción de seguridad evaluada. • Ambiente controlado
D02.10	No se debe retener información sobre la evidencia redactada en una copia redactada.
D02.11	En los casos donde se requiera que el documento redactado esté disponible en su formato original, se debe utilizar la conversión del documento a otro formato, seguida de la conversión al formato original, de modo que el proceso general elimine toda la evidencia de la información redactada.
D02.12	Cuando los documentos están en un formato de imagen, voz y / o video, se debe usar un software de redacción especial que puede acceder y actualizar el archivo para garantizar que la información redactada no sea recuperable.

D03 - Anonimato	
D03.01	La redacción digital debe tener como propósito eliminar la información de identificación personal (PII) de un documento para proteger el anonimato
D03.02	Cuando se requiera el anonimato, toda la información que pueda usarse para identificar a la persona debe ser eliminada.

D04 - Registros	
D04.01	Las organizaciones que realizan la redacción deben mantener registros de todas las redacciones realizadas, especialmente cuando las razones detrás de tales redacciones pueden ser cuestionadas. Dichos registros deben consistir en una copia del documento redactado o una descripción de las redacciones realizadas.
D04.02	Se debe mantener un registro de riesgos.
D04.03	El registro de la cadena de custodia debe ser establecido desde el proceso de recopilación o adquisición.
D04.04	Se debe tener un registro adecuado de la cadena de custodia y de los procesos aplicados a la evidencia digital potencial para garantizar que no hayan sido manipulados.
D04.05	Todas las actividades realizadas en relación con los procesos de investigación digital deben registrarse, junto con los detalles de la arquitectura y los componentes del sistema de información del incidente, si corresponde.

D05 - Herramientas software de redacción	
D05.01	Se deben utilizar herramientas software que funcionen de acuerdo con la norma UNE-EN ISO/IEC 27038:2016.
D05.02	Las herramientas de redacción deben funcionar de tal manera que el usuario marque el área apropiada del documento electrónico y seleccione la función de redacción. Debe haber una función que permita que los comentarios se asignen a áreas específicas de información redactada.
D05.03	Cuando las herramientas de redacción incluyen la facilidad para redactar partes o imágenes integradas completas, también deben permitir la eliminación permanente de partes o imágenes integradas completas y / u otra información incrustada.
D05.04	Las herramientas de redacción deberán tener la capacidad de redactar metadatos seleccionados o todos los documentos, información de propiedad del documento y otra información "secundaria".
D05.05	Cuando se utiliza una herramienta de software de redacción separada, el documento electrónico debe conservarse en su software original una vez que se complete la redacción.
D05.06	Cuando las herramientas de redacción permiten redacciones masivas, deben redactar cada documento de conformidad con la norma UNE-EN ISO/IEC 27038:2016.
D05.07	Para habilitar la redacción de múltiples apariciones de una palabra o frase, debe haber un enlace entre la facilidad de búsqueda del software y la herramienta de redacción.
D05.08	Debe haber una opción para aplicar diferentes marcas al documento electrónico para indicar diferentes tipos de información redactada.

D06 - Pruebas de redacción	
D06.01	Las pruebas deben seleccionarse según la disponibilidad de software adecuado y los requisitos generales de seguridad.
D06.02	Estas pruebas deben confirmar si el proceso de redacción se ha completado y si la redacción es irreversible.
D06.03	En cada caso, la prueba se debe realizar sobre el documento redactado. Si se identifica cualquier información o metadatos que deberían haberse redactado, entonces se debe repetir el proceso de redacción.

6.5. Riesgos y precauciones

RP01 - Riesgos	
RP01.01	El DEFR debe conocer primero todos los riesgos involucrados en la ejecución de todos los procesos durante la investigación.
RP01.02	Se deben evaluar los riesgos para reducir la exposición a reclamaciones por daños.
RP01.03	Los aspectos que deben ser considerados durante la evaluación de riesgos para la evidencia digital potencial incluyen, entre otros, los siguientes:

	• ¿Qué tipo de métodos de recopilación/adquisición se aplicarán? • ¿Cuál es el equipo que puede ser necesario? • ¿Cuál es el nivel de volatilidad de los datos y la información relacionada con la evidencia digital potencial? • ¿Qué pasa si los datos están dañados? • ¿Podrían haber sido comprometidos los datos? ¿Se podría haber configurado la página web para destruir, estropear u ofuscar datos si se accede de manera incontrolada?
RP01.04	La familiaridad del investigador con la herramienta o el proceso propuesto debe tenerse en cuenta, ya que cuanto menos familiarizado esté el usuario con una herramienta o proceso, mayor será la posibilidad de que se produzcan errores adicionales sin control.
RP01.05	Las características de incertidumbre deben ser adicionales al sistema lineal, como el modelo descrito y, por lo tanto, deben aumentar proporcionalmente en función del número de procesos utilizados.
RP01.06	Antes de utilizar una herramienta o método para realizar una investigación, los investigadores deben considerar los efectos probables de todas las debilidades de la secuencia del proceso completo que se ha seleccionado.

RP02 - Precauciones	
RP02.01	Se debe evitar cualquier acción que pueda conducir a la pérdida de la evidencia potencial que se almacena en dispositivos digitales debido a acciones intencionales o no intencionales.
RP02.02	El DEFR no debe acceder a dispositivos digitales, como realizar un volcado de memoria desde un dispositivo digital en vivo, a menos que tengan la competencia requerida y con el uso de procesos fiables y validados.
RP02.03	Durante el embalaje, el DEFR debe anotar y abordar las siguientes precauciones adicionales, cuando corresponda: • Usar guantes libres de pelusas y asegurarse de que las manos estén limpias y secas. • Proteger los dispositivos digitales de la influencia de las fuentes electromagnéticas. El entorno de embalaje debe estar libre de electricidad estática. • El entorno del embalaje debe estar libre de polvo, grasa y contaminantes químicos que promuevan el deterioro oxidativo y la condensación de humedad en la capa magnética. • Minimizar la posibilidad de impresión, lo que puede ocurrir cuando las cintas se almacenan durante largos períodos de tiempo sin un uso activo que resulte en una mala calidad de la señal. • Cuando sea necesario, las áreas de embalaje deben estar libres de luz UV. El DEFR debe considerar si los rayos UV representan un riesgo para la evidencia digital potencial antes de seleccionar un área de embalaje. Los dispositivos digitales deben estar fuertemente protegidos contra el choque térmico.
RP02.04	Los investigadores deben tener en cuenta las áreas de incertidumbre en los resultados. La incertidumbre debe considerarse inversamente proporcional a la calidad de la evidencia en apoyo a la hipótesis.

6.6. Leyes y jurisdicción

LJ01 - Leyes y jurisdicción	
RR01.01	Dependiendo de las leyes particulares en una jurisdicción particular, se debe tomar una consideración y un cuidado específicos cuando se determina que un acusado es inocente en un tribunal de justicia.
RR01.02	El DEFR y el DES deben tomar sólo acciones de su competencia.
RR01.03	En algunas jurisdicciones se debe recurrir a alguna persona con conocimientos científicos, técnicos o especialista para ayudar al tribunal a comprender la evidencia o a determinar un hecho en cuestión.
RR01.04	Todos los requisitos legales deben cumplirse y todos los procesos deben documentarse adecuadamente para preservar la cadena de custodia, ya que la evidencia es manejada por varias partes. Este proceso debe realizarse desde el proceso de detección de incidentes hasta el último proceso.

LJ02 - Autorización	
LJ02.01	Se debe obtener la autorización adecuada para cada proceso realizado dentro de todos los procesos de investigación digital. Es importante obtener la autorización adecuada para las acciones realizadas durante el proceso de investigación digital a fin de no infringir los derechos de los propietarios del sistema, los custodios, los directores, o usuarios, sino también para asegurar que no se infrinja ninguna norma legal.

LJ03 - Admisibilidad	
LJ03.01	Para ayudar a asegurar la admisibilidad de la opinión de los expertos, se deben considerar los siguientes factores: • Si las teorías y técnicas empleadas por el experto científico han sido probadas. • Si han sido sometidos a revisión y publicación. • Si se conoce una tasa de error para la técnica, debe informarse. • Si están sujetos a las normas que rigen su aplicación. Si las teorías y técnicas empleadas por el experto tienen amplia aceptación.
LJ03.02	Los requisitos de admisibilidad pueden variar considerablemente entre las jurisdicciones, por ello se debe obtener asesoramiento legal competente con respecto a esos requisitos específicos. Sin embargo, muchas jurisdicciones incluirán al menos lo siguiente en sus requisitos de admisibilidad para la evidencia: • Relevancia: la evidencia debe tener alguna relevancia con respecto a los hechos en disputa. • Autenticidad: debe mostrarse que la evidencia es lo que pretende ser.
LJ03.03	Las cuestiones legales se deben aplicar durante todo el proceso de investigación. Para cada uno de los subprocesos, se debe realizar una verificación legal para determinar si las leyes y regulaciones legales se cumplen dentro de la jurisdicción particular. Se debe buscar asesoramiento legal dentro de la jurisdicción particular en caso de incertidumbre.

6.7. Roles y responsabilidades

RR01 - Roles y responsabilidades	
RR01.01	Las personas que manejen las evidencias digitales deben ser competentes para identificar y gestionar los posibles riesgos y consecuencias.
RR01.02	El DEFR y el DES deben tomar sólo acciones de su competencia.
RR01.03	El DEFR debe identificar, recopilar, adquirir y preservar la evidencia digital potencial.
RR01.04	El DEFR debe tener experiencia, habilidades y conocimientos adecuados para manejar la evidencia digital potencial.
RR01.05	El DEFR debe evitar situaciones en las que se puedan hacer acusaciones en contra.
RR01.06	El DES debe dar soporte técnico al DEFR para identificar, recopilar, adquirir y preservar la evidencia digital potencial.
RR01.07	Las personas que trabajen con la evidencia digital deben entender y aceptar sus responsabilidades con respecto a la oferta y la demanda de evidencia digital.

