



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Evolución a Infraestructura Digital Eficiente para el manejo de evidencias en el entorno jurídico

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: José Alberto Pérez Martín

DIRECTORES: Luis Álvarez Sabucedo
Isidro Fernández García

CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Evolución a Infraestructura Digital Eficiente para el manejo de evidencias en el entorno jurídico

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de Telecomunicación

UniversidadeVigo

RESUMEN

En este trabajo, se plantea una evolución de del conjunto de procesos que dan soporte al manejo de las evidencias digitales mediante infraestructuras modernas de comunicación. Partiendo de un modelo en el que estos procesos se realizan en gran medida de manera manual, se persigue una mejora digital que permita la automatización y mejora en la seguridad de dicho proceso, además de un uso más racional de los recursos humanos y materiales. Para ello, se propone una transformación digital mediante la creación de una plataforma digital que introduzca elementos que mejoren y ofrezcan garantías adicionales al procedimiento.

Uno de los objetivos parciales planteados de cara a este objetivo global es la realización de un análisis del sistema actual utilizado por las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) para la recogida de evidencias digitales, que pueden surgir en cualquier intervención policial o judicial. A continuación, se examinará cómo se lleva a cabo la cadena de custodia de estas evidencias, garantizando su seguridad e integridad hasta que son presentadas ante la autoridad judicial competente o utilizadas en la fase oral del proceso. En este análisis se destacarán los aspectos que actualmente representan desafíos y limitaciones en dicho procedimiento.

Una vez expuesto el procedimiento y funcionamiento actual, se planteará una solución de mejora mediante la transformación digital, que abarque desde el inicio de la cadena de custodia. Para ello, se plantea el desarrollo de una plataforma digital de uso común para las FCSE y la Administración de Justicia, que permita optimizar la gestión y el intercambio de evidencias digitales. Dicha plataforma de gestión de evidencias se desarrolla con una interfaz interactiva y funcionalidades avanzadas de gestión, integrando un alto nivel de seguridad para garantizar la integridad de los datos, respaldada por las tecnologías más modernas.

Además de la mayor agilidad y cooperación que esta plataforma facilitaría entre los diferentes organismos implicados, se pretende garantizar un nivel superior de seguridad para las evidencias digitales, no solo asegurando su integridad mediante la implementación de una red blockchain, sino también aplicando tecnología NFT para reforzar la autenticidad y trazabilidad de cada evidencia. Esto permitirá una mayor confianza en el proceso, desde la recogida de la prueba hasta su presentación ante el tribunal.

PALABRAS CLAVE

Policía judicial, científica, evidencia digital, custodia, plataforma, intercambio, justicia, FCSE, blockchain, NFT

AGRADECIMIENTOS

Quiero expresar mi más sincero agradecimiento, en primer lugar, a mi familia: a mi madre y a mi pareja, por su apoyo incondicional, cariño y ayuda durante este largo trabajo, cuyo desarrollo no habría sido posible sin el tiempo y el respaldo que me brindaron. También deseo recordar a mi hermana y a mi padre, que aunque ya no están conmigo, siempre ocuparán un lugar especial en mi vida y me acompañan en espíritu.

Asimismo, agradezco a mis compañeros de trabajo y a mis jefes por darme la oportunidad de realizar este máster y por su apoyo, directo o indirecto, en este camino.

Extiendo también mi gratitud a los profesores que, con sus enseñanzas, hicieron posible el desarrollo de este máster, y de manera especial a mis directores de Trabajo de Fin de Máster, D. Luis Modesto Álvarez Sabucedo y D. Isidro Fernández García, cuya orientación y dedicación fueron fundamentales para la realización de este proyecto.

Por último, quiero agradecer al Centro Universitario de la Defensa, a la Escuela Naval Militar, a la Universidad de Vigo, y a todos los miembros de estas instituciones. También mi reconocimiento a mis compañeros y colegas del máster en Dirección TIC para la Defensa del curso 2023-2025, cuya colaboración y compañía han aportado un constante aprendizaje y enriquecimiento tanto profesional como personal.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	4
1 Introducción y objetivos	5
1.1 Motivación	5
1.2 Antecedentes	5
1.3 Contexto	7
1.4 Objetivos	9
1.5 Estructura del documento.....	10
2 Marco normativo	11
2.1 Introducción	11
2.2 Cadena de custodia y evidencias digitales. Legislación nacional.	11
2.3 Directrices técnicas y normativas complementarias	14
2.4 Normativa europea y comunitaria	14
2.4.1 Reglamento General de Protección de Datos	14
2.4.2 Órdenes europeas de producción y conservación de pruebas electrónicas.....	15
2.4.3 Convenio de Budapest	16
3 Estado del arte: tratamiento de evidencias digitales.....	19
3.1 Implementaciones y tendencias actuales en las FCSE.....	19
3.1.1 Competencias, recogida, remisión y recepción de evidencias digitales	20
3.1.2 Copiado forense de soportes informáticos.....	21
3.1.3 Análisis forense de soportes informáticos	22
3.2 Cadena de custodia.....	22
3.2.1 Definición	22
3.2.2 Procedimiento	22
3.3 Seguridad de la información	24
3.4 Metodología en otras organizaciones internacionales	25
4 Necesidad de transformación digital en organizaciones policiales	29
4.1 Consulta a las organizaciones policiales	30
4.1.1 Objetivo	30
4.1.2 Consulta ejecutiva/directiva.....	31
4.1.3 Consulta operativa	37
4.1.4 Conclusiones.....	47

5 Tecnología, metodología y arquitectura aplicada al dato.....	49
5.1 Integridad y autenticidad.....	49
5.1.1 Sistema de gestión de certificados PKI	50
5.1.2 Tecnología Blockchain, Smart Contract y NFTs.....	51
5.2 Modalidades de almacenamiento	53
5.3 Arquitectura	55
5.3.1 Descripción general	55
5.3.2 Componentes técnicos	56
5.4 Aplicación tecnológica a nuestra plataforma	57
5.4.1 Relación Blockchain-NFT-Evidencias Digitales.....	57
5.4.2 Ejemplo práctico	59
5.4.3 Detalles Técnicos y ventajas de implementación.	60
6 Propuesta de plataforma de intercambio de evidencias digitales	61
6.1 Introducción	61
6.2 Casos de uso.....	62
6.3 Diseño de sistema BACKEND	63
6.4 Diseño de sistema FRONT	64
6.4.1 Elementos principales del diseño.....	65
6.4.2 Herramientas utilizadas	65
6.4.3 Mockups y estructura visual	65
6.5 Usuarios, roles y funciones	66
6.6 Auditoría y control de datos.....	68
6.7 Infraestructura física y hardware.....	71
6.7.1 Infraestructura física	71
6.7.2 Hardware.....	73
6.8 Plan de formación	74
6.8.1 Diseño del plan de formación	75
6.8.2 Métodos de seguimiento y evaluación.....	75
6.8.3 Recursos necesarios	76
7 Conclusiones	77
8 Bibliografía.....	79
Anexo I: Acrónimos utilizados.....	81
Anexo II: Mockup EviCloud.....	82

ÍNDICE DE FIGURAS

Figura 1-1 Cibercriminalidad España (Observatorio Español de Delitos informáticos).....	7
Figura 2-1 Ciclo de vida evidencia digital (Govertis- part of Telefónica Tech).....	14
Figura 3-1 Hoja de Solicitud de Informe Pericial	21
Figura 3-2 Hoja de copiado forense de dispositivos informáticos	22
Figura 3-3 Diagrama de flujo Cadena de Custodia	23
Figura 4-1 Portada de la consulta a las organizaciones policiales.....	30
Figura 4-2 Consulta ejecutiva.....	37
Figura 4-3 Consulta operativa	47
Figura 5-1 Infraestructura de llave pública PKI.....	50
Figura 5-2 Funcionamiento Blockchain	51
Figura 5-3 Funcionamiento Smart contract.....	52
Figura 5-4 Arquitectura en capas de plataforma	56
Figura 6-1 Plan de Formación	75
Figura A-1 Acceso a Plataforma Evicloud.....	82
Figura A-2 Evicloud/Agente_investigador	82
Figura A-3 Evicloud/Agente_investigador/Mandamientos_judiciales	83
Figura A-4 Evicloud/Agente_investigador/Evidencia_digital	83
Figura A-5 Evicloud/Agente_investigador/Evidencia_digital_campo_requerido	84
Figura A-6 Evicloud/Administrador_del_sistema.....	84
Figura A-7 Evicloud/Autoridad_judicial.....	85
Figura A-8 Evicloud/Auditor	85

ÍNDICE DE TABLAS

Tabla 5-1 – Modalidades de almacenamiento 54

Tabla 6-1 – Herramientas Tecnológicas.....69

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Motivación

El exponencial crecimiento de los ciberdelitos y la proliferación de evidencias digitales en investigaciones judiciales plantean desafíos significativos para los sistemas legales y de seguridad en todo el mundo. En la actualidad, los métodos tradicionales de gestión y almacenamiento de evidencias, como el uso de soportes físicos, en ocasiones han demostrado ser insuficientes para garantizar la integridad, accesibilidad y seguridad de las pruebas. Este panorama motiva la necesidad de una transformación digital que optimice estos procesos, asegurando que la cadena de custodia sea confiable y adaptada a las exigencias del entorno digital. Mi interés en este trabajo radica en aportar una posible solución innovadora que permita abordar estas carencias, creando una infraestructura digital eficiente y segura que beneficie tanto a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) como al sistema judicial en su conjunto.

La motivación principal surge de la posibilidad de explorar y proponer una solución integral que no solo modernice la gestión de evidencias, sino que también reduzca riesgos como la pérdida de pruebas o la corrupción de datos. Este enfoque, además, abre la puerta a la colaboración interdisciplinar, integrando conceptos de ciberseguridad, blockchain y NFT, y dejando otras ventanas abiertas para una mayor evolución a otras tecnologías emergentes, con el objetivo de fortalecer la confianza en los sistemas judiciales y promover una justicia más ágil y efectiva en la era digital.

1.2 Antecedentes

Para abordar los antecedentes relacionados con las evidencias digitales y la cadena de custodia, los dos pilares fundamentales sobre los que se desarrolla este trabajo, es necesario referirse a dos áreas que, aunque surgieron en momentos distintos, se han entrelazado a lo largo del tiempo, volviéndose mutuamente indispensables para su correcto funcionamiento.

Policía científica

Como breve introducción a la misma, indicaremos que este concepto nació en nuestro país en 1882, en el que se reconoce por primera vez un sistema antropométrico identificativo desarrollado por el

francés Alphonse Bertillon¹. Dicho sistema permitía asegurar la identificación de un delincuente mediante una serie de datos referentes a la descripción, marcas particulares, fotografía e impresiones digitales de los dedos.

También hemos de mencionar a Edmond Locard, quien, a través del establecimiento de cuatro principios en 1910, se le considera padre de la criminalística y mediante los cuales se apoya la actividad que conocemos como policía científica o ciencias forenses.

Los cuatro principios que se hace referencia en su trabajo son: principio de transferencia, principio de reconstrucción de hechos, principio de correspondencia y principio de probabilidad. Siendo los dos últimos los que mayor correlación tienen con las evidencias digitales, ya que hacen referencia a la relación de los indicios con el autor del hecho (correspondencia) y la deducción de la posibilidad o no de un fenómeno con base en el número de características verificadas en un cotejo (probabilidad). [1]

Desde el inicio de la policía científica y hasta la actualidad se han desarrollado una serie de diferentes disciplinas dentro de las ciencias forenses, pudiendo destacar entre otras: antropología, entomología, toxicología, balística, documentoscopia, informática, etc. Dentro de las mencionadas anteriormente y de la que nos ocuparemos en mayor medida debido a la relación con este trabajo, está la informática forense.

Informática forense

La informática forense es una disciplina que surge a partir del desarrollo de los primeros sistemas de computación en la década de 1940 y la necesidad de investigar delitos relacionados con el uso de la tecnología. En sus inicios, la informática forense se centraba en la recuperación de datos borrados o dañados, con un enfoque muy técnico, pero sin reconocimiento formal en el ámbito judicial.

Con el avance de la tecnología y la masificación del uso de ordenadores y redes, especialmente desde los años 80, la necesidad de investigar delitos informáticos, como fraudes financieros o accesos no autorizados entre otros, se hizo más evidente. Fue en esta época cuando las primeras técnicas de análisis digital empezaron a desarrollarse de manera formal, permitiendo la recopilación, preservación y análisis de datos electrónicos.