RR02 - Competencias	
RR02.01	El DEFR y / o el DES deben tener las competencias técnicas y legales pertinentes.
RR02.02	El DEFR y el DES deben poder demostrar que están debidamente capacitados y que tienen un entendimiento técnico y legal suficiente para manejar la evidencia digital potencial de manera adecuada.
RR02.03	Cuando sea necesario, el DEFR y / o el DES deben poder demostrar que son competentes para manejar la evidencia digital potencial utilizando las herramientas y los métodos seleccionados para realizar las tareas.
RR02.04	El DEFR debe estar capacitado adecuadamente para manejar dispositivos digitales en el contexto de actividades de investigación.
RR02.05	El DEFR debe demostrar y mantener sus habilidades y competencias ante las autoridades apropiadas en el área relevante de manejo de evidencia digital potencial.
RR02.06	El empleador debe garantizar que el DEFR esté capacitado adecuadamente y que mantiene las habilidades y competencias.
RR02.07	Los investigadores y su personal de apoyo deben ser competentes para llevar a cabo sus funciones durante el análisis de evidencias digitales.
RR02.08	Todos los pasos involucrados en la investigación de un incidente deben ser llevados a cabo por personas que sean demostrablemente competentes para completar las tareas asignadas a ellos. Deben estar lo suficientemente familiarizados con las herramientas, los métodos y las técnicas que utilizarán para poder llevarlos a cabo con la supervisión mínima y tener experiencia. También deberían poder reconocer los límites de sus propias capacidades. En caso de que un investigador reconozca sus propias limitaciones, el problema se debe remitir a una persona más importante o competente para que tome las medidas adecuadas.

RR02.09	La competencia debe medirse con un conjunto de habilidades básicas identificadas para los procesos involucrados en la investigación. Se debe buscar evidencia objetiva de las calificaciones y experiencia de la persona.
RR02.10	La competencia de una persona debe revisarse regularmente para garantizar que el historial de competencia de la persona sea correcto. La revisión debe tener en cuenta las nuevas áreas y niveles de competencia que se han logrado y también debe "eliminar" aquellas competencias que ya no son relevantes para la persona en cuestión.
RR02.11	Si la competencia de una persona en un área en particular no es suficiente para su rol en una investigación, se deben tomar medidas.
RR02.12	Un equipo de investigación competente puede considerarse competente cuando, dada una muestra de evidencia digital potencial, su análisis produce resultados equivalentes a los producidos por otro equipo de investigación competente que utiliza un análisis similar.
RR02.13	Las pruebas de aptitud deben repetirse regularmente para mostrar que se mantiene la competencia.
RR02.14	Si no se dispone de una prueba de terceros independiente, un equipo de investigación puede establecer con otros equipos de investigación un esquema de prueba adecuado a sus propias necesidades. Dicho esquema debe someterse a un escrutinio independiente para asegurar que sea apropiado.

RR03 - Instrucciones	
RR03.01	El DEFR y el DES deben estar informados adecuadamente por la autoridad pertinente antes de realizar sus tareas, respetando las leyes y restricciones de confidencialidad.
RR03.02	El DEFR y el DES deben seguir los procesos documentados para asegurar que la integridad y la fiabilidad de la evidencia digital potencial se mantiene.
RR03.03	Se debe realizar una sesión informativa formal para comprender el incidente, qué esperar y qué no esperar durante la investigación, además de un recordatorio contra la manipulación o despojo de pruebas.
RR03.04	La sesión informativa debe ser suficiente para que los miembros estén bien preparados para desempeñar sus funciones y responsabilidades.
RR03.05	Durante la sesión informativa, se debe proporcionar al DEFR y al DES la información relevante y las instrucciones detalladas relacionadas con la evidencia digital potencial que se recopilará o adquirirá.
RR03.06	La información sobre el incidente, a medida que se desarrolle, debe compartirse entre el equipo lo más rápido posible para garantizar que las decisiones sobre las acciones a tomar se pueden hacer de manera eficiente y teniendo en cuenta la necesidad de justificación.
RR03.07	Durante la sesión informativa, el equipo de investigación debe recibir instrucciones sobre el personal relacionado con la investigación

RR04 - Garantías	
RR04.01	El DEFR debe garantizar la integridad y autenticidad de la evidencia digital potencial.
RR04.02	Las etapas de garantías individual deben llevarse a cabo, en la medida de lo posible, independientemente del desarrollo de los procesos, a fin de proporcionar un nivel adicional de confianza.
RR04.03	Se deben tomar medidas para garantizar que las etapas de garantías se lleven a cabo de manera tal que se asegure de que no estén indebidamente influenciadas por consideraciones de diseño e implementación.
RR04.04	La organización debe utilizar un conjunto de validación que represente sus propios usos previstos para los procesos, llevar a cabo las pruebas pertinentes y registrar que los procesos se realizan con un propósito a través de una confirmación formal.
RR04.05	Cuando el organismo externo solo realiza la validación, la organización que realiza la implementación y el organismo que realiza la validación deben acordar los requisitos y el conjunto de validación antes de realizar la validación.
RR04.06	La investigación debe garantizar que los hallazgos sean reportados de forma exhaustiva e imparcial. La investigación debe adoptar un enfoque estructurado. Además, debe llevarse a cabo por investigadores competentes y de manera fehaciente, con posibles fuentes de evidencia digital que se sometan a análisis.

6.8. Herramientas

HE01 - Herramientas	
HE01.01	El DEFR debe tener cuidado al usar una herramienta específica para recopilar o adquirir evidencia digital potencial.
HE01.02	La selección de herramientas debe basarse en los requisitos acordados y los procesos que conforman el análisis. El usuario debe ser competente para utilizar las herramientas en el contexto del proceso relevante.
HE01.03	Los procesos que involucran nuevas herramientas deben ser capaces de pasar la validación y la confirmación antes de la implementación. Los usuarios deben tener esto en cuenta antes de adoptar nuevas herramientas. Para la selección de herramientas para su uso en procesos validados, se debe seguir el procedimiento especificado en UNE-EN ISO/IEC 27041.

7. Recopilación de capturas de evidencias electrónicas

7.1. General

Tras asegurar la escena e identificar todas las evidencias electrónicas relevantes para la investigación, se recopilarán todas las evidencias electrónicas identificadas.

Durante la recolección de las evidencias digitales hay que justificar la decisión tomada en el proceso teniendo en cuenta la situación, el coste y el tiempo.

En todo momento nos debemos asegurar que estamos usando los medios adecuados al extraer las evidencias digitales para que éstas no sean alteradas.

En los casos en los que no se recopile una evidencia digital hay que documentarlo y justificar por qué no se ha recopilado. Esto puede suceder cuando no sea apropiado extraerla, ya que podría modificarse durante el proceso.

Existen casos en los que se puede recopilar evidencias hablando con las personas, como el administrador del sistema, el propietario de la página web, usuarios, etc., que puedan tener información útil o relevante sobre la evidencia. En estos casos se documentará con precisión la información que ha recabado. Si es necesario, se solicitará información sobre la configuración del sistema donde estén alojados los servidores y la contraseña del administrador.

7.2. Leyes aplicables

Las evidencias digitales de páginas web o correos electrónicos se rigen por los mismos principios generales que cualquier documento privado en cuanto a su valoración como medio de prueba según el artículo 325 de la Ley de Enjuiciamiento Civil (LEC)[8].

> "**Artículo 325.** *Modo de producción de la prueba.*
>
> *Los documentos privados se presentarán del modo establecido en el artículo 268 de esta Ley.*"
>
> "**Artículo 268.** *Forma de presentación de los documentos privados.*
>
> *1. Los documentos privados que hayan de aportarse se presentarán en original o mediante copia autenticada por el fedatario público competente y se unirán a los autos o se dejará testimonio de ellos, con devolución de los originales o copias fehacientes presentadas, si así lo solicitan los interesados. Estos documentos podrán ser también presentados mediante imágenes digitalizadas, incorporadas a anexos firmados electrónicamente.*
>
> *2. Si la parte sólo posee copia simple del documento privado, podrá presentar ésta, ya sea en soporte papel o mediante imagen digitalizada en la forma descrita en el apartado anterior, que surtirá los mismos efectos que el original, siempre que la conformidad de aquélla con éste no sea cuestionada por cualquiera de las demás partes.*
>
> *3. En el caso de que el original del documento privado se encuentre en un expediente, protocolo, archivo o registro público, se presentará copia auténtica o se designará el archivo, protocolo o registro, según lo dispuesto en el apartado 2 del artículo 265."*

Basándonos en los artículos citados, para que las páginas web o correos electrónicos se pueda presentar como evidencia digital, da igual que se presente original o copia, siempre y cuando no se pueda cuestionar su autenticidad. En caso en el que se dude de su autenticidad, será

[8] BOE Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil

necesario presentar un informe pericial donde se haga constatar la veracidad de dicha prueba según lo establecido en el artículo 326 de la Ley de Enjuiciamiento Civil.

> "**Artículo 326.** *Fuerza probatoria de los documentos privados.*
>
> *1. Los documentos privados harán prueba plena en el proceso, en los términos del artículo 319, cuando su autenticidad no sea impugnada por la parte a quien perjudiquen.*
>
> *2. Cuando se impugnare la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto. Si del cotejo o de otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.*
>
> *3. Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica.*"

Un correo electrónico se puede aportar como una evidencia digital en un proceso judicial, ya que, una vez que se haya enviado un correo electrónico, su contenido deja de pertenecer al emisor. Pero siempre que se quiera aportar como evidencia digital tiene que demostrarse su autenticidad.

Cualquier evidencia digital puede ser impugnada en un procedimiento judicial según establece el artículo 427.1 de la LEC.

> "**Artículo 427.** *Posición de las partes ante los documentos y dictámenes presentados.*
>
> *1. En la audiencia, cada parte se pronunciará sobre los documentos aportados de contrario hasta ese momento, manifestando si los admite o impugna o reconoce o si, en su caso, propone prueba acerca de su autenticidad.*"

En el caso de que su autenticidad haya sido impugnada por la parte de a quien perjudique, el que haya presentado la evidencia digital, podrá pedir el cotejo pericial o cualquier otro medio que pruebe su autenticidad. Si del cotejo o el método practicado no se dedujera su autenticidad, el tribunal deberá valorarlo según el artículo 334 de la LEC.

> "**Artículo 334.** *Valor probatorio de las copias reprográficas y cotejo*
>
> *1. Si la parte a quien perjudique el documento presentado por copia reprográfica impugnare la exactitud de la reproducción, se cotejará con el original, si fuere posible y, no siendo así, se determinará su valor probatorio según las reglas de la sana crítica, teniendo en cuenta el resultado de las demás pruebas.*
>
> *2. Lo dispuesto en el apartado anterior de este artículo también será de aplicación a los dibujos, fotografías, pinturas, croquis, planos, mapas y documentos semejantes.*
>
> *3. El cotejo a que el presente artículo se refiere se verificará por el Secretario Judicial, salvo el derecho de las partes a proponer prueba pericial.*"

La evidencia digital del correo electrónico será presentada en el proceso judicial junto con la impresión en papel del correo electrónico de dicha evidencia. Además se entregará un informe pericial que demuestre el origen de la evidencia digital y su preservación.

En un informe pericial hay que demostrar si los correos electrónicos o páginas web que se aportan como evidencias digitales han sido manipulados o no.

En los correos electrónicos, es necesario recrear todo el proceso que ha seguido para verificar su autenticidad. Para ello tenemos que partir del correo electrónico auténtico que ha sufrido modificaciones. Si al recrear todo el proceso y al realizar un análisis exhaustivo de la evidencia digital no se ha encontrado ninguna irregularidad, el perito puede verificar la autenticidad del correo electrónico.

No hay que olvidar que siempre que se estén recopilando evidencias digitales hay que cumplir con la ley, de lo contrario, la evidencia digital obtenida puede ser impugnada en un proceso judicial.

7.3. Datos sensibles

Tanto los correos electrónicos como las páginas web pueden contener datos sensibles que deben ser protegidos bajo la Ley Orgánica de Protección de Datos (LOPD). Esta ley se basa en el artículo 18 de la Constitución Española[9] y tiene la finalidad de proteger y garantizar los datos personales de las personas

Durante todo el proceso de investigación debemos velar por:

- Confidencialidad: Debemos garantizar que la información es accesible sólo para el personal autorizado.
- Integridad: Debemos garantizar que los datos son auténticos y fiables.
- Disponibilidad: Debemos garantizar que los datos a consultar por el personal autorizado están accesibles en todo momento.

7.4. Consideraciones

7.4.1. Previas

Al recolectar las evidencias digitales identificadas, debemos tener en cuenta los siguientes factores de riesgo:

- Método de recopilación que se va a aplicar.
- Volatilidad de la evidencia digital y de la información relacionada.
- Datos dañados.
- Existencia de encriptación.
- Criticidad del sistema.
- Jurisdicción.
- Recursos como herramientas disponibles, personal con el que se cuenta, limitación de tiempo, etc.

En el caso de páginas web, hay que tener cuidado por si ésta ha podido ser configurada para destruir, estropear u ofuscar datos si se accede de manera incontrolada.

Es importante destacar que, en todo momento, se deben preservar las evidencias digitales y que hay que cumplir con la legislación, desde el primer momento de la investigación y hasta que ésta finalice.

7.4.2. Durante la recopilación

Durante el embalaje, debemos anotar y abordar las siguientes precauciones adicionales, cuando corresponda:

- Usar guantes libres de pelusas y asegurarse de que las manos estén limpias y secas.
- Proteger los dispositivos digitales de la influencia de las fuentes electromagnéticas. El entorno de embalaje debe estar libre de electricidad estática.
- El entorno del embalaje debe estar libre de polvo, grasa y contaminantes químicos que promuevan el deterioro oxidativo y la condensación de humedad en la capa magnética.

[9] BOE Constitución Española

- Minimizar la posibilidad de impresión.
- Cuando sea necesario, las áreas de embalaje deben estar libres de luz UV.
- Los dispositivos digitales deben estar fuertemente protegidos contra el choque térmico.

7.5. Recopilación de evidencias digitales

Una vez evaluado los riesgos de las evidencias digitales que se van a capturar, procedemos a su recopilación. Debemos recopilar toda la información posible y no sólo la que esté al alcance, ya que nos podemos pasar por alto detalles fundamentales en la investigación.

Durante el proceso de adquisición de las evidencias digitales se describirán detalladamente todos los procedimientos que se han seguido, justificando las decisiones tomadas, por si hubiera que reproducirlas, que se llegue al mismo punto obteniendo los mismos resultados.

El método que se emplee para adquirir la evidencia digital potencial tiene que ser una copia exacta de ésta, sin manipulaciones ni alteraciones, y deben realizare de la manera menos intrusiva sobre un soporte limpio. Las capturas de evidencias digitales se deben realizar sobre dispositivos que no se hayan usado o, en el caso de que se hayan usado, debemos asegurarnos de que se ha realizado un borrado seguro del contenido anterior para evitar contaminaciones.

Se verificará la integridad de la copia procesando la misma salida de la función de verificación que la fuente original. Es decir, calcularemos el hash tanto de la fuente original como de la copia y el resultado debe ser el mismo. De esta manera, se certificará que se trata de una copia exacta y que no ha sido manipulada.

Una vez que hemos comprobado que tenemos una copia exacta de la evidencia digital, realizaremos una segunda copia sobre ésta para poder entregar una al secretario judicial y trabajar con la otra. En esta segunda copia también comprobaremos que se trata de una copia exacta, por ello debemos de calcular el hash que debe ser el mismo que en el caso anterior.

Es importante tener siempre una copia de respaldo de la evidencia capturada y trabajar con otra copia exacta, por ello, se realizará una tercera copia. En esta también se verificará la integridad calculando el hash. Esta tercera copia es la que se usa para el análisis de la evidencia digital. Se hace de esta manera, por si mientras se analiza, ésta resulta alterada. Si esto pasa, siempre podemos volver a realizar una copia de la evidencia que se ha capturado, partiendo de la copia que tenemos de respaldo.

En resumen, de la evidencia digital identificada debemos realizar tres copias:

- La primera se entregará para el proceso judicial.
- La segunda se guardará como copia de respaldo en el laboratorio.
- La tercera copia es la que se usará para trabajar en el laboratorio.

7.6. Páginas web

A continuación, nos centraremos en la recopilación de evidencias digitales de páginas web.

7.6.1. Consideraciones

Antes de recopilar evidencias digitales de aplicaciones web debemos tener en cuenta la arquitectura sobre la que está montada. Es decir, no es lo mismo que se encuentre alojada en un servidor único que balanceada en varios servidores, o en un servidor de un tercero. Por eso es importante saber qué equipos están relacionados.

7.6.2. Recopilación de evidencias electrónicas

En la recopilación de evidencias electrónicas de páginas web se realizarán:

- Copia exacta del servidor o servidores donde se aloje la página web.
- Copia de la BBDD de la aplicación web.

- Copia de la aplicación web.

Se solicitarán diagramas de arquitectura, ficheros de logs o configuraciones de los sistemas relacionados con la página web.

En los casos en los que tengamos acceso al código fuente de la aplicación, también se recopilará como evidencia digital por si hay que analizarlo.

También recopilaremos información sobre:

- Direcciones IP de los servidores y máquinas.
- Dominio al que pertenece.
- Subdominios que tiene.
- Nombres de máquinas.
- Arquitectura de la red.
- Perfiles y configuración de servidores.
- Software y hardware.
- Sistemas operativos.
- Arquitectura de la página web

Es importante obtener información sobre los servidores, qué sistemas operativos tienen, qué configuración tienen, qué los puertos que tienen abiertos, etc.

Mapeado

Con el fin de obtener un mapeado completo de la página web de la que se quiere capturar evidencias electrónicas, navegaremos por ella como cualquier usuario, pero usando un web proxy que nos permita conocer y modificar las interacciones entre el navegador y la aplicación web. De esta manera obtendremos el flujo lógico de las distintas páginas que componen la aplicación web, junto con las relaciones que existen entre ellas.

Durante el mapeado, tomaremos notas detalladas de todos los procedimientos seguidos por si hay que reproducirlos en otro momento.

Escaneo de puertos

Como se ha comentado anteriormente, es importante conocer qué puertos están abiertos, así que realizaremos un escaneo de puertos en cada una de las máquinas relacionadas con la investigación.

Durante el escaneo de puertos tomaremos notas detalladas sobre los puertos abiertos que nos hemos encontrado en cada una de las máquinas, así como todos los procedimientos que hemos seguido.

Confidencialidad de las comunicaciones

En aplicaciones web es importante establecer una conexión segura entre el cliente y el servidor web mediante HTTP. Para ello se usa el protocolo de cifrado SSL (Secure Socket Layer) que garantiza la confidencialidad de las comunicaciones.

Debemos recopilar información sobre:

- Si el servidor soporta SSL.
- Si las versiones de SSL soportadas son seguras.
- El tamaño de las claves y los tipos de cifrados soportados por el servidor.
- Si el certificado del servidor es aceptado por todos los navegadores o muestra algún tipo de error.

Balanceadores de carga

Es importante saber si la aplicación web esté alojada en varios servidores balanceados, ya que los balanceadores de carga distribuyen el tráfico entre varios servidores web.