El reconocimiento de las evidencias digitales como pruebas válidas en un juicio no se consolidó hasta finales de los años 90 y principios de los 2000, cuando los tribunales empezaron a aceptar archivos digitales (como correos electrónicos, archivos de registro, y documentos electrónicos) como evidencia en procesos judiciales, siempre que se garantizara su integridad. A partir de entonces, la informática forense adquirió un rol clave en las investigaciones policiales y judiciales, gracias a la capacidad de asegurar que la información digital no fuera manipulada durante la recolección y el análisis.

Hoy en día, con el crecimiento exponencial de la tecnología, las evidencias digitales son fundamentales en prácticamente todas las investigaciones criminales. La informática forense no solo se encarga de recuperar datos, sino de garantizar que las pruebas digitales mantengan su integridad a lo largo de toda la cadena de custodia, permitiendo su uso fiable en tribunales y reforzando su importancia en la lucha contra el crimen en la era digital.

En última instancia y para situar finalmente la temática de nuestro trabajo, nos quedan por mencionar dos conceptos clave que definiremos brevemente.

Evidencia digital

Son datos o información almacenados o transmitidos en formato digital que pueden ser utilizados como prueba en investigaciones legales o judiciales. Pueden incluir documentos electrónicos, correos, registros de transacciones, imágenes, videos, y cualquier otro tipo de información digital relevante para un caso.

¹ Policía Científica. 100 años de Ciencia al servicio de la justicia. Catálogo de Publicaciones de la Administración General del Estado (AGE): <http://www.publicacionesoficiales.boe.es>

Cadena de custodia

Es el proceso de documentación y control que asegura la integridad y autenticidad de la evidencia, desde su recogida hasta su puesta a disposición en un órgano judicial. Este seguimiento riguroso garantiza que la evidencia no ha sido manipulada ni alterada

1.3 Contexto

En primer lugar, debemos reseñar el crecimiento exponencial del número de ciberdelitos que se llevan registrando desde el año 2011 hasta la actualidad por medio del Observatorio Español de Delitos Informáticos (OEDI). En la gráfica siguiente se observa como la cantidad de delitos oficiales en 2011 fueron 37.485, teniendo por cifra en 2022 unos 374.737. Lo que supone un incremento del 899.7% desde entonces y del 22.67% con respecto a 2021 con 305.477 delitos registrados.

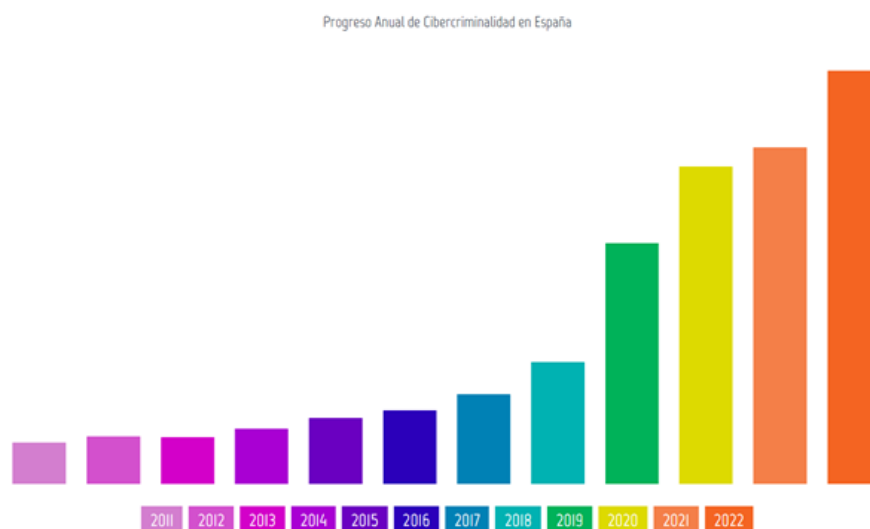


Figura 1-1 Cibercriminalidad España (Observatorio Español de Delitos informáticos)

Estos datos aportados por esta entidad son datos públicos que aparecen en el Informe sobre la Cibercriminalidad en España de 2022, realizado por la Dirección General de Coordinación y Estudios de la Secretaría de Estado de Seguridad (SES) del Ministerio del Interior. [2]

Desde la experiencia profesional podría decir que el número sea posiblemente bastante más elevado ya que muchas de las personas afectadas por estos delitos no realizan denuncia por motivos diversos como ser delitos de menor entidad, vergüenza por haber sido engañados o por la entidad del delito en sí o la dificultad de restitución del mal causado entre otros.

Gran parte de estos delitos son de tipo informático, otros se han realizado mediante algún medio o instrumento el cual puede dejar alguna evidencia electrónica. Los delitos a los que referimos son: fraude informático, amenazas, coacciones, falsificación informática, acceso e interceptación ilícita, contra el honor, delitos sexuales, interferencia en los datos y el sistema, contra la propiedad industrial/intelectual, contra la salud pública, etc.

Los números previamente mencionados nos hacen tener una idea aproximada del volumen y el crecimiento de los procedimientos o intervenciones policiales o judiciales en los que, de alguna forma, están involucradas evidencias digitales.

Por cada uno de estos sucesos ocurridos, el tipo de evidencia digital que se genera puede ser diferente, enumerando entre otros: imágenes, videos, conversaciones, metadatos, correos electrónicos,

archivos y documentos electrónicos, dispositivos móviles y de almacenamiento, registros de transacciones, contraseñas y credenciales, software o código malicioso, etc.

Se ha realizado un estudio aproximado para el cálculo de almacenamiento de todos estos datos generados en estos sucesos. En el caso de Policía Nacional, se reciben una media de 40TB/mes de datos que deberán ser evidenciados. Datos que entre otros se deben a informes periciales de la Comisaría General de Policía Científica y las intervenciones de la Comisaría General de Policía Judicial y Comisaría General de Información. Se estima un alcance similar para las Unidades de Guardia Civil.

La gran cantidad de datos y dispositivos que se obtienen y almacenan, a menudo permanecen en las instalaciones de la unidad correspondiente de los cuerpos de seguridad que intervinieron en su obtención hasta que su remisión es solicitada a la autoridad judicial. En otras ocasiones, estas evidencias son enviadas a las diferentes unidades de policía científica para su análisis, extracción y estudio. También pueden ser remitidas a la autoridad judicial para su custodia hasta la celebración del juicio. Dependiendo de la evidencia en sí, la tipología del delito, del juzgado que lo instruya y otros factores, el tiempo que transcurre desde la obtención de la evidencia hasta su presentación en juicio puede extenderse desde meses hasta años. También debemos de considerar el tiempo que las evidencias se almacenan hasta que pueden ser destruidas, lo que viene indicado más adelante en el apartado del marco normativo, según lo establecido por la ley.

En España, la custodia de evidencias judiciales, particularmente en el ámbito de los cuerpos de seguridad, está evolucionando para adaptarse a los desafíos tanto de las pruebas físicas como digitales. La cadena de custodia es fundamental para asegurar que las evidencias recogidas en un hecho criminal se mantengan íntegras y auténticas durante todo el proceso judicial, desde su recogida en el lugar de los hechos hasta su presentación en un juicio.

Las evidencias físicas, como drogas incautadas o armas, deben seguir protocolos muy específicos que aseguren su correcta identificación, almacenamiento, custodia y análisis. Este proceso está regulado por diversas normativas, como la Ley de Enjuiciamiento Criminal (LECrim) y acuerdos internacionales, que detallan cómo deben documentarse y manipularse estas pruebas para evitar su contaminación o pérdida de integridad. Sin embargo, aún se enfrentan desafíos relacionados con la uniformidad y precisión en la aplicación de estos protocolos, lo que puede llevar a absoluciones si se demuestran fallos en la cadena de custodia.

La cadena de custodia digital es especialmente delicada debido a la facilidad con la que las pruebas electrónicas pueden ser manipuladas o alteradas sin dejar rastro evidente. Las pruebas digitales, como los datos de dispositivos electrónicos, requieren un tratamiento aún más riguroso. Los tribunales españoles han subrayado la importancia de seguir estrictamente los protocolos de cadena de custodia digital, como la identificación de las "claves HASH" que verifican la autenticidad de los datos. Cualquier fallo en este proceso puede llevar a la exclusión de la prueba, como se evidenció en casos recientes donde la inadecuada custodia de pruebas digitales resultó en la absolución de los acusados.

En ambos tipos de cadena de custodia existe una parte de gestión y control que se realiza manualmente. Es en esta parte en la que al depender del factor humano cabe la posibilidad que se cometa un error invalidando la evidencia como prueba.

Es importante tener en cuenta que, actualmente, en relación con muchas de las evidencias electrónicas, se almacenan en soportes físicos. Es por esto que el volumen físico que ocupan y la acumulación en unidades con espacio de almacenamiento limitado generan un problema significativo. Asimismo, la integridad de estos soportes puede verse comprometida debido a su deterioro físico, lo que en ocasiones impide que funcionen correctamente cuando se requiere su peritaje o análisis y, por tanto, no pueden ser considerados pruebas válidas.

Por lo tanto, podemos afirmar que a lo largo del tiempo han surgido una serie de retos que, con el transcurso de los años, han ido adquiriendo una mayor relevancia en la actualidad. Nos referimos de una manera específica a los siguientes:

- Aumento del volumen de forma exponencial de casos de cibercriminalidad y de otro tipo, en los que se generan evidencias electrónicas como prueba.
- Capacidad física de almacenamiento en las unidades policiales/judiciales de los múltiples tipos de dispositivos de evidencia.
- Integridad física y deterioro de los soportes de almacenamiento de las evidencias.
- Integridad de la evidencia o del dato, cadena de custodia.
- Trazabilidad total de cada evidencia.
- Demora o falta de agilidad en determinados procesos, como solicitud y remisión de autorizaciones judiciales.

1.4 Objetivos

El objetivo de este trabajo es la propuesta de un despliegue a nivel interno de Guardia Civil y Policía Nacional de una herramienta de gestión o plataforma, que permita el intercambio de información digital generada en las diferentes evidencias forenses como archivos multimedia y demás evidencias electrónicas. El sistema precisará una plataforma de almacenamiento ágil, y de grandes dimensiones a la que tengan acceso tanto las FFCCSE como la Administración de Justicia.

Para este objetivo global, se necesitan cumplir una serie de objetivos secundarios, de manera que al cumplir todos ellos, alcancemos el objetivo global con las mejores garantías posibles. Los objetivos secundarios a los que nos referimos son:

- Objetivo secundario 1 (OS1):

Realizar un estudio detallado de la situación actual y necesidades tanto de unidades centrales como periféricas de FCSE y la interacción entre las mismas y la administración de justicia en el proceso de intercambio de evidencias digitales. De esta manera se podrá tener una visión más detallada de los procesos que se van a digitalizar e incluir en la plataforma a desarrollar.

- Objetivo secundario 2 (OS2):

Evaluar el grado de satisfacción de las herramientas actuales y valorar la necesidad de una nueva solución.

- Objetivo secundario 3 (OS3):

Diseño de una arquitectura de servicio que permita dar cabida a una solución superadora del estado actual del arte a este respecto. Se busca que cumpla de una manera más eficiente con los requisitos judiciales y procedimentales actuales, garantizando la integridad del proceso en el tratamiento de evidencias digitales.

- Objetivo secundario 4 (OS4):

Provisión de un modelo o propuesta funcional, que permita implementar la arquitectura definida. Para ello, se escribirá la estructura y funcionamiento de la plataforma con el correspondiente flujo de negocio, casos de uso, perfiles y roles, administración, criptografía, integridad del dato a través de Blockchain como eje central y tecnología NFT, auditoría y control de datos.

Adicionalmente, se realizará una definición de la parte de hardware necesaria para dicha plataforma, las conexiones necesarias para dar servicio a las FCSE, garantizando la seguridad de las instalaciones y equipamiento y plena disponibilidad del servicio.

1.5 Estructura del documento

Siguiendo el índice como referencia y los capítulos principales de este, vamos a explicar la estructura que hemos seguido en dicho trabajo y como en cada uno de los capítulos o en varios de ellos se han desarrollado los objetivos secundarios que hemos referido en el apartado anterior.

En primer lugar, en el capítulo 1, se presenta una contextualización e introducción a la situación actual en el ámbito digital y la gestión de evidencias, acompañada de una breve exposición de los objetivos que se persiguen con este trabajo y una descripción de la estructura del documento.

A continuación, en los capítulos 2, 3 y 4, abordan una descripción más detallada de diversos aspectos, incluyendo el marco normativo, el estado del arte en el tratamiento de evidencias digitales, y un análisis de la necesidad que impulsa este trabajo, sustentado en consultas y análisis directos con profesionales cuya labor diaria está vinculada al uso, gestión y control de evidencias digitales.