Para detectar o identificar balanceadores de carga haremos lo siguiente:

- Capturar todas las URLs relacionadas.
- Capturar marcas de tiempo de los servidores.
- Capturar los valores de la última modificación de la página web.
- Capturar cookies.

Configuración del software

También es importante conocer la configuración del software. Por ello, capturaremos información sobre las siguientes configuraciones:

- Sistema operativo.
- Servicios de red.
- Servidor web.

Además, si podemos también recopilaremos evidencias digitales sobre:

- Métodos HTTP que soporta el servidor.
- Documentación almacenada en el servidor.
- Páginas instaladas por defecto en el servidor.
- Scripts o programas almacenados en el servidor.

7.6.3. Procedimiento

A continuación, se muestran los pasos que seguiremos durante la recopilación de evidencias digitales en páginas web.

1. Planificar la metodología a seguir en el proceso de investigación, asegurando la idoneidad de los métodos de investigación que se van a emplear.
2. Acceder a los servidores que alberguen las evidencias digitales.
3. Identificar todas evidencias electrónicas que se van a capturar.
4. Priorizar las evidencias electrónicas que se van a recopilar.
5. Recopilar toda la información de las evidencias electrónicas identificadas.
6. Adquirir las evidencias digitales mediante una copia.
7. Calcular los hashes de las evidencias digitales y añadir marcas temporales.
8. Realizar copias de todas las evidencias.
9. Documentar todos los pasos de los procedimientos que se están siguiendo, con sus respectivos registros.
    a. Registrar:
        i. Identificador de la evidencia digital.
        ii. Quién accedió a la evidencia, la fecha y la ubicación.
        iii. Quién verificó la evidencia y la fecha.
        iv. Por qué se verificó la evidencia (en qué caso y con qué propósito) y la autoridad pertinente, si corresponde.
        v. Si se produce algún cambio en la evidencia, hay que registrarlo junto con el responsable y la justificación de dicho cambio.

7.7. Correos electrónicos

A continuación, nos centraremos en la recopilación de evidencias digitales de correos electrónicos.

7.7.1. Consideraciones

Antes de realizar un informe pericial de una evidencia digital de un correo electrónico hay que tener en cuenta que no es lo mismo hacerlo sobre un correo electrónico recibido que sobre uno enviado, ya que éste último es más difícil de analizar porque a veces es necesario verificar que éste fue entregado a su destinatario.

También hay que tener en cuenta el servidor que almacena el correo electrónico de la evidencia digital. Se analizará de distinta manera si se trata de un servidor local, un servidor en la nube o un servidor de un tercero.

Correos electrónicos recibidos

En el caso de que esté el servidor configurado para mantener copias de los correos electrónicos enviados, se cotejaría con la copia almacenada en el servidor con el correo recibido.

Si, por el contrario, el servidor está configurado para eliminar los correos electrónicos enviados, en análisis resultaría más complejo que en el caso anterior porque sólo se dispondría del correo recibido. En este caso, habría que analizar exhaustivamente las cabeceras del correo recibido, el fichero contenedor del mismo y de otros elementos relacionados, para determinar la autenticidad de dicho correo.

Además, se realizará un análisis forense del fichero contenedor de correos electrónicos del disco duro del destinatario. De esta manera, se confirmará que los correos que se han analizado no han sido manipulados después de su entrega.

Correo electrónico enviado

En el caso de correos electrónicos enviados se trata de un análisis complejo, ya que éstos no tienen cabeceras. Comprobar la autenticidad de estos correos es complejo, ya que se pueden falsificar fácilmente. También hay que tener en cuenta que un correo enviado no tiene siempre que llegar a su destino.

Una manera de comprobar si un correo enviado ha llegado a su destino es que se haya enviado con confirmación de entrega. Si el servidor que recibe el correo le envía al servidor lo ha enviado un correo de confirmación, se confirmaría la entrega. Pero puede ocurrir que el mensaje de confirmación nunca llegue.

Servidor local

Si durante el peritaje el servidor de correos de la evidencia digital está accesible, se realizará un análisis forense de éste para comprobar que no haya sido manipulado.

Servidor de terceros

En el caso de que el servidor de correos de la evidencia digital es de un tercero, el perito decidirá si es necesario realizar un análisis forense de dicho servidor, basándose en las evidencias digitales que haya recolectado. Si considera que no tiene suficiente información para realizar el informe pericial, deberá realizar el análisis forense del servidor. Si, por el contrario, cree que ya tiene pruebas suficientes para comprobar la autenticidad del correo electrónico a analizar, no es necesario que realice el análisis forense del servidor.

Servidor en la nube

En el caso de que el correo electrónico que se vaya a analizar se encuentre en un servidor en la nube, el perito no podrá realizar un análisis forense de este. Lo que conllevará a que tenga que utilizar herramientas que certifiquen que el contenido interno de una página web en la que se ha iniciado sesión.

7.7.2. Recopilación de evidencias electrónicas

En la recopilación de evidencias digitales de correos electrónicos tenemos que adquirir las cabeceras MIME, los archivos adjuntos y metadatos que puedan contener. Los metadatos es una información valiosa en las evidencias digitales ya que nos aporta mucha información. En los metadatos que se extraen de un correo electrónico, si éste los tiene, se obtiene información sobre qué usuario creó lo creó, a qué hora, a veces incluso podemos obtener la localización, etc. Es por ello por lo que nos resulta valiosa dicha información.

Este proceso se debe realizar delante de un fedatario público o notario, para que levante un acta notarial del proceso que se ha seguido durante la extracción de la evidencia. De esta manera se prueba que la evidencia digital no es manipulada ni alterada.

Después de extraer la cabecera, se guarda o exporta en un archivo con formato txt, y se calcula el hash antes de almacenarlo en una memoria externa. Se documentará y registrará el proceso del manejo de la evidencia, y se dejará en posesión del notario por si durante el proceso judicial se exige dicha prueba. Es importante registrar y documentar todo el proceso del manejo de la evidencia digital para acreditar la autenticidad de esta. Se añadirá una autoridad de sellado de tiempo (TSA – Time Stamp Authority) para garantizar que los documentos no son alterados después de su firma.

Una vez analizado, hay que preservar la evidencia digital, teniendo cuidado en mantener la cadena de custodia para evitar que sea impugnado o invalidado como prueba en un proceso judicial, protegiéndose así ante una posible impugnación.

7.7.3. Procedimiento

A continuación, se muestran los pasos que seguiremos durante la recopilación de evidencias digitales en correos electrónicos.

1. Planificar la metodología a seguir en el proceso de investigación, asegurando la idoneidad de los métodos de investigación que se van a emplear.
2. Acceder a los servidores que alberguen los correos electrónicos que hay que recoger como evidencias digitales.
3. Identificar los correos electrónicos que se van a capturar como evidencias electrónicas.
4. Priorizar las evidencias electrónicas que se van a recopilar.
5. Recopilar toda la información de las evidencias electrónicas identificadas.
6. Adquirir las evidencias digitales mediante una copia.
7. Calcular los hashes de las evidencias digitales y añadir marcas temporales.
8. Realizar copias de todas las evidencias.
9. Documentar todos los pasos de los procedimientos que se están siguiendo, con sus respectivos registros.
    a. Documentar:
        i. Quién envío el correo.
        ii. A quién iba dirigido.
        iii. Contenido del correo.
        iv. Fecha y hora del envío.
        v. Metadatos del correo (si los tiene)
        vi. Direcciones IP.
    b. Registrar:
        i. Identificador de la evidencia digital.
        ii. Quién accedió a la evidencia, la fecha y la ubicación.
        iii. Quién verificó la evidencia y la fecha.
        iv. Por qué se verificó la evidencia (en qué caso y con qué propósito) y la autoridad pertinente, si corresponde.
        v. Si se produce algún cambio en la evidencia, hay que registrarlo junto con el responsable y la justificación de dicho cambio.

7.8. Herramientas[10]

A continuación, hablaremos de algunas de las herramientas que se usan en análisis forense de capturas de evidencias digitales de páginas web y correos electrónicos.

7.8.1. Correos electrónicos

Nuix

Se usa para analizar correos electrónicos. Esta herramienta permite procesar grandes volúmenes de evidencias para un análisis detallado.

[10] INCIBE – Buscador de soluciones

Está diseñada para buscar y relacionar información de manera rápida y eficiente.

eMailTrackerPro
Se utiliza para analizar los encabezados de los correos electrónicos.

Aid4Mail Forense
Esta herramienta se usa para extraer, procesar y exportar correos electrónicos de los buzones.

Encase Forensic
Es una herramienta software para crear imágenes de correo electrónicos para preservarlos.

7.8.2. Páginas web

Maltego
Maltego es una herramienta de minería de datos que permite recopilar información.

Acunetix
Acunetix es una herramienta software para el escaneo de vulnerabilidades web.

Burp Suite
Burp Suite es una plataforma para la realización de test de seguridad sobre aplicaciones web realizando mapeos, análisis y búsquedas de vulnerabilidades

OpenVAS
OpenVAS es un framework de servicios y herramientas que ofrece escaneo y gestión de vulnerabilidades.

Vega Vulnerability Scanner
Vega Vulnerability Scanner es una herramienta de código libre de escaneo y testeo de la seguridad de aplicaciones web, ayudando a encontrar y arreglar XSS, SQL injection y otras vulnerabilidades.

LOGalyze
LOGalyze es un software de código abierto de gestión centralizada de logs y de monitorización de red.

OSSIM
OSSIM es un producto de seguridad de la información y gestión de eventos (SIEM) de código abierto de AlienVault. Proporciona un SIEM completo con recolección de eventos, normalización y correlación.

eGarante
Testigo tercero independiente para certificar contenido online.

WhatWeb
Esta herramienta permite identificar los servicios web.

Dirb
Dirb es una herramienta software con la que podemos encontrar objetos, archivos y directorios ocultos en una página web.

OWASP-ZAP
Permite auditar la seguridad de una página web.

HTTRACK
HTTRACK es una herramienta software para el clonado de páginas web. Esta herramienta nos permite copiar todo el código de una página web.

7.8.3. Dominios IP

MX ToolBox
Es una herramienta que sirve para rastrear direcciones IP.

Whois
Whois se utiliza para consultar datos sobre dominios y direcciones IPs.

7.8.4. Servidores

Nikto
Es una herramienta software para escanear servidores web. Permite detectar malas configuraciones y vulnerabilidades en servidores, detecta ficheros que existen por defecto, muestra un listado de la estructura del servidor, así como su versión y fecha de actualización, etc.

7.8.5. Dispositivos digitales

DBAN
Es una herramienta software para el borrado seguro de un dispositivo digital.

KillDisk
Es una herramienta software para el borrado seguro de un dispositivo digital.

7.8.6. Tratamiento de datos

FACILITA RGPD
Esta herramienta está destinada a aquellas empresas que realizan tratamientos de datos personales que, a priori, implicarían escaso nivel de riesgos.

7.8.7. Almacenamiento de datos

EnCFSMP
EncFSMP es una herramienta que permite tener carpetas de archivos cifrados protegidos por contraseña en el sistema.

Protected Folder
Protege su privacidad mediante Protected Folder para proteger sus archivos importantes y personales de otras personas que puedan utilizar su ordenador o cuando su equipo se comparte en el trabajo.

Prot-on
Con Prot-On se protegen los archivos que compartes por la red, permitiéndote decidir y conocer en cada momento, quién, cómo y cuándo accede a su contenido.

VeraCrypt
VeraCrypt es un software gratuito para el cifrado de discos, basado en la herramienta TrueCrypt.

7.8.8. Firma electrónica

AccessData's FTK
Es una herramienta software que ofrece análisis forenses y descifrado de contraseñas dentro de una interfaz intuitiva y personalizable.

Clicksign
Es una herramienta software de firma electrónica de escritorio.

HelloSign
Es una herramienta software de firma electrónica de documentos.

XolidoSign
XolidoSign se usa para firmar electrónicamente los archivos de la forma más segura, con certificado electrónico reconocido, sellado de tiempo reconocido y verificación inteligente de archivos firmados, firmas y sellos de tiempo.

8. Preservación de capturas de evidencias electrónicas

8.1. General

La etapa de preservación de capturas de evidencias electrónicas es muy importante, ya que si no se toman las medidas oportunas podría echar por tierra la investigación y las evidencias digitales aportadas no sean admisibles como pruebas.

Toda evidencia digital recopilada debe ser preservada, en el soporte en el que originalmente fueron creadas, para garantizar su utilidad en la investigación, asegurándolas de manera que se evite el despojo o su manipulación.

El proceso de preservación debe iniciarse y mantenerse a lo largo de los procesos de manejo de la evidencia digital, a partir de la identificación de las evidencias digitales potenciales. Hay que seguir todos los procedimientos de manera estricta, desde el momento en el que se detecta el incidente, hasta que se cierra la investigación, con el fin de preservar la evidencia digital.

Después de adquirir las evidencias digitales, se deben sellar los datos adquiridos mediante funciones de verificación o firmas digitales, así nos aseguramos de que las copias de las evidencias digitales adquiridas son iguales a las originales, y lo haremos ante un notario o fedatario público para que levante un acta notarial del proceso que se ha seguido durante la extracción de las evidencias digitales. El acta notarial no acredita la autenticidad, veracidad o autoría de las evidencias, pero sí certificaremos que no han sido alteradas ni manipuladas durante el proceso de extracción.

En todo momento hay que garantizar que la evidencia original no se cambie, además de que no sea alterada, modificada, perdida, robada o destruida.

8.2. Confiabilidad

Para minimizar todo lo posible que se cuestione la veracidad de las evidencias electrónicas y la exactitud de su manejo, es necesario basarse en procesos y procedimientos fiables. Por ello debemos cumplir con los siguientes atributos:

- Autenticación e integridad.
- Disponibilidad y completitud.
- Cumplimiento y gestión.

8.2.1. Autenticación e integridad

La autenticación e integridad de la evidencia digital garantiza el amparo de las características originales de la información, el contexto, la estructura y el contenido, generándose una certeza del autor o firmante de la información y el contexto.

Si la captura de la evidencia digital proviene de otro soporte o sistema, debemos garantizar la recogida fidedigna de la información.

Una vez que se declara el sistema de gestión, las evidencias digitales deben estar protegidas contra modificaciones o alteraciones no autorizadas. En el caso de que la evidencia digital sufra una modificación o alteración autorizada, se debe registrar y dejar traza de ello.

Para que una evidencia digital se considere auténtica se debe probar:

- Que es lo que afirma ser.
- Que ha sido creada por la persona que afirma haberla creado y almacenado.
- Que ha sido creada y almacenada cuando lo afirma.

8.2.2. Disponibilidad y completitud

Toda evidencia digital tiene que estar disponible, es decir, tiene que poder ser localizada, recuperada, presentada e interpretada. Además, tiene que estar completa, es decir, tiene que responder a una representación completa de las operaciones, actividades o hechos de los que da testimonio, a la que se puede recurrir en otro momento de la investigación. De esta manera, se garantiza el acceso y utilización de la evidencia durante su ciclo de vida.

8.2.3. Cumplimiento y gestión

El cumplimiento y gestión de una evidencia digital garantiza que se ha obtenido conforme a los esperado, al haberse gestionado y usado los procedimientos planificados de manera exhaustiva, repetitiva, controlada, medible y auditable. Asimismo, toda evidencia debe ser capaz de demostrar ante terceros, que ha sido generada y almacenada según las políticas, normas y procedimientos de actuación.

8.3. Precauciones

Con el fin de preservar las evidencias digitales, se debe evitar cualquier acción que pueda conducir a la pérdida de ésta debido a acciones intencionales o no intencionales.

Siempre seguiremos y haremos uso de procedimientos fiables y validados en el manejo de evidencias digitales, por ello, no se accederán a dispositivos digitales a menos que se asegure que el acceso no implique modificación en la evidencia digital. Tampoco se harán volcados de memoria en vivo de dispositivos digitales a menos que el volcado no implique alteración en la evidencia.

Durante el embalaje de dispositivos que contengan evidencias digitales, debemos anotar y abordar las siguientes precauciones adicionales, cuando corresponda con el fin de preservar las evidencias electrónicas:

- Usar guantes libres de pelusas y asegurarse de que las manos estén limpias y secas.
- Proteger los dispositivos digitales de la influencia de las fuentes electromagnéticas. El entorno de embalaje debe estar libre de electricidad estática.
- El entorno del embalaje debe estar libre de polvo, grasa y contaminantes químicos que promuevan el deterioro oxidativo y la condensación de humedad en la capa magnética.
- Minimizar la posibilidad de impresión.
- Cuando sea necesario, las áreas de embalaje deben estar libres de luz UV. El DEFR debe considerar si los rayos UV representan un riesgo para la evidencia digital potencial antes de seleccionar un área de embalaje.
- Los dispositivos digitales deben estar fuertemente protegidos contra el choque térmico.

Antes de hacer uso de alguna herramienta o método durante la investigación, se comprobará que la evidencia digital seguirá preservada, sin sufrir modificaciones.

Siempre que vayamos a presentar una evidencia digital como prueba, debemos asegurar su licitud y veracidad. Es decir, que se ha mantenido la cadena de custodia durante toda la investigación y sin vulnerar ninguna ley.

8.4. Cadena de custodia

La finalidad de la cadena de custodia es "*garantizar la exacta identidad de lo incautado y de lo analizado. Tiene por tanto un valor instrumental para garantizar que lo analizado fue lo mismo que lo recogido*" según el Tribunal Supremo. Por tanto, es indispensable mantener la cadena de custodia durante toda la vida útil de la evidencia y conservarse durante un cierto período de tiempo después del final de la vida útil de la evidencia, para que el análisis pericial no sea impugnado.

La cadena de custodia de las evidencias electrónicas es necesaria para acreditar qué se ha hecho sobre la evidencia electrónica y en qué manos ha estado, desde que se ha extraído hasta

que llega al juzgado. La cadena de custodia tiene como objetivo demostrar que la prueba que se presenta es exactamente la misma que se ha recopilado. Además, logramos tener un mayor control sobre las evidencias recopiladas.

Durante la identificación y recopilación de evidencias digitales detallaremos todos los pasos seguidos para obtener un mayor control sobre las evidencias y poder realizar trazas sobre las pruebas adquiridas, asegurando la repetibilidad y reproducibilidad de las evidencias.

Para mantener la cadena de custodia de las evidencias digitales, mientras que no se estén trabajando sobre los dispositivos que las contienen, éstos permanecerán en su embalaje. Todos los dispositivos que contengan evidencias digitales estarán etiquetados con un identificador único. Este identificador único aparecerá en un registro, junto con información sobre las evidencias que contiene, dónde y cuándo fue recopilada la evidencia, además de quién lo hizo y anotaciones relevantes para la investigación si se consideran oportunas. En el registro también se anotará la fecha y la persona que analice la evidencia y, en el caso de que la evidencia sea alterada, también aparecerá registrado.

En el registro de custodia anotaremos la siguiente información:

- Identificador único de la evidencia electrónica.
- Cuándo fue capturada la evidencia.
- Quién accedió a la evidencia y la hora y ubicación en que se llevó a cabo.
- Quién verificó la evidencia y cuándo sucedió.
- Por qué se verificó la evidencia (en qué caso y con qué propósito) y la autoridad pertinente, si corresponde.
- Si se ha transportado la evidencia: quién la transportó, cuándo y porqué.
- Si se modifica la ubicación: quién modificó la ubicación, cuándo y porqué.