Posteriormente, en los capítulos 5 y 6 se desarrolla de manera progresiva la propuesta de la plataforma, comenzando con una introducción a las tecnologías que se pretenden utilizar, justificando su elección y explicando su aplicación. Seguidamente, se presenta la propuesta de una plataforma para el intercambio de evidencias digitales, diseñada para responder a las necesidades identificadas durante el análisis previo.

Finalmente, en el capítulo 7, se exponen los resultados obtenidos y las conclusiones alcanzadas tras el desarrollo de este trabajo.

De este modo el lector puede encontrar una respuesta adaptada a los objetivos identificados en estos capítulos, en particular podemos establecer la siguiente relación entre objetivos y capítulos:

Objetivo Secundario 1 (OS1):

Se aborda en los capítulos 1(Introducción y objetivos), 2(Marco normativo) y 3(Estado del arte).

Objetivo Secundario 2 (OS2):

Abordado en detalle en el capítulo 4(Necesidad de transformación digital en organizaciones policiales).

Objetivo Secundario 3 (OS3):

Se cubre en los capítulos 5(Tecnología, metodología y arquitectura aplicada al dato) y 6 (Propuesta de plataforma de intercambio de evidencias digitales).

Objetivo Secundario 4 (OS4):

Se desarrolla en el capítulo 6(Propuesta de plataforma de intercambio de evidencias digitales).

Finalmente se presentan en el capítulo 7 unas conclusiones y líneas futuras en las que se exponen las lecciones aprendidas y el camino que podría seguir este trabajo y que pueden ser de interés para el lector que desee continuar por esta senda.

2 MARCO NORMATIVO

2.1 Introducción

En este apartado se ofrece una visión conceptual desde el enfoque normativo que influye, de forma directa o indirecta, en el tratamiento de pruebas, tanto físicas como digitales. Se analizarán los aspectos relacionados con la obtención, custodia, metodología y buenas prácticas en estos procesos, prestando especial atención al marco normativo nacional. No obstante, dado que en ocasiones los delitos pueden tener un alcance transnacional, también se incluirá una referencia a la normativa internacional y comunitaria pertinente.

2.2 Cadena de custodia y evidencias digitales. Legislación nacional.

En primer lugar, se realiza una pequeña definición de la **cadena de custodia** desde el punto de vista normativo que es el que ocupa este apartado. Se define como el conjunto de pasos que se siguen desde la intervención de un objeto relacionado con un delito por parte de los agentes policiales, hasta su presentación y análisis en un proceso judicial. Este proceso tiene como objetivo asegurar que el objeto intervenido sea el mismo que se examina y se presenta en el juicio, garantizando que no ha sufrido alteraciones, manipulaciones o reemplazos, ya sea de manera intencionada o accidental.

Otra definición más actualizada que proporciona la Sala 2ª del Tribunal Supremo en STS 93/2024, de 31 de mayo, seguida por la STS 1012/2024, de 13 de noviembre es: “podemos definirla como la garantía de la autenticidad de los elementos probatorios recogidos durante la fase de investigación preliminar, al incidir sobre las condiciones de conservación del cuerpo y de los efectos e instrumentos del delito, de modo que no haya duda de que sean ellos mismos los elementos sobre los que se verifiquen las oportunas pericias, o sean mostradas en el juicio oral, como auténticas piezas de convicción.”

Es importante también hablar de la **admisibilidad** de una prueba en el proceso penal español. Para que esto ocurra, depende de que haya sido obtenida de manera legal y respetando los derechos fundamentales. Para que una prueba sea admitida, debe cumplir con los principios de relevancia, licitud y pertinencia. Cualquier prueba obtenida de manera ilícita, como mediante violación de derechos fundamentales o sin respetar la cadena de custodia, puede ser declarada inadmisibile, lo que impide que sea utilizada en un juicio.

En el marco español, la **Ley de Enjuiciamiento Criminal (LECrim)**²[3], establece los procedimientos y condiciones para garantizar un proceso justo. Haciendo referencia a la correcta metodología de

² Ley de Enjuiciamiento Criminal (Última modificación por Ley Orgánica 1/2015). España.

conservación y transmisión de las pruebas desde su recogida hasta su presentación en juicio, y cómo esto afecta a la integridad de las evidencias. Con la reforma de la Ley Orgánica 13/2015, de 5 de octubre, es cuando se introducen referencias más precisas sobre cómo deben ser gestionadas estas pruebas para garantizar su integridad y autenticidad.

En el **artículo 282** de la LECrim habla sobre la policía judicial y de cómo el Juez de Instrucción les asigna la función de asegurar las piezas de convicción relacionadas con el delito.

“El Juez de Instrucción tiene entre sus funciones propias e inherentes a su labor instructora la de recoger, por sí o a través de la Policía Judicial, los bienes o efectos que tengan relación con el delito, ya porque el delito se haya cometido sobre ellos, ya porque hayan sido utilizados para su comisión o porque procedan del mismo; y además habrá de disponer lo necesario para su conservación para el juicio o, en otro caso, conferirlos el destino previsto legal o reglamentariamente”

En el **artículo 334** de la misma ley habla sobre la recogida y conservación de los objetos relacionados con el delito en los primeros momentos de la investigación.

“El Juez instructor ordenará recoger en los primeros momentos las armas, instrumentos o efectos de cualquiera clase que puedan tener relación con el delito y se hallen en el lugar en que éste se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida. El secretario judicial extenderá diligencia expresiva del lugar, tiempo y ocasión en que se encontraren, describiéndolos minuciosamente para que se pueda formar idea cabal de los mismos y de las circunstancias de su hallazgo.”

En el **artículo 338** se establece en que la forma de recogida de las pruebas garantice la integridad de estas y que sean remitidas y/o custodiadas por el organismo competente.

“Sin perjuicio de lo establecido en el Capítulo II bis del presente título, los instrumentos, armas y efectos a que se refiere el artículo 334 se recogerán de tal forma que se garantice su integridad y el Juez acordará su retención, conservación o envío al organismo adecuado para su depósito.”

En los **artículos 588 bis a** (principios rectores), **588 bis b** (solicitud de autorización judicial) y **588 bis k**, se regulan aspectos fundamentales sobre la autorización, ejecución y tratamiento posterior de las medidas de investigación tecnológica. Estas disposiciones destacan la importancia de garantizar la proporcionalidad, la necesidad y la correcta eliminación de registros, asegurando así el equilibrio entre los derechos fundamentales y la eficacia en la investigación de delitos.

Hay que destacar que en el **artículo 588 bis k**, se habla sobre la destrucción de registros, y en los puntos **2** y **3**, se especifica el tiempo de conservación, la destrucción definitiva de registros y la responsabilidad en quien recae, del siguiente modo:

“2. Se acordará la destrucción de las copias conservadas cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal.

3. Los tribunales dictarán las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción contemplada en los anteriores apartados.”

También es relevante la **Ley Orgánica 1/2015** de 30 de marzo [4], que modifica la Ley Orgánica 10/1995, de 23 de noviembre, del **Código Penal**, especialmente en lo referente a delitos informáticos y cibercriminalidad, que establece la relevancia de las evidencias digitales en la investigación de este tipo de delitos. Y donde recalca la importancia desde que las evidencias son recogidas hasta que son presentadas en los procesos judiciales, garantizando la integridad de estas.

Otro aspecto importante es el que señala la **Ley 25/2007, de 18 de octubre** [5], sobre conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, establece obligaciones específicas para los operadores de telecomunicaciones en relación con la conservación de datos que puedan ser relevantes en la investigación de delitos graves.

En los **artículos 3, 5 y 7** se mencionan respectivamente aspectos de importancia como:

- Obligaciones de conservación por el operador durante 12 meses datos para identificar usuarios, fecha, duración de la comunicación, equipo utilizado y localización. Datos completamente utilizables en procedimientos judiciales.
- Acceso a datos conservados, únicamente con autorización judicial y en el marco de una investigación sobre delitos graves. Este punto refuerza la necesidad de garantizar el cumplimiento de la cadena de custodia en el manejo de estos datos.
- Protección de datos conservados, en el que se obliga a los operadores a garantizar la seguridad y confidencialidad de los datos, evitando accesos no autorizados y asegurando su integridad durante el período de conservación.

Por último, pero no menos importante, se expone parte de la visión que tiene el **Tribunal Supremo**. Su concepción sobre la cadena de custodia es clara, ya que la considera fundamental para garantizar la validez de las pruebas en el proceso penal. Según jurisprudencia, la cadena de custodia si se realiza de forma correcta permite garantizar la autenticidad e integridad de las pruebas, desde el momento de su obtención hasta su presentación en juicio, evitando cualquier manipulación, alteración o pérdida que pueda comprometer su fiabilidad.

El Tribunal Supremo establece que la ruptura de la cadena de custodia puede provocar que la prueba pierda su valor probatorio, afectando su admisibilidad en juicio. Por eso, es fundamental que en cada fase del proceso (obtención, almacenamiento, traslado y presentación) se documente adecuadamente por quién, cómo y cuándo se manipulan las pruebas para garantizar su conservación en condiciones óptimas.

En numerosas ocasiones, se cuestiona si ha ocurrido una ruptura en la cadena de custodia con el fin de invalidar las pruebas y, en consecuencia, su valor en el juicio. A continuación, se presentan algunos ejemplos, como el caso planteado por una de las partes defensoras mediante un recurso de casación ante el Tribunal Supremo, alegando este motivo. Sin embargo, dicho recurso fue desestimado al no acreditarse la manipulación de pruebas (**STS 2570/2024**[8]). Asimismo, existen otras sentencias en un sentido similar, aunque emitidas por órganos judiciales de menor rango, como la **STSJ CAT 6401/2024**, de 16 de julio.

En el mismo sentido, recientemente existe otra sentencia del Tribunal Supremo (**STS**) **54/2024**, de 18 de enero, donde se ofrece otro ejemplo sobre la relevancia de la cadena de custodia y las implicaciones de su ruptura, además de abordar cuestiones relacionadas con el almacenamiento masivo de datos de tráfico y localización. En esta sentencia vuelve a incidir en que la cadena de custodia no constituye una prueba en sí misma, sino que actúa como una garantía formal de autenticidad e indemnidad de la prueba. La infracción de esta afecta a la verosimilitud de la prueba, comprometiendo su admisibilidad y eficacia en el proceso judicial.

En relación con esta última sentencia mencionada, la parte sobre el almacenamiento masivo de datos de tráfico y localización refiere que, es fundamental que la conservación y el acceso a estos datos se lleven a cabo bajo estrictas garantías legales, protegiendo los derechos fundamentales y previniendo injerencias desproporcionadas en la privacidad de las personas.

Como cierre a este apartado, se puede decir que en cierta manera la normativa española da los medios necesarios para garantizar la cadena de custodia, la cual es clave para la integridad y validez de las pruebas en un proceso penal. Tanto la legislación como la jurisprudencia insisten en la importancia de un manejo adecuado de las pruebas, ya sean físicas o digitales, para evitar su manipulación o alteración. Además, se subraya que la ruptura de esta cadena puede comprometer la admisibilidad de las pruebas en juicio, afectando el desarrollo del proceso judicial.

2.3 Directrices técnicas y normativas complementarias

En España, además de las normativas nacionales, existen normas técnicas que se aplican al tratamiento de evidencias digitales. La Norma UNE 71505 [6] sobre la "Seguridad en los sistemas de información y la evidencia digital" establece requisitos técnicos y buenas prácticas para la gestión de pruebas digitales.

Esta norma se considera marco de referencia o manual de buenas prácticas en la gestión de evidencias digitales a lo largo de todo el ciclo de vida de estas. Si bien, aunque no todas ellas se den en cada evidencia podemos destacar principalmente las siguientes fases:

- Generación
- Almacenamiento
- Transmisión
- Recuperación (extracción y exportación)
- Tratamiento (consolidación, agregación, correlación)
- Comunicación



Figura 2-1 Ciclo de vida evidencia digital (Govertis- part of Telefónica Tech)

También podemos añadir que esta norma tiene amplia relación con el desarrollo nuestro trabajo, puesto que se utiliza principalmente en Sistemas de Gestión de Evidencias Digitales (SGEE), y también en todos aquellos procedimientos donde se realizan intercambios de evidencias, de manera que aseguren la integridad y confianza de los datos.

2.4 Normativa europea y comunitaria

En relación con la normativa europea que puedan afectar o servir como referencia en relación con la protección de datos y evidencias digitales en el ámbito internacional, destacamos a nivel europeo el Reglamento General de Protección de Datos y el Convenio de Budapest.