Cualquier cambio inevitable en la evidencia digital potencial, así como el nombre del responsable individual y la justificación para la introducción del cambio.

Durante todo el proceso que dure la investigación debemos garantizar la integridad y la autenticidad de las evidencias digitales.

8.5. Transporte y almacenamiento

La evidencia digital potencial adquirida debe almacenarse en una instalación de preservación de evidencia que aplique controles de seguridad físicos como sistemas de control de acceso, sistemas de vigilancia o detección de intrusos u otro entorno controlado para la preservación de evidencia digital.

También hay que proteger los dispositivos que contengan evidencias digitales contra golpes y caídas cuando sean transportados.

Además, hay que tener en cuenta las condiciones ambientales en todo momento. Los dispositivos que contengan evidencias electrónicas no se pueden exponer a temperaturas ambientales extremas, ni a ambientes con mucho polvo o suciedad.

9. Implementación de capturas de evidencias electrónicas

Para la implementación de captura de evidencias digitales de una página web, primero se ha capturado el código web de la evidencia digital. Para ello hemos realizado una solicitud HTTP GET.

Para poder sellar la evidencia digital mediante la autoridad de sellado de tiempo (TSA) y garantizar que la evidencia digital no resulta alterada, se calcula el hash del código de la evidencia digital capturado mediante la función hash SHA-256 y se pasa como entrada a la TSA, cumpliendo con la normativa RFC-3161[11].

Lo que hace la TSA[12] es obtener la fecha y hora de una fuente de tiempo confiable y adjuntar el timestamp (sello de tiempo) al dato proporcionado, es decir, al hash que se ha facilitado. Después calcula el hash del timestamp y del dato, el cual firma digitalmente la TSA y lo devuelve.

La respuesta obtenida de la TSA[13] se aportará junto a la evidencia digital en la investigación para garantizar que se ha preservado la evidencia digital.

A lo largo de este apartado explicaremos el funcionamiento del sistema desarrollado para la generación y conservación de evidencias digitales.

9.1. Sistema desarrollado

9.1.1. Laboratorio forense

Para poder gestionar incidentes de forma correcta hemos montado un laboratorio forense virtual, con el fin de realizar las pericias correspondientes.

Hemos optado por una distribución de Kali Linux para el manejo de las evidencias digitales por los siguientes motivos:

- Es gratuito.
- Hay muchas herramientas de análisis forense desarrolladas para este sistema operativo.
- Se puede usar como CD Live.

El inconveniente que podríamos tener es que fuera del ámbito técnico no se conoce este entorno, por lo que puede generar dudas en jueces y abogados. Por ello tenemos que demostrar que la captura de evidencias digitales se realiza de manera segura y son preservadas en todo momento.

9.1.2. Clonación

Una vez que ya tenemos nuestro laboratorio forense preparado, realizaremos dos copias de la página web que se va a investigar. Una copia sería para trabajar sobre ella, y otra la tenemos como copia de respaldo, por si en algún momento de la investigación tenemos que hacer uso de ella.

Para clonar la página web haremos uso de la herramienta httrack.

Una vez que tengamos clonada la página web podemos proceder a la captura de las evidencias digitales de dicha web.

[11] https://tools.ietf.org/html/rfc3161
[12] https://administracionelectronica.gob.es/ctt/resources/Soluciones/190/Descargas/TSA--Firma-Guia-de-Uso-del-Sello-de-Tiempo-y-Marca-de-Tiempo.pdf?idIniciativa=190&idElemento=135
[13] https://psc.sia.es/AC_SIA_P_TSA.pdf

9.1.3. Capturar evidencias digitales

Para la captura de evidencias digitales hemos desarrollado una aplicación en Python. Esta aplicación se encarga de capturar las evidencias digitales de cada uno de los links que encuentre en la página web que le indiquemos.

La estructura que sigue esta aplicación es la siguiente:

1. Buscar los links de la página web que estamos analizando.
2. Capturar el código de cada link.
3. Calcular el hash del código del link, el cual es enviado al TSA.
4. Añadir el sellado de tiempo TSA a cada captura.

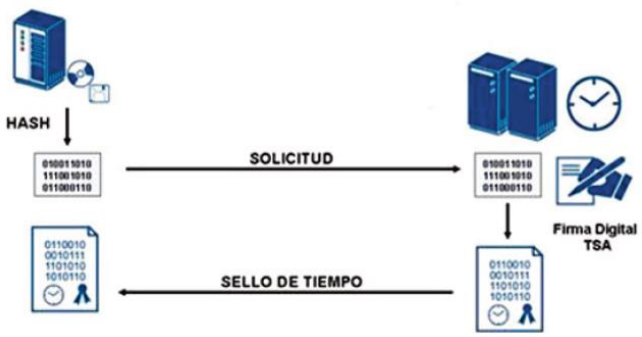

Figura 3 *– Procedimiento para la captura de evidencias digitales*

Cada vez que capturemos una evidencia digital quedará registrada (ver sección **Registro**). En el caso de que nos encontremos con algún problema a la hora de capturar la evidencia digital, también quedará registrado con motivo de su justificación.

Una vez que tengamos todas las capturas de las evidencias digitales encontradas damos por finalizada el proceso de recopilación, ya que tenemos material suficiente para la investigación.

9.1.4. Registro

Mantendremos un registro de todas las evidencias digitales capturadas con la siguiente información:

- ID: Identificador de la evidencia.
- Label: Etiqueta de la evidencia.
- Timestamp: Fecha y hora de la captura.
- Hash: Hash de la evidencia digital.
- TSA: Respuesta hash del TSA.

De esta manera podemos demostrar la preservación de las pruebas aportadas en la investigación.

10. Conclusiones

El motivo por el cual se desarrolló este trabajo fue generar evidencias electrónicas de páginas web con motivo de demostrar que cierto contenido estaba publicado. A lo largo del desarrollo de este trabajo hemos analizados los requisitos técnicos y legales, necesarios para el manejo de las evidencias generadas, para que éstas sean consideradas legalmente válidas.

Hemos observado que es muy importante preservar las evidencias generadas para evitar su despojo y manipulación.

Se ha seguido una metodología en la que hemos analizado los requisitos necesarios para capturar y preservar dichas capturas. En base a los requisitos analizados, hemos diseñado una serie de procedimientos o pautas que debemos seguir a lo largo del proceso. Una vez que supimos los pasos que debíamos seguir, diseñamos un sistema para generar evidencias electrónicas cumpliendo con los objetivos marcados y con los requisitos analizados.

El sistema consiste en capturar evidencias electrónicas de páginas web, añadiendo el sellado de tiempo para probar su integridad. Además, este sistema mantiene un registro de las capturas de evidencias generadas para la cadena de custodia.

Con este sistema podremos probar que las evidencias electrónicas capturadas son auténticas y veraces, pero siempre se puede mejorar el procedimiento.

Ahora mismo, con los resultados obtenidos del sistema, se tiene que hacer manualmente el informe forense, pero como futura línea de investigación, se podría desarrollar un sistema que fuese capaz de generar un informe de cada captura. Este informe contendría el código de la web capturada, junto con el sellado de tiempo y la firma digital del perito forense que hiciera la captura.

Otra futura línea de investigación podría ser desarrollar el sistema para que crease la estructura en árbol de la página web a analizar y que pudiera mostrar el contenido capturado de forma guiada.

11. Glosario

11.1. Abreviaturas

- **BBDD:** Bases de datos.
- **HTTP:** Hypertext Transfer Protocol.
- **LEC:** Ley de Enjuiciamiento Civil.
- **LOPD:** Ley Orgánica de Protección de Datos.
- **SSL:** Secure Socket Layer.
- **TFM**: Trabajo Fin de Master
- **TSA**: Time-Stamp Authority (Autoridad de sellado de tiempo)

11.2. Definiciones

- **Evidencia electrónica** o **evidencia digital**: Contiene información digital con valor probatorio en procedimientos judiciales, es decir, es una prueba digital.
- **DEFR** (Digital Evidence First Responder): El DEFR se encarga de tareas de campo en procedimientos judiciales vinculadas con la identificación y preservación de evidencia digital. Es la persona que recopila y adquiere las evidencias digitales.
- **DES** (Digital Evidence Specialist): El DES es el personal técnico o especialista en evidencias digitales. Puede hacer las tareas del DEFR con conocimientos y habilidades especializadas, es decir, es el perito informático.

12. Bibliografía

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

[2] UNE-EN ISO/IEC 27041:2016 - Tecnología de la información. Técnicas de seguridad. Directrices para garantizar la idoneidad y adecuación del método de investigación de incidentes (ISO/IEC 27041:2015) (Ratificada por AENOR en diciembre de 2016.)

[3] UNE-EN ISO/IEC 27038:2016 - Tecnología de la información. Técnicas de seguridad. Especificación para la redacción digital (ISO/IEC 27038:2014) (Ratificada por AENOR en diciembre de 2016.)

[4] UNE-EN ISO/IEC 27040:2016 - Tecnología de la información. Técnicas de seguridad. Seguridad en el almacenamiento (ISO/IEC 27040:2015) (Ratificada por AENOR en diciembre de 2016.)

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

[6] UNE-EN ISO/IEC 27043:2016 - Tecnología de la información. Técnicas de seguridad. Principios y procesos de investigación de incidentes (ISO/IEC 27043:2015) (Ratificada por AENOR en diciembre de 2016.)

[7] UNE-EN ISO/IEC 30121:2016 - Tecnologías de la información. Gobernanza del marco de riesgo de la investigación digital (ISO/IEC 30121:2015) (Ratificada por AENOR en diciembre de 2016.)