2.4.1 Reglamento General de Protección de Datos

A nivel comunitario, el Reglamento General de Protección de Datos (GDPR)³ o Reglamento 2016/679 [7], como ley comunitaria que, aunque centrada en la protección de datos personales de las personas físicas y a la libre circulación en la Unión Europea y el Espacio Económico Europeo, tiene un

³ Reglamento General de Protección de Datos (RGPD). (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea, L119, 1-88

impacto en el manejo de evidencias digitales, particularmente en lo que se refiere a la gestión y almacenamiento de información personal contenida en dichas evidencias.

El artículo 32 del GDPR aborda las obligaciones de seguridad en el tratamiento de datos personales relativos a: la seguridad en el tratamiento, cifrado de datos personales, capacidad de garantizar confidencialidad, integridad, disponibilidad y resiliencia, responsable y encargado del tratamiento.

Este artículo se puede extrapolar a la necesidad de asegurar la integridad y confidencialidad de las evidencias digitales a lo largo de todo el proceso de la cadena de custodia.

Por otro lado, es importante resaltar la Directiva Europea (UE) 2016/680, que se enmarca en la protección de datos en el ámbito penal, garantizando los derechos de todas las personas implicadas en el proceso, ya sean testigos, víctimas o sospechosos. Esta normativa subraya varios puntos clave, exigiendo que las autoridades policiales traten los datos de manera justa, lícita y con fines legítimos, además de asegurar una protección adecuada. Asimismo, establece la obligación de garantizar la seguridad y registro de los datos, evitando el acceso no autorizado, su copia, modificación o eliminación indebida, y asegurando su almacenamiento correcto. Una vez más, observamos la importancia de seguir pautas que aseguren la integridad y seguridad de los datos.

2.4.2 Órdenes europeas de producción y conservación de pruebas electrónicas

El **Reglamento (UE) 2023/1543** del Parlamento Europeo y del Consejo, de 12 de julio de 2023 ⁴, constituye un avance significativo en la cooperación judicial en materia penal dentro de la Unión Europea.

Este reglamento es relevante en el contexto de este trabajo, ya que regula la obtención y conservación de evidencias digitales transfronterizas, abordando desafíos clave como la inmediatez, la integridad de la prueba y la protección de derechos fundamentales. Además, establece estándares claros para la cooperación entre Estados miembros, garantizando una mayor eficiencia y seguridad jurídica en el manejo de datos digitales sensibles.

Su ámbito de aplicación incluye datos esenciales para esclarecer delitos graves, como los datos de abonados, datos de tráfico y otras pruebas electrónicas. Dentro de este reglamento, se destacan una serie de aspectos importantes como:

➤ **Orden europea de producción (EPOC)**

Definición (artículo 3.1): es un instrumento legal que permite requerir datos específicos de una persona o entidad que preste servicios en otro Estado miembro, siempre que dichos datos sean necesarios para un procedimiento penal o para la ejecución de una pena privativa de libertad. Se aplica a datos de abonados, datos de acceso, datos de tráfico y datos de contenido.

Ejecución de una EPOC (artículo 10)

Establece que el proveedor de servicios debe transmitir los datos solicitados directamente a la autoridad competente del Estado miembro requirente dentro del plazo establecido (normalmente 10 días). En casos de urgencia, este plazo se puede reducir a 8 horas. Las transmisiones deben garantizar la integridad, confidencialidad y autenticidad de los datos.

⁴ Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo de 12 de julio de 2023 sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales

➤ Orden europea de conservación (EPOC-PR)

Definición (artículo 3.2): es una herramienta destinada a preservar temporalmente datos almacenados, asegurando que estén disponibles para futuras solicitudes de acceso o producción en el contexto de una investigación penal.

Ejecución de una EPOC-PR (artículo 11)

Obliga al proveedor de servicios a conservar los datos solicitados durante un período inicial de 60 días, prorrogables si la autoridad judicial competente lo requiere. Durante este tiempo, los datos no pueden ser eliminados ni modificados.

Otras definiciones que también hemos encontrado interesantes mencionar que aparecen en el reglamento, debido a las similitudes encontradas con el marco normativo español son las siguientes:

- **Pruebas electrónicas:** cualquier dato almacenado o transmitido por medios electrónicos que pueda ser relevante en el marco de un procedimiento penal.
- **Datos de abonados:** los datos de abonados donde se identifican a los usuarios de servicios electrónicos (nombre, dirección, etc.)
- **Datos de tráfico:** los datos de tráfico que hacen referencia a información sobre la comunicación en sí (hora, duración, ubicación, etc.), crucial para rastrear actividades ilícitas.

2.4.3 Convenio de Budapest

Otro de los referentes clave a nivel internacional es el Convenio sobre la Ciberdelincuencia o Convenio de Budapest⁵ sobre el Ciberdelito del año 2001 del Consejo de Europa [9], considerado también un marco jurídico clave. Aunque es un tratado internacional, tiene implicaciones directas sobre la cooperación transnacional en la investigación de delitos informáticos, y establece principios sobre la obtención y preservación de evidencias electrónicas en este tipo de investigaciones.

A fecha de febrero de 2024 existen 69 países que forman parte de este Convenio, la mayor parte de los países europeos junto con otros de gran notoriedad como Australia, Estados Unidos, Japón, Argentina, Canadá entre otros. 2 países más han firmado hace poco (Irlanda y Sudáfrica) y otros 22 que han sido invitados a su adhesión.

Uno de los puntos que dicho Convenio prevé y que está ligado con el tema de este trabajo, es dotar de herramientas de derecho procesal para hacer más efectiva la investigación de ciberdelitos o de otros en los que hay obtención de evidencias electrónicas.

Posteriormente este convenio se completa con una serie de protocolos en los que se han ido trabajando entre los años 2017 y 2021, no siendo hasta mayo de 2022 cuando se firma el Segundo Protocolo Adicional relativo a la cooperación internacional avanzada y la divulgación de pruebas electrónicas.⁶

Este segundo protocolo introduce varias medidas clave para preservar la integridad de las pruebas electrónicas cuando son solicitadas y transmitidas en el contexto de la cooperación internacional. Dado que las pruebas digitales son especialmente vulnerables a la alteración o destrucción, el protocolo establece mecanismos y procedimientos que garantizan su autenticidad y fiabilidad durante todo el proceso de intercambio transfronterizo. [10]

Parte de las medidas a las que hace referencia son:

- Preservación rápida de los datos.

⁵ <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>

⁶ <https://www.coe.int/en/web/cybercrime/t-cy-drafting-group>

- Conservación de la cadena de custodia (registro detallado y trazabilidad).
- Uso de copias autenticadas.
- Transmisión segura de datos.
- Auditoría y control de acceso.
- Normas técnicas uniformes.
- Destrucción de datos innecesarios.

3 ESTADO DEL ARTE: TRATAMIENTO DE EVIDENCIAS DIGITALES

El objetivo de este capítulo, a través de sus distintos apartados, es ofrecer un enfoque integral sobre el tratamiento de evidencias digitales, estableciendo una base sólida para comprender el estado actual, principalmente en el ámbito nacional, con algunas referencias internacionales. Asimismo, se pueden inferir las posibles direcciones en el futuro de la gestión de evidencias y la seguridad digital en el contexto policial, en base a las necesidades existentes.

3.1 Implementaciones y tendencias actuales en las FCSE

En el ámbito del tratamiento de evidencias digitales, la Guardia Civil y la Policía Nacional, como cuerpos con competencias similares, aplican procedimientos parecidos. No obstante, este apartado se centrará en el modelo utilizado por la Policía Nacional, ejemplificado a través del **Manual de Normas Generales** de la Unidad Central de Criminalística [19], dependiente de la Comisaría General de Policía Científica. Este documento regula los procedimientos aplicados por los Laboratorios de Informática Forense, tanto centrales como territoriales, para la gestión de evidencias digitales.

Características del Manual de Normas Generales:

- Cumplimiento obligatorio a todos los niveles de competencia.
- Unificación y sistematización en el tratamiento de evidencias digitales.
- Estandarización de operaciones en cada etapa del proceso.
- Protocolo detallado para la actuación forense.

Este manual se organiza en cinco procedimientos ordenados o títulos generales, que también podemos entender como una serie de fases que explicaremos para tener un conocimiento de los procedimientos actuales en la manipulación de evidencias digitales. Los títulos son:

1. Competencias, recogida, remisión y recepción de evidencias digitales.
2. Copiado forense de soportes informáticos.
3. Análisis forense de soportes informáticos.
4. Análisis de dispositivos móviles.
5. Análisis de dispositivos electrónicos.

3.1.1 Competencias, recogida, remisión y recepción de evidencias digitales

En este apartado omitiremos la parte de competencia por falta de relevancia en el trabajo, detallando y contextualizando el resto [16]. El manual clasifica las evidencias digitales en tres tipos principales:

➤ **Soportes informáticos:**

Incluyen hardware y software que almacenan y procesan información, como ordenadores sobremesa, portátiles y dispositivos portátiles alimentados por baterías.

➤ **Terminales de telefonía móvil:**

Dispositivos como smartphones y tabletas, junto con sus componentes internos (memoria, tarjetas SIM, tarjetas adicionales).

➤ **Dispositivos electrónicos:**

Incluyen dispositivos como skimmers⁷, lectores de banda magnética y hardware utilizado en la manipulación de cajeros automáticos o terminales de pago electrónico.

Para la **recogida** de soportes informáticos o terminales móviles, en un registro con evidencias digitales se debe tener en cuenta una serie de **consideraciones básicas**, como utilizar herramientas adecuadas y advertir sobre los riesgos de una mala manipulación, que podría invalidar las pruebas.

Por otro lado, existen otro tipo de **consideraciones especiales** del siguiente tipo:

- Si el equipo está encendido, si el equipo se apaga correctamente, los datos en memoria se guardarán en el disco, preservando la estructura del sistema de archivos, pero esto podría activar procesos configurados por el usuario, como el borrado de información. Apagar cortando la alimentación evita estos procesos, pero puede dañar la estructura del sistema de archivos. La elección del método debe considerar la gravedad del delito y el perfil técnico del usuario.
- Tras el apagado, la CPU debe protegerse para su remisión, registrando marca, modelo y número de serie en el acta. Otros dispositivos con capacidad de almacenamiento, como cámaras, reproductores o consolas, también deben protegerse y documentarse en el **acta de inspección ocular**. (Es en este punto donde propiamente dicho comenzaría la cadena custodia)
- En el caso necesario de encendido por causa de fuerza mayor, se evitará cualquier alteración de la evidencia utilizando sistemas especializados que no modifiquen el contenido (bloqueadores CD o memoria USB o dispositivos preparados).
- En dispositivos móviles, se recomienda activar el "modo avión", NUNCA desconectar, o utilizar bolsas Faraday para evitar la conectividad.

Remisión y recepción de evidencias:

Solo se aceptarán elementos intervenidos mediante un procedimiento legal que cumpla con las siguientes condiciones:

1. **Cadena de custodia correcta y petición judicial** que justifique la necesidad de un análisis técnico-científico.
2. **Urgencia:** en casos de autorización judicial en trámite, las evidencias se almacenarán hasta obtener el permiso.

Se realizará un estudio preliminar de los objetos recibidos, detallando su estado técnico y posibles deterioros en el informe pericial que se realice a posteriori. Si los soportes corresponden a distintas personas o registros, deberán etiquetarse y diferenciarse claramente.

⁷ Un skimmer es un dispositivo utilizado para robar información de tarjetas de crédito o débito, generalmente instalado de manera encubierta

La remisión de los efectos debe cumplir con los siguientes documentos:

- Oficio judicial que autorice el análisis.
- Oficio de la unidad solicitante describiendo el material remitido.

3.1.2 Copiado forense de soportes informáticos

Tiene como objetivo garantizar la obtención de copias fieles de las evidencias, preservando su integridad. Esta acción se realiza en un entorno aislado, libre de conexiones a internet o redes internas; compuesto por hardware y software que impiden la modificación accidental de los datos, conociéndose dicho ecosistema como **entorno forense**. [24]

Se realizará por personal especializado, y preferentemente la copia se hará en forma de imagen o contenedor de evidencia. Si bien en ocasiones debido a determinadas circunstancias técnicas se opta por un duplicado o clon forense.

Procedimiento:

- Verificar de manera previa la existencia de documentos clave: oficios judiciales, solicitud pericial y hoja de solicitud de informe pericial.
- Realizar una identificación detallada de los soportes mediante marca, modelo y número de serie.
- Fotografiar los dispositivos antes de su desmontaje y registrar los datos en una hoja forense.

Figura 3-1 Hoja de Solicitud de Informe Pericial

Obtención de la copia forense

La conexión del soporte al entorno forense debe realizarse utilizando hardware bloqueador de escritura para evitar modificaciones en el original. También se pueden emplear métodos alternativos como bloqueadores por software o entornos forenses Live-CD previamente validados.

La copia puede realizarse en forma de:

- **Imagen o contenedor de evidencia** (recomendado): usando software como *Encase* (.e01), con bloqueo de escritura y partición de archivos en segmentos menores a 4 GB. Excepcionalmente, se puede optar por formatos como RAW o imágenes en un solo archivo.
- **Duplicado o clon forense**: antes de copiar, el disco de destino debe esterilizarse (wipeado). Tras el clonado, se verificará mediante algoritmos como Checksum64 que el contenido original y el de la copia son idénticos y no ha habido alteraciones en este proceso.

El software de copiado forense deberá estar configurado para la realización de firma digital o **Hash**⁸ del soporte copiado, obteniendo el mismo mediante el algoritmo **SHA1 o MD5** para mayor seguridad y garantizar la integridad de la copia.

Como fase documental de este proceso habrá que rellenar la “hoja de copiado forense de dispositivos informáticos”, con los datos e incidencias como que el soporte está defectuoso o errores de lectura. Se incluye el hash en la columna de observaciones.

Hoja de Copiado Forense de Dispositivos Informáticos

CASO	EVIDENCIA		SOPORTE		CLONADO		FUNCIONARIO	FINALIZACIÓN		UBICACIÓN	OBSERVACIONES	FOTOGRAFÍA
	Nº	Evidencia	Soporte	Nº	Día	Hora		Día	Hora			

Figura 3-2 Hoja de copiado forense de dispositivos informáticos

3.1.3 Análisis forense de soportes informáticos

En relación con los análisis forenses, sin entrar en mucho detalle solo comentaremos que en dicha fase no existe un procedimiento formal aplicable de la misma manera a todos los casos ya que, dependiendo del tipo del delito, objeto del informe, cantidad y tipo de evidencia los pasos variarán.

Posteriormente a la realización del análisis forense se procede a la remisión de del original, sin modificar, y la evidencia fruto del análisis junto al **informe pericial** de la misma donde se incluyen las conclusiones basadas en la evidencia científica.

La evidencia original se devuelve intacta, con el mismo hash que se creó de manera inicial para garantizar la integridad de dicha evidencia que en ningún momento ha sido alterada o modificada.

Los procedimientos realizados en todos estos procesos siguen normativas internacionales, como las ISO 17025 (Estándar de calidad en organismos de inspección y de competencia en laboratorios de calibración y ensayo [20]) y 27037:2012 (Guía para la identificación, incautación, adquisición y preservación de las evidencias digitales [21]).

3.2 Cadena de custodia

3.2.1 Definición

La cadena de custodia es el conjunto de actuaciones realizadas por los agentes de las Fuerzas y Cuerpos de Seguridad, orientadas a garantizar la integridad y permanencia de las evidencias desde el momento de su recogida hasta su presentación ante la autoridad judicial. Este proceso asegura que las pruebas presentadas en el juicio son exactamente las mismas que se obtuvieron en el lugar de los hechos, ya sea tanto en un entorno físico como digital. Cualquier alteración o irregularidad podría comprometer la validez procesal de dichas evidencias, afectando negativamente al caso.[22][23]

3.2.2 Procedimiento

Este apartado aborda el desarrollo completo del proceso, desde la recopilación de las pruebas hasta su presentación ante la autoridad judicial. En este recorrido, las pruebas pueden pasar por diferentes fases o acciones necesarias, implicando la transferencia de su custodia entre diversas “manos”.

⁸ Hash: función para resumir o identificar un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor. Uno de los métodos más usados es el conocido MD5, que es un algoritmo de reducción criptográfica de 128 bits. La probabilidad de que dos archivos tengan el mismo hash MD5 es de 2 elevado 128.

En este contexto, resulta pertinente referenciar el trabajo de fin de máster realizado por Don Diego Luis Santiago Gutiérrez durante el curso académico 2022-2023 en este mismo Máster Universitario, titulado “*La cadena de custodia mediante tecnología Blockchain*”. En dicho trabajo, se ofrece una definición y un análisis de la cadena de custodia de manera precisa y acertada. Como bien señala en el apartado 2.1 de su estudio, las Fuerzas y Cuerpos de Seguridad, en sus funciones de Policía Judicial, deben actuar conforme al ordenamiento jurídico y bajo las instrucciones de los órganos judiciales, entre los cuales se encuentran los jueces, tribunales y el Ministerio Fiscal. [11][12]

Por lo tanto, y perteneciendo a cuerpos hermanos, aunque este trabajo busca aportar nuevas perspectivas o matices al tema, es inevitable que ciertos aspectos coincidan, ya que el procedimiento y los principios que lo rigen no presentan variaciones sustanciales.

A continuación, se indica un diagrama de flujo sobre un ejemplo práctico en el marco del inicio de una intervención policial hasta la finalización de esta en el Juicio Oral ante la autoridad judicial. En el ejemplo se representa sobre una entrada/registro, incautación, remisión y análisis de un dispositivo digital de cualquier tipo como teléfono/USB/disco duro/portátil.



Figura 3-3 Diagrama de flujo Cadena de Custodia

En dicho diagrama se muestra el desarrollo del ejemplo que hemos comentado, se remarca la importancia de cada una de las fases evitar la alteración de las evidencias tanto físicas como digitales. También se manifiesta la cantidad de fases existentes, aquellas que están resaltadas en rojo es donde la cadena de custodia comienza desde que se incauta la evidencia, se traslada a dependencias policiales, se analiza, custodia y finalmente se remite al juicio oral. En todas esas fases las evidencias son tratadas de formas diferentes y por una variedad de personas.

Por tanto y observando la cantidad de posibles actores y acciones que se desarrollan en este procedimiento, es de vital importancia que la cadena de custodia y su trazabilidad se realice de forma escrupulosa y metódica, para que no exista fallo que invalide las evidencias.

Actualmente, la naturaleza de este proceso, aunque no esté formalmente procedimentada, podría considerarse mixta. Si bien existen documentos en formato digital, la mayoría comienza con un documento físico en papel. Este documento sirve para registrar datos clave relacionados con el inicio y los cambios en la cadena de custodia, como el carné profesional del funcionario, firma, fecha, dependencias, actuaciones e incidencias.

Las tecnologías empleadas para el almacenamiento seguro de evidencias digitales incluyen discos duros, USB y DVD. En caso de ser posible, se prefiere el uso de DVD, ya que este formato no permite modificaciones posteriores y facilita adjuntar una copia al archivo de las propias dependencias. Por otro lado, las imágenes forenses de dispositivos como móviles, ordenadores o unidades de almacenamiento

se guardan en discos duros o USB, dado que estas imágenes también están diseñadas para impedir cualquier alteración.

Las evidencias originales almacenadas en esos soportes físicos pueden permanecer meses o incluso años hasta que se autoriza el análisis o el volcado y la posterior remisión al juzgado. Mientras el almacenamiento y custodia de todas ellas se realiza en salas habilitadas para ello, pero en la mayoría de los casos no están adaptadas de manera especial para su conservación. [17]

3.3 Seguridad de la información

La seguridad de la información es fundamental para proteger la confidencialidad, integridad y disponibilidad de los datos en cualquier entorno digital, especialmente cuando se manejan activos que pueden actuar como evidencia digital.

En este contexto, el Esquema Nacional de Seguridad (ENS) recogido en el Real Decreto 311/2022 del 3 de mayo, establecido en el artículo 156.2 de la Ley 40/2015, 1 de octubre, de Régimen Jurídico del Sector Público establece un marco de referencia que recoge una serie de elementos esenciales para garantizar una gestión segura de la información.

El Esquema Nacional de Seguridad recoge los siguientes elementos a la seguridad de información aplicada al dato:

- **Mecanismo control de acceso y autenticación:** proceso que verifica la identidad de un usuario o sistema antes de otorgarle acceso a recursos exclusivos y/o privados.
- **Sellos de tiempo:** registro que verifica fecha y hora de creación o modificación del activo digital y se aplica a aquella información que pueda ser usada como evidencia digital en el futuro (integridad).
- **Firma electrónica:** mecanismo digital que asegura la identidad del firmante sobre un activo digital y que es utilizada en aquellos tipos previstos en el ordenamiento jurídico.
- **Certificados cualificados:** son credenciales digitales que garantizan la identidad de una persona o entidad, con validez legal y emitidas por una autoridad certificadora.
- **Criptografía:** técnica de codificación que protege la confidencialidad e integridad de los datos mediante el uso de algoritmos y claves, previniendo accesos no autorizados y alteraciones.
- **Auditoría y trazabilidad:** consiste en llevar un registro de actividades (logs) y accesos que permite detectar y rastrear incidentes, accesos, modificaciones, etc.
- **Marcado de soportes:** identificación física o digital de dispositivos de almacenamiento para controlar su contenido y asegurar el manejo adecuado de información sensible.
- **Custodia:** control que se realiza bajo la responsabilidad de la organización garantizando el acceso tanto con medidas físicas a los dispositivos, como de manera lógica.
- **Transporte:** fuera de las zonas de la organización, el transporte o bien a unidades para su análisis como remisión a la autoridad judicial, deben permanecer bajo control y manteniendo los requisitos de seguridad.
- **Borrado y destrucción:** borrado seguro según criterios y sensibilidad de la información y reutilización cuando sea posible (Guía CCN- STIC). Cuando la naturaleza del soporte de información no permita el borrado, se procederá a la destrucción.

Si consideramos todos estos elementos podremos hablar de un sistema integral de protección respecto al dato, el cual permite garantizar un manejo seguro de la información sensible manteniendo la cadena de custodia.

Por otro lado, y siguiendo el **Esquema Nacional de Seguridad (ENS)** [13], los nuevos sistemas de información desde su concepción y por real decreto, deben aplicar dicho esquema el cual está constituido por una serie de principios básicos y requisitos mínimos para una protección adecuada de la información.

Además, para definir el tipo de sistema de seguridad adecuado, es necesario atender a su **nivel de seguridad**, el cual se aplica tanto a las dimensiones de seguridad de los servicios o la información, como a las categorías de los sistemas de información.⁹ La categoría de un sistema se determina por la clasificación más alta que alcance alguna de las dimensiones de seguridad, en función de los servicios prestados o la información gestionada. Estas dimensiones se califican en **nivel bajo, medio o alto**, según el impacto que un incidente de seguridad tendría en las funciones de la organización, sus activos o las personas involucradas.

Otro aspecto clave en la seguridad de la información es la respuesta ante incidentes, donde el Centro Criptológico Nacional (CCN) juega un papel esencial en el marco del Esquema Nacional de Seguridad (ENS). El CCN coordina la respuesta técnica a incidentes de ciberseguridad en el sector público, desarrollando programas de formación y concienciación, validando perfiles de cumplimiento, y publicando instrucciones técnicas y guías de seguridad. A través del CCN-CERT, su unidad operativa, también ofrece soporte en la gestión de vulnerabilidades y en la resolución de incidentes, estableciendo las medidas necesarias para mitigar su impacto.¹⁰

En conclusión, los elementos descritos en el ENS ofrecen un marco integral y robusto para la protección de la información sensible y el mantenimiento de la cadena de custodia de la evidencia digital. Aplicar estos principios y requisitos desde la concepción de los sistemas de información no solo cumple con los estándares legales, sino que también fortalece la posición de las organizaciones frente a amenazas y garantiza una gestión responsable y segura de los datos en un entorno cada vez más digitalizado y dependiente de la integridad de la información.

3.4 Metodología en otras organizaciones internacionales

Es innegable que la tendencia global indica un aumento significativo en la incorporación de evidencias electrónicas como tipos de pruebas en los procesos legales, debido al impulso creado por la digitalización y el uso generalizado de tecnologías de la información.

Existen varios ejemplos de cómo diferentes países gestionan la cadena de custodia de evidencias digitales y garantizan su integridad y validez en el contexto judicial. Se han tomado como referencia algunos de los países punteros tecnológicamente o con un mayor volumen de casos judiciales simplemente por volumen de población.

Estados Unidos

En Estados Unidos, la gestión de la cadena de custodia de evidencias digitales está altamente reglamentada debido a la importancia del cumplimiento de las leyes federales y estatales [14][15]. Aquí podemos ver una serie de procedimientos y métodos que utilizan:

- **Reglas federales de evidencia** o *Federal Rules of Evidence*, las cuales requieren que la parte que presenta la evidencia demuestre que esta no ha sido alterada desde el momento en que se recogió.¹¹
- **Manuales** de diferentes tipos en los que se observa desde hace tiempo que trabajan en la misma línea, por ejemplo, “Mejores prácticas para la autenticación de Evidencias digitales or Best practices for authenticating Digital Evidence” escrito por Hon. Paul W. Grimm y Gregory P.