[8] BOE Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil - https://www.boe.es/buscar/pdf/2000/BOE-A-2000-323-consolidado.pdf

[9] BOE Constitución Española - https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf

[10] INCIBE – Buscador de soluciones - https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/buscador-soluciones

[11] RFC3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) - https://tools.ietf.org/html/rfc3161

[12] Guía de uso del sello de tiempo y marca de tiempo. Uso de la TSA – Madrid, septiembre 2011 – Ministerio de Política Territorial y Administración Pública. Secretaría General Técnica - https://administracionelectronica.gob.es/ctt/resources/Soluciones/190/Descargas/TSA--Firma-Guia-de-Uso-del-Sello-de-Tiempo-y-Marca-de-Tiempo.pdf?idIniciativa=190&idElemento=135

[13] Política de sellado de tiempo (TSA) – TSA – SIA - https://psc.sia.es/AC_SIA_P_TSA.pdf

[14] Python Web Scraping – Second Edition – Richard Lawson, Katharine Jarmul – May 2017

[15] Implementing the TimeStamp Protocol natively un Python - https://medium.com/kuranda-labs-engineering/implementing-the-timestamp-protocol-natively-in-python-446817e3a89d

[16] Prácticas y Políticas de Sellado de Tiempo del CORPME - http://registradores.org/wp-content/normativapki/REG-PKI-DPC04v.1.2.0%20Practicas%20y%20Politicas%20de%20Sellado%20de%20Tiempo%20del%20CORPME.pdf

13. Anexos

13.1. Manual de usuario

13.1.1. Instalación y Configuración

La aplicación se puede descargar desde el repositorio https://github.com/carmenales/TFM

Una vez que tengamos descargada la aplicación, la descomprimiremos en un directorio que deseemos. Una vez que esté descomprimido el contenido ejecutaremos el bash setup.sh para instalar las librerías de Python necesarias para ejecutar la aplicación (requests, ASN. 1, Beautifulsoup y rfc3161).

13.1.2. Ejecución

Cuando queramos capturar evidencias de una página web tenemos que irnos a un terminal, movernos hasta el directorio donde hayamos descomprimido la aplicación y ejecutar el script cdew.py con Python seguido de la página web que queremos capturar.

Ejemplo:

```
python3 cdew.py http://example.webscraping.com
```

Una vez terminada la ejecución podremos consultar:

- Los códigos de las páginas web en la carpeta **codes**
- Las respuestas TSA en la carpeta **responses**.
- Los registros en la carpeta **registers**.

Nota: Para un buen uso de la herramienta cada vez que queramos capturar evidencias electrónicas de una página web hay que repetir el proceso visto en este apartado desde el principio. De esta forma nos aseguremos que el entorno no está contaminado.

13.2. Ejemplo

En este apartado se mostrará un ejemplo de los resultados obtenidos con sistema desarrollado.

En el ejemplo se va a usar la siguiente página web como evidencia digital: http://example.webscraping.com

13.2.1. Captura código

A continuación, se muestra el código de uno de los links encontrados en la página web.

```
<!--[if HTML5]><![endif]-->
<!DOCTYPE html>
<!-- paulirish.com/2008/conditional-stylesheets-vs-css-hacks-answer-neither/ -->
<!--[if lt IE 7]><html class="ie ie6 ie-lte9 ie-lte8 ie-lte7 no-js" lang="es"> <![endif]-->
<!--[if IE 7]><html class="ie ie7 ie-lte9 ie-lte8 ie-lte7 no-js" lang="es"> <![endif]-->
<!--[if IE 8]><html class="ie ie8 ie-lte9 ie-lte8 no-js" lang="es"> <![endif]-->
<!--[if IE 9]><html class="ie9 ie-lte9 no-js" lang="es"> <![endif]-->
<!--[if (gt IE 9)|!(IE)]><!--> <html class="no-js" lang="es"> <!--<![endif]-->
<head>
<title>Example web scraping website</title>
  <!--[if !HTML5]>
      <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <![endif]-->
  <!-- www.phpied.com/conditional-comments-block-downloads/ -->
  <!-- Always force latest IE rendering engine
       (even in intranet) & Chrome Frame
       Remove this if you use the .htaccess -->

  <meta charset="utf-8" />
```

```
  <!-- http://dev.w3.org/html5/markup/meta.name.html -->
  <meta name="application-name" content="places" />

  <!--  Mobile Viewport Fix
        j.mp/mobileviewport & davidbcalhoun.com/2010/viewport-metatag
        device-width: Occupy full width of the screen in its current orientation
        initial-scale = 1.0 retains dimensions instead of zooming out if page height > device
height
        user-scalable = yes allows the user to zoom in -->
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />

  <link rel="shortcut icon" href="/places/static/images/favicon.ico" type="image/x-icon">
  <link rel="apple-touch-icon" href="/places/static/images/favicon.png">

  <!-- All JavaScript at the bottom, except for Modernizr which enables
       HTML5 elements & feature detects -->
  <script src="/places/static/js/modernizr.custom.js"></script>

  <!-- include stylesheets -->


  <script type="text/javascript"><!--
    // These variables are used by the web2py_ajax_init function in web2py_ajax.js (which is
loaded below).
    var w2p_ajax_confirm_message = "¿Está seguro que desea borrar este objeto?";
    var w2p_ajax_disable_with_message = "Trabajando...";
    var w2p_ajax_date_format = "%d/%m/%Y";
    var w2p_ajax_datetime_format = "%d/%m/%Y %H:%M:%S";
    var ajax_error_500 = 'Ha ocurrido un error, por favor <a
href="/places/default/index">recargar</a> la página'
    //--></script>

<meta name="keywords" content="web2py, python, web scraping" />
<meta name="generator" content="Web2py Web Framework" />
<meta name="author" content="Richard Penman" />
<script src="/places/static/js/jquery.js" type="text/javascript"></script><link
href="/places/static/css/calendar.css" rel="stylesheet" type="text/css" /><script
src="/places/static/js/calendar.js" type="text/javascript"></script><script
src="/places/static/js/web2py.js" type="text/javascript"></script><link
href="/places/static/css/web2py.css" rel="stylesheet" type="text/css" /><link
href="/places/static/css/bootstrap.min.css" rel="stylesheet" type="text/css" /><link
href="/places/static/css/bootstrap-responsive.min.css" rel="stylesheet" type="text/css"
/><link href="/places/static/css/style.css" rel="stylesheet" type="text/css" /><link
href="/places/static/css/web2py_bootstrap.css" rel="stylesheet" type="text/css" />




  <!-- uncomment here to load jquery-ui
       <link rel="stylesheet"
href="http://ajax.googleapis.com/ajax/libs/jqueryui/1.10.3/themes/ui-lightness/jquery-ui.css"
type="text/css" media="all" />
       <script src="http://ajax.googleapis.com/ajax/libs/jqueryui/1.10.3/jquery-ui.min.js"
type="text/javascript"></script>
       uncomment to load jquery-ui //-->
  <noscript><link href="/places/static/css/web2py_bootstrap_nojs.css" rel="stylesheet"
type="text/css" /></noscript>

</head>

<body>
  <!-- Navbar ================================================== -->
  <div class="navbar navbar-inverse">
    <div class="flash"></div>
    <div class="navbar-inner">
      <div class="container">

        <!-- the next tag is necessary for bootstrap menus, do not remove -->
        <button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-
collapse" style="display:none;">
          <span class="icon-bar"></span>
          <span class="icon-bar"></span>
          <span class="icon-bar"></span>
```

```
        </button>

        <ul id="navbar" class="nav pull-right"><li class="dropdown"><a class="dropdown-toggle"
data-toggle="dropdown" href="#" rel="nofollow">Log In</a><ul class="dropdown-menu"><li><a
href="/places/default/user/register?_next=/places/default/index" rel="nofollow"><i class="icon
icon-user glyphicon glyphicon-user"></i> Sign Up</a></li><li class="divider"></li><li><a
href="/places/default/user/login?_next=/places/default/index" rel="nofollow"><i class="icon
icon-off glyphicon glyphicon-off"></i> Log In</a></li></ul></li></ul>
        <div class="nav">

          <ul class="nav"><li class="web2py-menu-first"><a
href="/places/default/index">Inicio</a></li><li class="web2py-menu-last"><a
href="/places/default/search">Buscar</a></li></ul>

        </div><!--/.nav-collapse -->
      </div>
    </div>
  </div><!--/top navbar -->

  <div class="container">
    <!-- Masthead ================================================== -->

    <header class="mastheader row" id="header">
        <div class="span12">
            <div class="page-header">
                <h1>
                    Example web scraping website
                    <small></small>
                </h1>
            </div>
        </div>
    </header>


    <section id="main" class="main row">


        <div class="span12">



<div id="results">
<table><tr><td><div><a href="/places/default/view/Afghanistan-1"><img
src="/places/static/images/flags/af.png" /> Afghanistan</a></div></td><td><div><a
href="/places/default/view/Aland-Islands-2"><img src="/places/static/images/flags/ax.png" />
Aland Islands</a></div></td></tr><tr><td><div><a href="/places/default/view/Albania-3"><img
src="/places/static/images/flags/al.png" /> Albania</a></div></td><td><div><a
href="/places/default/view/Algeria-4"><img src="/places/static/images/flags/dz.png" />
Algeria</a></div></td></tr><tr><td><div><a href="/places/default/view/American-Samoa-5"><img
src="/places/static/images/flags/as.png" /> American Samoa</a></div></td><td><div><a
href="/places/default/view/Andorra-6"><img src="/places/static/images/flags/ad.png" />
Andorra</a></div></td></tr><tr><td><div><a href="/places/default/view/Angola-7"><img
src="/places/static/images/flags/ao.png" /> Angola</a></div></td><td><div><a
href="/places/default/view/Anguilla-8"><img src="/places/static/images/flags/ai.png" />
Anguilla</a></div></td></tr><tr><td><div><a href="/places/default/view/Antarctica-9"><img
src="/places/static/images/flags/aq.png" /> Antarctica</a></div></td><td><div><a
href="/places/default/view/Antigua-and-Barbuda-10"><img
src="/places/static/images/flags/ag.png" /> Antigua and Barbuda</a></div></td></tr></table>
</div>

<div id="pagination">

    &lt; Previous

|

    <a href="/places/default/index/1">Next &gt;</a>

</div>


        </div>
```

```
    </section><!--/main-->

    <!-- Footer ================================================== -->
    <div class="row">
        <footer class="footer span12" id="footer">
        </footer>
    </div>

  </div> <!-- /container -->

  <!-- The javascript ============================================
       (Placed at the end of the document so the pages load faster) -->
  <script src="/places/static/js/bootstrap.min.js"></script>
  <script src="/places/static/js/web2py_bootstrap.js"></script>
  <!--[if lt IE 7 ]>
      <script src="/places/static/js/dd_belatedpng.js"></script>
      <script> DD_belatedPNG.fix('img, .png_bg'); //fix any <img> or .png_bg background-images
</script>
      <![endif]-->
</body>
</html>
```