⁹<https://gobernanza.ccn-cert.cni.es/ens-navegable>

¹⁰<https://ens.ccn.cni.es/es/docman/documentos-publicos/21-infografia-05-ens-2022-el-papel-del-ccn-en-el-nuevo-ens/file>

¹¹ <https://www.law.cornell.edu/rules/fre>

Joseph, en la conferencia judicial del comité de asesoramiento sobre reglamentación en las evidencias.¹²

- Para garantizar la integridad de las evidencias digitales se utilizan métodos de **hash criptográfico** también conocidos y utilizados en otros países que mencionaremos más adelante, como es el cálculo de hash (SHA-256, MD5). Esto asegura que los archivos digitales no se hayan modificado desde su obtención.
- **Herramientas forenses certificadas**, utilizadas por las fuerzas del orden y expertos forenses para copiar discos duros, sistemas y otros dispositivos digitales de manera que la copia sea exacta y se mantenga la integridad de los datos originales. Herramientas como EnCase, que igualmente se utilizan en diferentes países de entorno internacional.
- **Testimonios periciales**, del mismo modo que de la cadena de custodia se tratara, los expertos forenses que manejan la evidencia digital testifican sobre el proceso de adquisición, análisis y presentación de la evidencia, explicando los pasos seguidos para preservar la integridad de los datos a través de estos testimonios.

Reino Unido

- **Reglamento ACPO** mediante la “**Guía de buenas prácticas para Evidencias Digitales**” o “*Good practice for Digital Evidence*” donde se recogen las pautas para la obtención y el manejo de evidencias digitales, siendo establecidas por la Asociación de jefes de Policía (ACPO, por sus siglas en inglés). Estas pautas incluyen una serie de principios básicos para garantizar la cadena de custodia de las evidencias digitales.

Los principios clave incluyen entre otros:

- No modificar los datos originales durante la obtención.
- Mantener un registro detallado de todos los pasos seguidos durante la adquisición y análisis de las evidencias.
- Solo los expertos forenses cualificados deben manipular las pruebas digitales.
- **Herramientas forenses especializadas**: al igual que en Estados Unidos, se utilizan herramientas como *X-Ways Forensics* o *Cellebrite* para recolectar y analizar datos de manera que se garantice su integridad.
- **Procedimientos judiciales**: los tribunales británicos requieren que las pruebas digitales sean presentadas en su forma original o con copias forenses debidamente verificadas, acompañadas de una cadena de custodia clara y verificable.¹³

Australia

- **Estándares AS 5388**: sigue dichos estándares para la gestión de la cadena de custodia en evidencias digitales. Estos estándares especifican cómo deben ser recolectadas, almacenadas, transportadas y analizadas las evidencias para mantener su validez. De manera paralela y como normativa adicional tanto en Australia como Nueva Zelanda siguen la **Guía de pautas de Evidencias Digitales** de la ANZPAA (Australia New Zeland Policing Advisory Agency).
- **Sistemas de gestión de evidencia digital**: en algunas jurisdicciones, Australia ya se utilizan sistemas especializados de gestión de evidencias digitales (como *CaseGuard* o *Evidence.com* de AXON) que facilitan el registro digital de la cadena de custodia, donde cada persona que accede a la evidencia queda registrada electrónicamente.

¹² https://www.uscourts.gov/sites/default/files/2016-04-evidence-agenda_book_final_0.pdf

¹³ <https://www.datainvestigations.co.uk/files/ACPO%20Guidelines%20Computer%20Evidence%20v4.pdf>

- **Hash criptográfico:** Al igual que en otros países, el uso de hash es una técnica esencial para garantizar la integridad de las evidencias digitales.^{14 15}

Alemania

- **Código de procedimiento penal alemán** (Strafprozessordnung, **StPO**): en dicho código, Alemania exige que toda evidencia, incluida la digital, sea recolectada y preservada siguiendo estrictas normas para garantizar su validez en los tribunales.
- **Uso de pruebas con imágenes forenses:** la Oficina Federal de Policía Criminal (Bundeskriminalamt) y otras fuerzas policiales emplean imágenes forenses de los sistemas y dispositivos digitales, en los que se hacen copias exactas (bit a bit) para preservar la evidencia original.
- **Herramientas forenses especializadas:** como *Magnet AXIOM* y *Caine* son empleadas para adquirir y analizar datos, con mecanismos integrados para garantizar la cadena de custodia digital y la integridad de los datos.
- **Sellos de tiempo electrónicos:** para asegurar que los datos no han sido manipulados tras su captura.
- **Cifrado y aseguramiento de evidencias:** en ocasiones las evidencias son cifradas durante su almacenamiento y transporte para garantizar que no se alteren ni se acceda a ellas sin autorización. Esta práctica viene regulada en la Oficina Federal de Seguridad de la Información (Bundesamt für Sicherheit in der Informationstechnik), como autoridad federal de ciberseguridad.

Cada uno de estos países emplea metodologías que aseguran la preservación de la integridad de las pruebas digitales a través de mecanismos como el hash criptográfico, herramientas forenses certificadas y el mantenimiento riguroso de la cadena de custodia.

En resumen, se observa que estos enfoques varían según la legislación de cada país, pero la constante en todos ellos es la importancia de la obtención meticulosa, el almacenamiento seguro y el seguimiento riguroso de la cadena de custodia para evitar que la evidencia sea cuestionada en el tribunal.

¹⁴ <https://www.anzpaa.org.au/products/products/australia-and-new-zealand-guidelines-for-digital-imaging-processes>

¹⁵ <https://evidence.com/>

4 NECESIDAD DE TRANSFORMACIÓN DIGITAL EN ORGANIZACIONES POLICIALES

Teniendo en cuenta la situación actual definida en los capítulos anteriores sobre el Estado del arte, relativo al tratamiento de evidencias digitales en el ámbito de las Fuerzas y Cuerpos de Seguridad del Estado, se resalta sobremanera la importancia y criticidad de este proceso. Es imprescindible que los procedimientos funcionen con la precisión de un reloj suizo, donde el más mínimo error o mal funcionamiento pueda comprometer su validez, generando consecuencias negativas que las organizaciones de seguridad del estado y administración de justicia no pueden permitirse.

Además, se han identificado áreas dentro de estos procedimientos que presentan oportunidades de mejora, tanto en términos de automatización como de eficiencia, para garantizar una mayor fiabilidad y eficacia en su aplicación.

La transformación digital en las organizaciones policiales no es solo una tendencia, sino una necesidad imperativa en el contexto actual marcado por el aumento de los ciberdelitos, el volumen de datos digitales y las expectativas de una respuesta más ágil y eficiente por parte de la ciudadanía. Este proceso implica integrar tecnologías avanzadas y reformar los procedimientos tradicionales para adaptarse a un entorno en constante evolución.

A continuación, se enumeran los factores clave que justifican esta necesidad, tal como se han observado:

1. Evolución en el panorama delictivo.
2. Crecimiento exponencial de evidencias digitales.
3. Optimización de recursos y procesos.
4. Mejora en la interoperabilidad y colaboración.
5. Cumplimiento normativo y fortalecimiento de la cadena de custodia.
6. Aumento de la confianza sobre este procedimiento.

Resumiendo, la transformación digital no solo es una oportunidad, es una necesidad urgente para que las organizaciones policiales se mantengan relevantes y efectivas en el siglo XXI. Adaptarse a este cambio implica enfrentar desafíos iniciales como la resistencia organizacional o los costos de implementación, pero los beneficios a largo plazo en términos de eficiencia, eficacia y confianza ciudadana superan con creces estas barreras en un entorno cada vez más digital.

4.1 Consulta a las organizaciones policiales

En este contexto de transformación digital, resulta fundamental comprender en detalle las necesidades y desafíos específicos que enfrentan las organizaciones policiales. Para ello, se llevaron a cabo consultas operativas y ejecutivas con el objetivo de obtener una perspectiva integral que sustente las conclusiones y propuestas de este trabajo. Dichas consultas se diseñaron para abordar tanto los aspectos estratégicos a nivel directivo como los retos prácticos enfrentados por los operadores en su interacción diaria con evidencias digitales. A continuación, se presenta un análisis detallado de estas consultas, incluyendo su metodología, resultados y las implicaciones clave para avanzar en la digitalización de los procedimientos policiales.



Figura 4-1 Portada de la consulta a las organizaciones policiales

4.1.1 Objetivo

El propósito principal de estas consultas fue identificar áreas críticas de mejora, validar las hipótesis del trabajo y proponer soluciones alineadas con las necesidades prácticas y estratégicas de los profesionales involucrados.

Para ello se han abordado dos perspectivas complementarias:

➤ Consulta ejecutiva o directiva

Orientada hacia responsables que lideran o han liderado unidades y grupos relacionados con este ámbito. Además de su experiencia, aportan una perspectiva más global y estratégica, identificando necesidades y oportunidades de mejora a nivel superior, donde se toman decisiones clave para la evolución hacia nuevos sistemas.

➤ Consulta operativa

Dirigida a aquellos profesionales que interactúan diariamente con las evidencias digitales. Su propósito era recabar información directa sobre los retos y necesidades prácticas del manejo de estas evidencias.

Ambas consultas se llevaron a cabo mediante Google Forms y fueron enviadas a profesionales especializados de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), principalmente de la Policía Nacional y la Guardia Civil, con experiencia directa y diaria o relación con el uso y manejo de evidencias digitales. La participación fue voluntaria, logrando un total de 7 respuestas en la consulta ejecutiva/directiva, enfocada en aspectos estratégicos, y 24 respuestas en la consulta operativa.

A continuación, se incluyen los formularios utilizados con sus respectivas preguntas y respuestas, seguidos de una síntesis de los resultados obtenidos para cada consulta.

4.1.2 Consulta ejecutiva/directiva

La consulta ejecutiva se centró en analizar las necesidades estratégicas y los desafíos a nivel organizativo. Las preguntas se orientaron hacia los siguientes aspectos clave:

- Identificación de prioridades estratégicas en la gestión de evidencias digitales.
- Evaluación de los principales obstáculos en la implementación de soluciones digitales.
- Impacto esperado de una plataforma centralizada y segura.

A continuación, se muestran imágenes y resultados de la consulta:

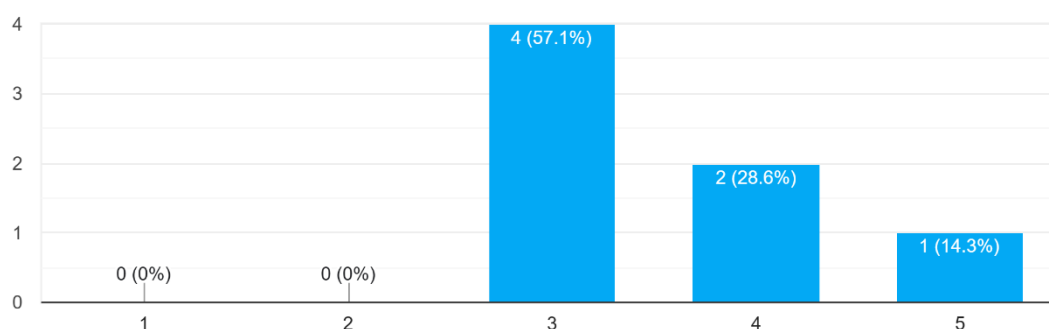
Formulario de consulta Plataforma evidencias digitales (ejecutiva/directiva)

B I U  

El propósito de esta encuesta es realizar un estudio sobre una posible transformación digital en el manejo de evidencias digitales, enfocándose en la implementación de una plataforma para el intercambio eficiente de evidencias entre distintas unidades y la autoridad judicial. **Su colaboración es altamente valorada.**

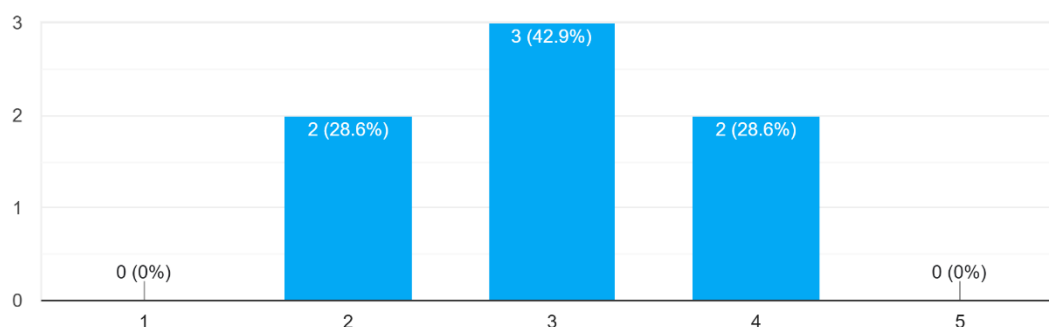
Valore de 1 a 5 cómo calificaría la eficiencia del proceso actual de manejo de evidencias digitales en términos de trazabilidad (siendo 1 muy ineficiente y 5 muy eficiente):

7 responses



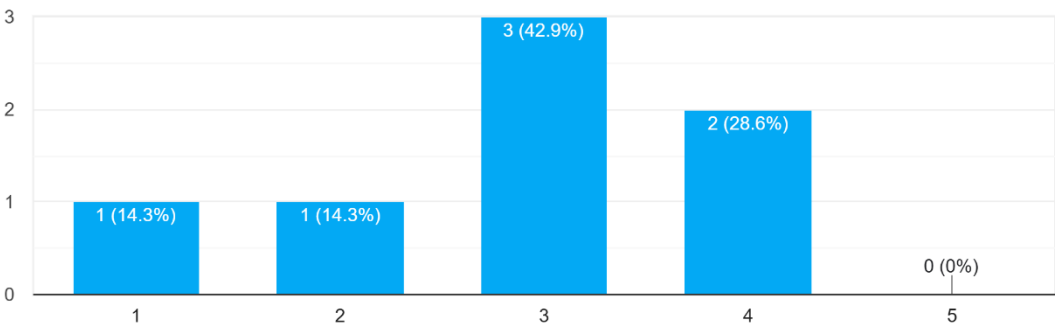
Valore de 1 a 5 cómo calificaría la eficiencia del proceso actual de manejo de evidencias digitales en términos de custodia (siendo 1 muy ineficiente y 5 muy eficiente):

7 responses



Valore de 1 a 5 cómo calificaría la eficiencia del proceso actual de manejo de evidencias digitales en términos de almacenamiento (siendo 1 muy ineficiente y 5 muy eficiente):

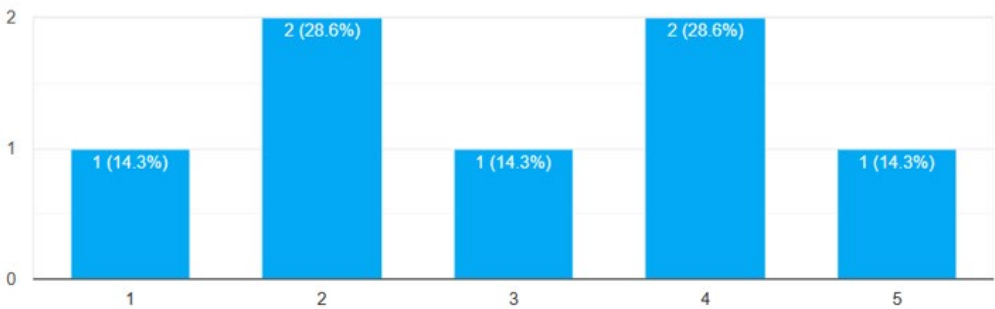
7 responses



Valore de 1 a 5 que impacto tienen cada una de las siguientes opciones en el proceso actual de custodia de evidencias digitales (siendo 1 no apreciado y 5 crítico):

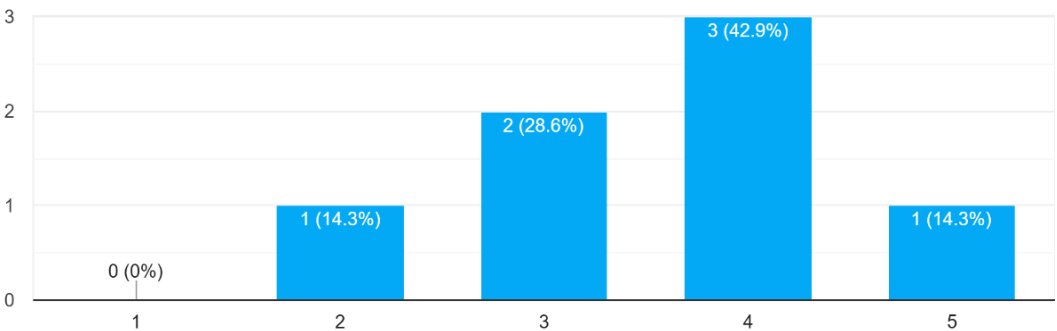
Falta de trazabilidad clara y confiable.

7 responses



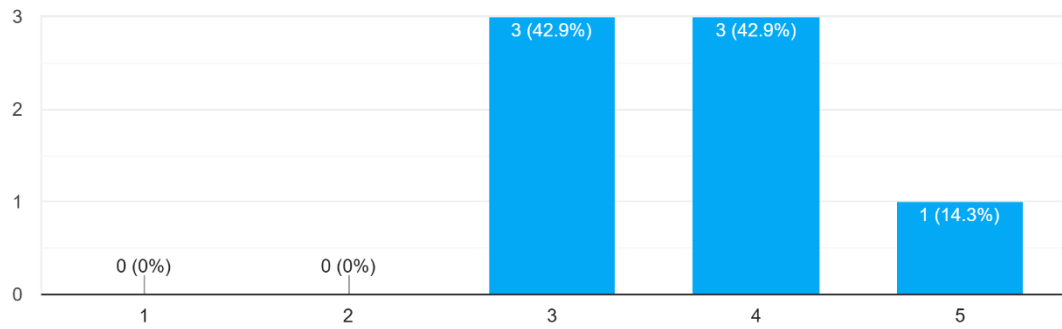
Vulnerabilidad a manipulaciones o pérdidas.

7 responses



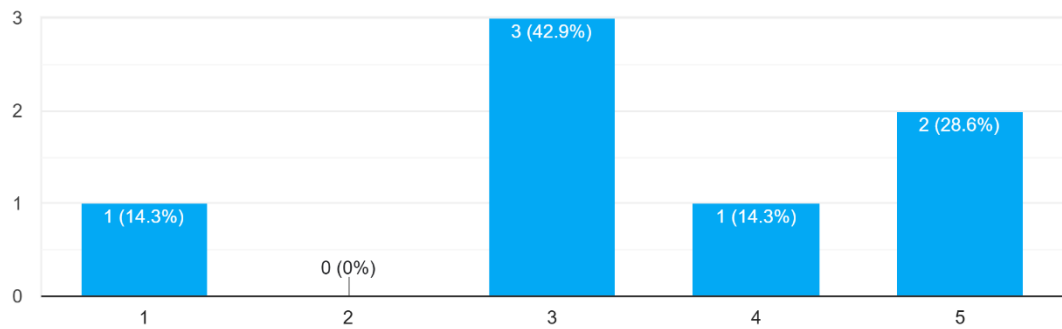
Costes elevados de almacenamiento físico.

7 responses



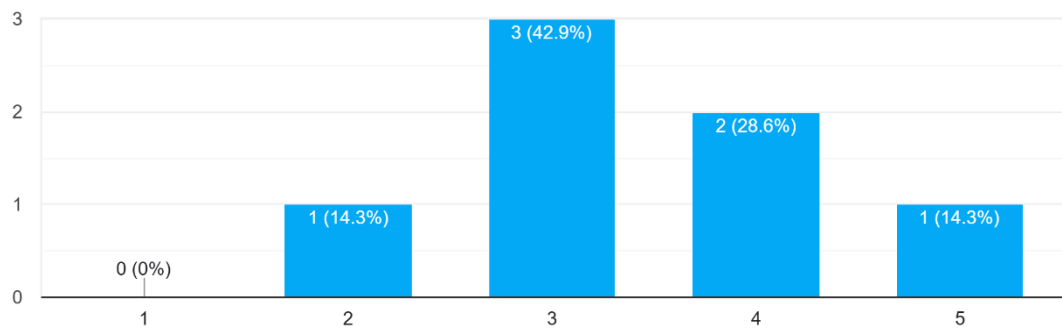
Retrasos en la coordinación entre unidades operativas y judiciales.

7 responses



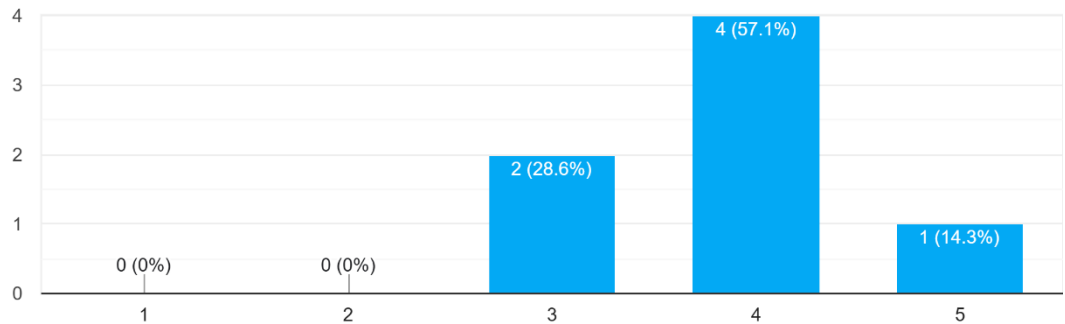
Falta de estándares operativos claros.

7 responses



Limitación en el acceso a herramientas tecnológicas avanzadas.

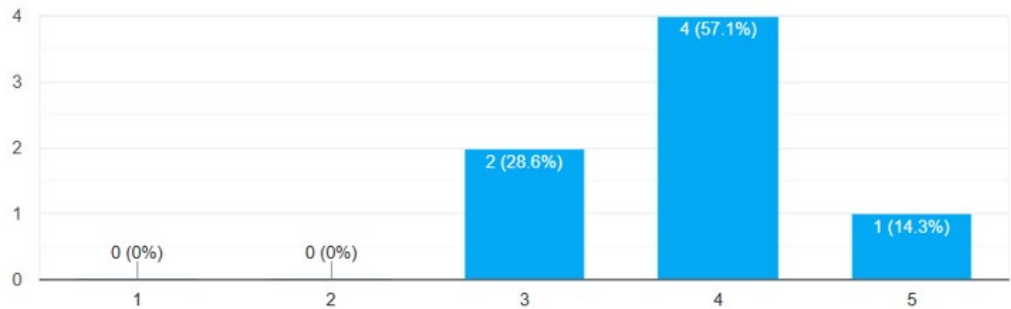
7 responses



Valore de 1 a 5 según importancia los siguientes factores que se consideran a continuación, para justificar la inversión en un sistema digital (siendo 1 sin relevancia y 5 crítica):

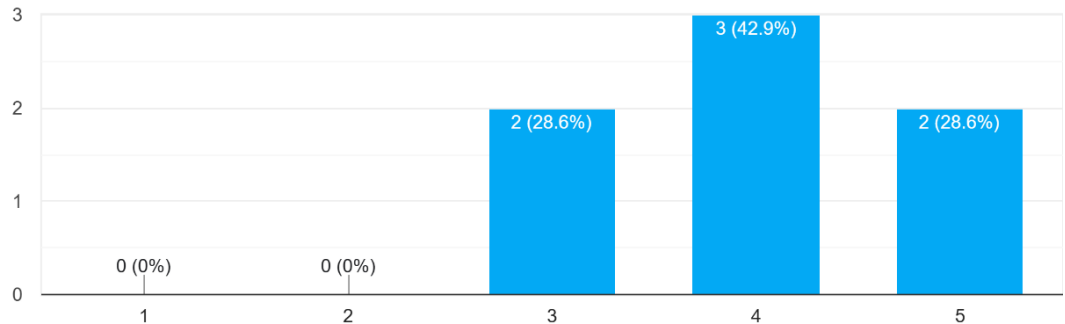
Reducción de errores humanos.

7 responses



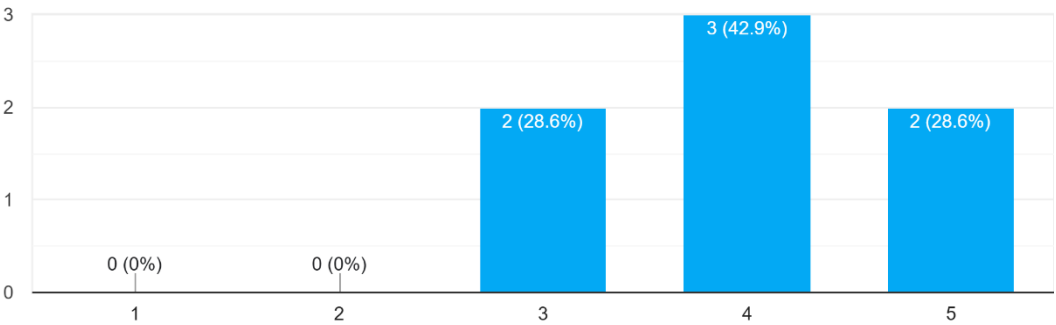
Ahorro en costes operativos y logísticos.