13.2.2. Hash

A continuación, se muestra el hash calculado del código anterior.

```
ced79dfbb02b892a4396cb18780f420a830a1dc7575885c06f888905b67846a8
```

13.2.3. Respuesta TSA

A continuación, se muestra la respuesta obtenida del TSA.

```
TimeStampResp:
 status=PKIStatusInfo:
  status=granted

 timeStampToken=TimeStampToken:
  contentType=1.2.840.113549.1.7.2
  content=SignedData:
   version=3
   digestAlgorithms=DigestAlgorithmIdentifiers:
    DigestAlgorithmIdentifier:
     algorithm=2.16.840.1.101.3.4.2.1

   contentInfo=ContentInfo:
    contentType=1.2.840.113549.1.9.16.1.4

content=0x0481d03081cd020101060b2a84680186f6770205010b301f300706052b0e03021a0414dc49a2602f0c6c
b973817603bfc5ad5efc995ac40207038d7eafe43510180f32303139303630343138333233315a3003020101a07ba4
793077310b3009060355040613025043102504c3122302006035504 0a0c19556e697a65746f20546563686e6f6c6f67696573
20532e412e31273025060355040b0c1e43657274756d2043657274696669636174696f6e20417574686f7269747931
1b301906035504030c1243657274756d20455620545341205348413 2

   signerInfos=SignerInfos:
    SignerInfo:
     version=1
     issuerAndSerialNumber=IssuerAndSerialNumber:
      issuer=Name:
       =RDNSequence:
        RelativeDistinguishedName:
         AttributeTypeAndValue:
          type=2.5.4.6
          value=0x1302504c
        RelativeDistinguishedName:
         AttributeTypeAndValue:
          type=2.5.4.10
          value=0x1319556e697a65746f20546563686e6f6c6f6769657320532e412e
        RelativeDistinguishedName:
         AttributeTypeAndValue:
```

```
          type=2.5.4.11
          value=0x131e43657274756d204365727469666963617469 6f6e20417574686f72697479
        RelativeDistinguishedName:
         AttributeTypeAndValue:
          type=2.5.4.3
          value=0x131943657274756d2054727573746564204e6574776f726b204341


      serialNumber=338163361017072765325902304937699866224

     digestAlgorithm=DigestAlgorithmIdentifier:
      algorithm=2.16.840.1.101.3.4.2.1
      parameters=0x0500

     authenticatedAttributes=Attributes:
      Attribute:
       type=1.2.840.113549.1.9.3
       values=SetOf:
        0x060b2a864886f70d0109100104
      Attribute:
       type=1.2.840.113549.1.9.5
       values=SetOf:
        0x170d313930363034313833323315a
      Attribute:
       type=1.2.840.113549.1.9.4
       values=SetOf:
        0x0420141c8e373ff6cce91c804d3d0ad6290577e97daa0dcd4f07c8dc280b49174437
      Attribute:
       type=1.2.840.113549.1.9.16.2.12
       values=SetOf:

0x3081b83081b53081b204144f8d4c480649426aef8b86d4d5fc7932e7142d85308199308183a48180307e310b3009
060355040613025042c31223020060355040a1319556e697a65746f20546563686e6f6c6f6769657320532e412e3127
3025060355040b131e43657274756d204365727469666963617469 6f6e20417574686f726974793122302006035504
03131943657274756d2054727573746564204e6574776f726b204341021100fe67e4f15a24e3c60d547ca020c27670

     digestEncryptionAlgorithm=DigestEncryptionAlgorithmIdentifier:
      algorithm=1.2.840.113549.1.1.1
      parameters=0x0500


encryptedDigest=0x9c9e71eaba83c05d40a9a9b230c22d62ed1985da51f9c679f5def028b0d209870fb9b2e072b9
6fe53677af07357170bba77ec24b5b539ade394733943cc3eb77920c6dbd9c3bc9ca240c5f32f7dbc710bbb9ab9eef
f36858ccd27701cb7083bf89c028c443f168dccda5c1ad299ec0a828f108ec672704961f0b87340219ca3927d3e003
f7c5061038e137bede2735831094fa6c5222ec21e2641062cb78755cde70e2fa6b21fa8c8e18affd157c5f429d58b8
31e23508726a380da22f77ced8d4955791e20f9b063a0289c58e16689a323834568c50075f7d0f563b87179c00b58b
29615a06cf0fa66345af976dffcd38f21b8e204b9728280451becc363df8
```

13.2.4. Registro

A continuación, se muestra un ejemplo del registro de capturas de evidencias digitales:

ID	Label	Time-Stamp	Hash	TSA	Commentary
1	LogIn	20190526_10_26_3	ced79dfbb02b892a4396cb18780f420a830a1dc7575885c06f888905b67846a	8a7a49fa8022982ac4f5839ebce07fff848def6ae44d2ae26733be6cb73dd7646199423	
2	SignUp	20190526_10_26_3	907ef23ca27c9fd79dcdcc8455ecb6f0ee8d5e133c7402666b846b2ffb6d53bb	58d82c1b569110527acdf804ec55b39b8dc1a2c99faf961863e09ff4bc28414f10fb09c	
3	LogIn	20190526_10_26_4	17f5f70980925da3a3d143439ba66b5de741742897b0edd4d60eaadf42a969c	6ae32160ef4c7a9f1addc09ba6f1b0d216cb4cd6eb3cc00e50ed8c14dcb02504ad98b1	
4	Inicio	20190526_10_26_4	ced79dfbb02b892a4396cb18780f420a830a1dc7575885c06f888905b67846a	3bb612613897ece0a7eb157680b25b77298f49cd4e82a8e35e6d1b913b590f5461d17	
5	Buscar	20190526_10_26_4	187d889648552e2d59153b607f79d63d1af7cd31bfa42381294996bd6a7d75	2bea1b408e913c850adc99b0ea36b0da7107eea04da60abe5c869ba1cc01047a9529	
6	Afghanistan	20190526_10_26_5	e2858e1fc62ff3f5f97911addca27b8b92d9159cc0582d25044b30ce55054660	623fd1c4c33813e835aa708fdaaeac9efb2d0e5e5955a3aaafa762c36cc657366b1f6ac	
7	Alandislands	20190526_10_26_5	23b3239d520e8d3436f1e42f53568e6b3363e16a11e7b2568a2a1899db7829	71a98e150464a08c6763717ba7bf822235069c17e655c299d9e289f6de9ad5dea369c	
8	Albania	20190526_10_26_5	148b9b9a24a3f9180Od049ed9afe45e39d1999eda1b6629cbf883a3ecaffb3de	55cb963af5f473feba5a2682e5157d19f21075bba13080b6721921fa391048a2e8644c	
9	Algeria	20190526_10_27_0	d1a75569b3397574237677ce0cb039984fe9f9569f22568b5e62ac3c622d551	3322971d8ca9a16160426b58a01be542354a03e4b2c2844b3709346156 26b9481fc7	
10	AmericanSamoa	20190526_10_27_0	1babd2891e8562e8022f11c33818faf8698a27744ad79868d82a7c52f2ba7ac	a327428694e336d3c5f29125b076cf896e8bf609972fce81f0adaaadd5db97e97fbf53c	
11	Andorra	20190526_10_27_1	f731d69555b7d1b8515c6f2fb8688aa939b2f00a39e48490f1e5066dabb952e	2435c4b40b906bbdb9aa25c0ff8fcc746b52d0e1570440855330b45b0399ce9388908e	
12	Angola	20190526_10_27_1	a2db66e979644a2b6854a3ecf937116ceebb2ddd750e60a36bb662f6cd4176e	a1742cd1be66ed07a2ead2c789c8719b0ce36d113b03ebda7a0ea87f2a6a97f11d21b	
13	Anguilla	20190526_10_27_1	261349508e875727fc6dffbf92c0bbe2332da06fe477612aa8eb6596c585f894	b366a9ef353ed00240ae082e0ac6c33c5685d73145Oe4714d1079986bd4f7dc3739eb	
14	Antarctica	20190526_10_27_2	cfe9faf71e31d71b261250838e018f30e3a35a69fc123813f6f3667752ff8899	927bfd57e282a5ac39df399e9ddcd94bc92b8ce252dc22b450737d6d9c8f8afe426173	
15	AntiguaandBarbuda	20190526_10_27_2	3e0982eb52b8a363058e3d20bc60015332bab18649545bc039e94e3b06c7e5	693f02681090d7a5a6c351de2977461c71c868e695e47ce93af12ec16d21a6254473d	
16	Next	20190526_10_27_2	7e68d61f5d30f464fb2e2470ba5a6020f51ce2a1c547088cbf1b4585ce15628d	4400dc6fcdf702da5db091144d9db09131cfa4641d99b6c805db542c105a134a4aedf3	