7 responses



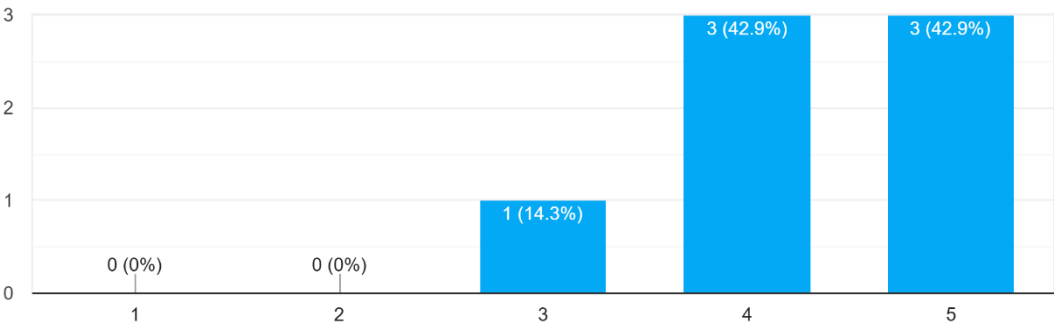
Incremento de la seguridad y la trazabilidad.

7 responses



Mejora en la coordinación con el sistema judicial.

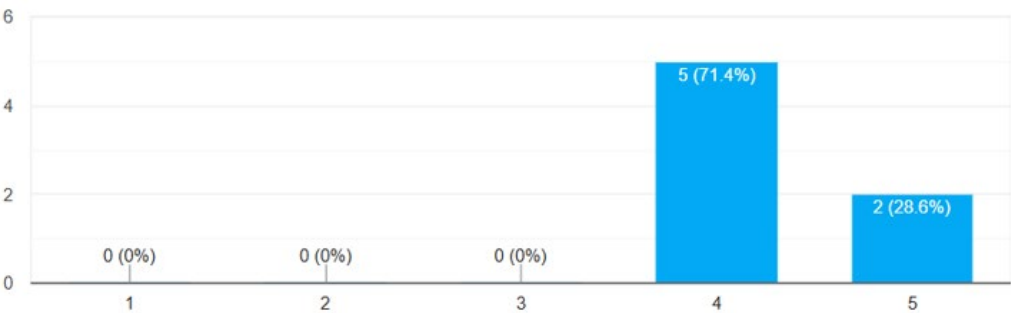
7 responses



Valore de 1 a 5 según nivel de importancia las métricas que considere para evaluar el éxito de la implementación de un sistema digital (siendo 1 sin relevancia y 5 crítica):

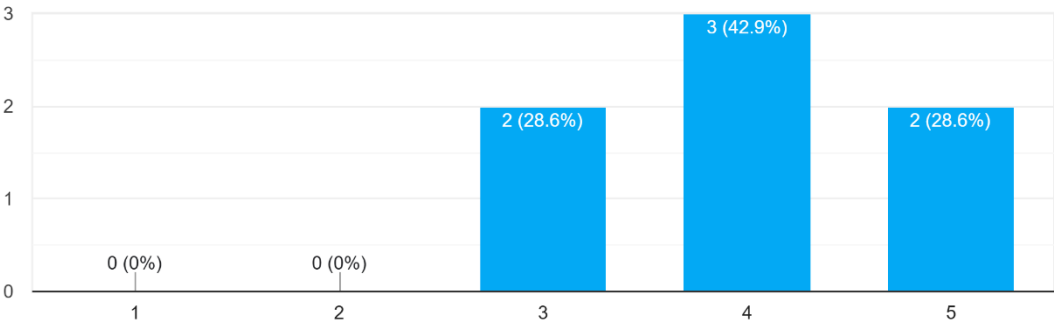
Reducción de tiempos de respuesta.

7 responses



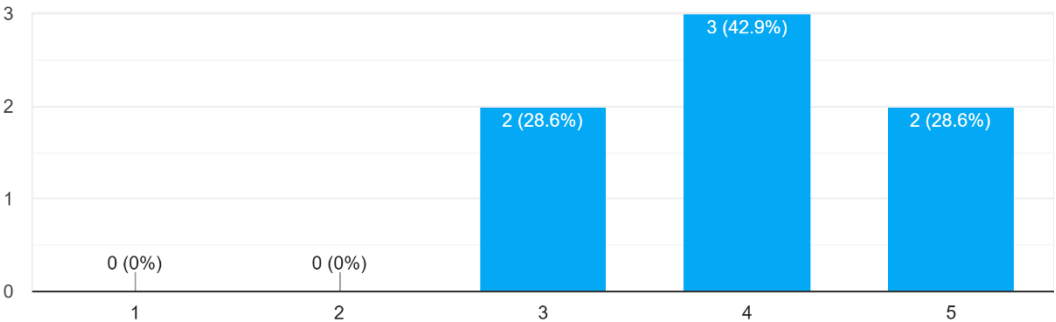
Disminución de errores en la custodia.

7 responses



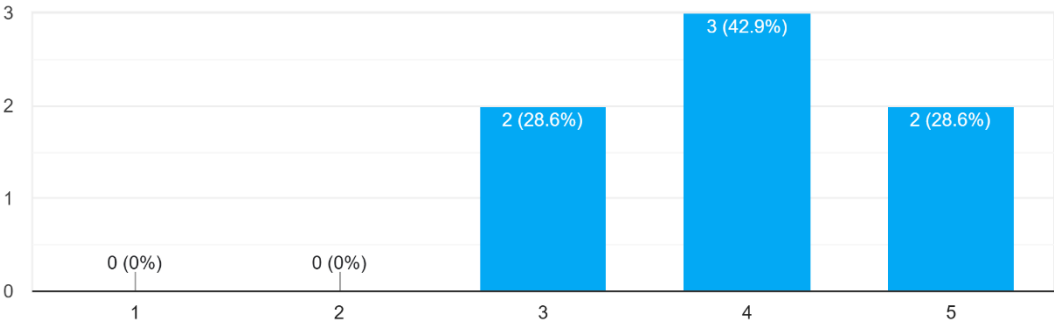
Aumento de la trazabilidad y la seguridad.

7 responses



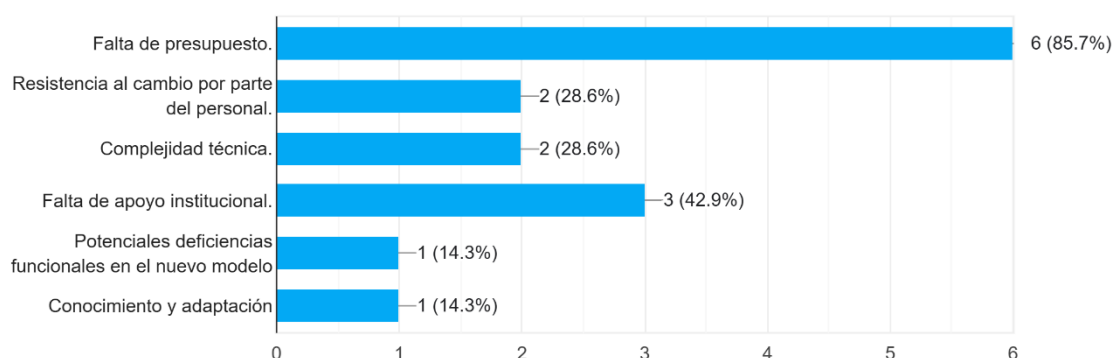
Incremento en la satisfacción de las unidades operativas y judiciales.

7 responses



¿Cuál sería el mayor obstáculo para implementar un sistema digital?

7 responses



¿Qué priorizaría más al implementar un sistema digital de gestión de evidencias?

7 responses

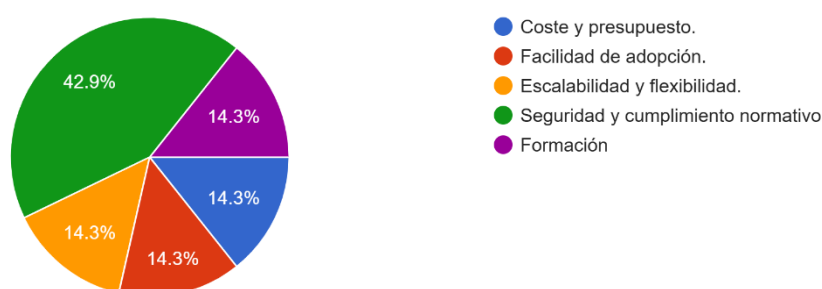


Figura 4-2 Consulta ejecutiva

Síntesis del formulario ejecutivo/directivo

El formulario enfocado en roles ejecutivos destaca como prioridades críticas:

- Incrementar la trazabilidad y seguridad de las evidencias.
- Reducir tiempos de respuesta y costes operativos asociados al manejo de evidencias digitales.
- Superar obstáculos como la resistencia al cambio y la falta de apoyo institucional, factores clave para el éxito de la implementación de un sistema digital.

Además, se reconoce que una plataforma centralizada y segura tendría un impacto significativo en la mejora de la coordinación entre unidades operativas y judiciales.

4.1.3 Consulta operativa

La consulta operativa buscó capturar las experiencias y retos cotidianos enfrentados por los profesionales que gestionan evidencias digitales. Las preguntas abordaron entre otros temas la integridad de las evidencias, la eficiencia en los procedimientos y el acceso a herramientas tecnológicas avanzadas.

A continuación, se muestran imágenes y resultados de la consulta:

Formulario de consulta Plataforma evidencias digitales (uso operativo)

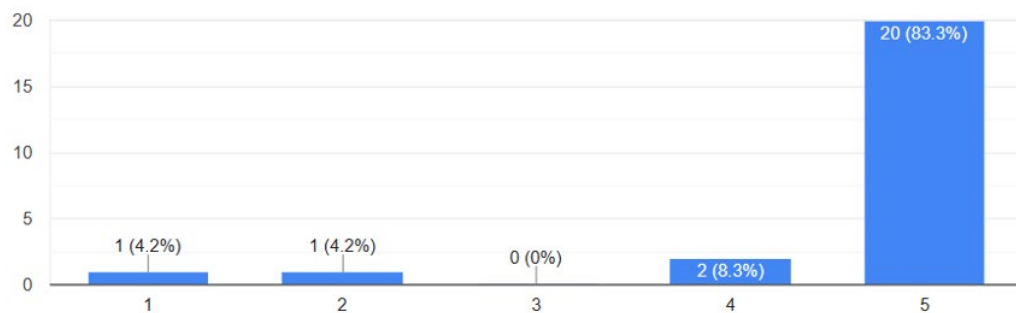
B *I* U  

El propósito de esta encuesta es realizar un estudio sobre una posible transformación digital en el manejo de evidencias digitales, enfocándose en la implementación de una plataforma para el intercambio eficiente de evidencias entre distintas unidades y la autoridad judicial. **Su colaboración es altamente valorada.**

Valore de 1 a 5 la **gravedad** de las siguientes acciones en la gestión de las evidencias digitales (siendo 1 leve y 5 muy grave):

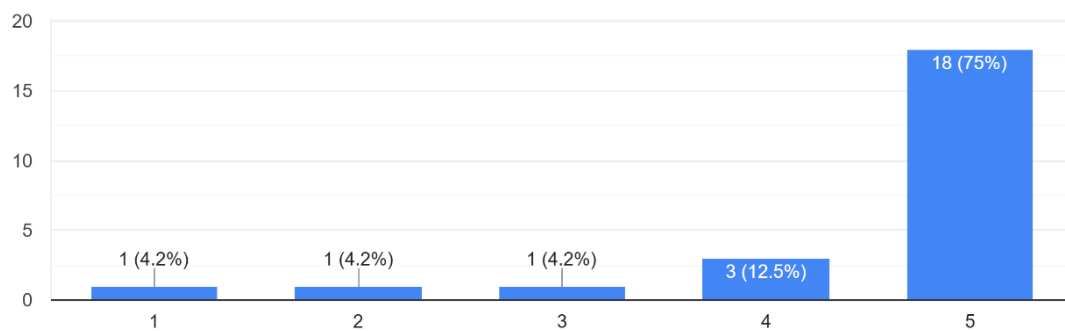
Pérdida de integridad en las evidencias durante su traslado o manipulación.

24 responses



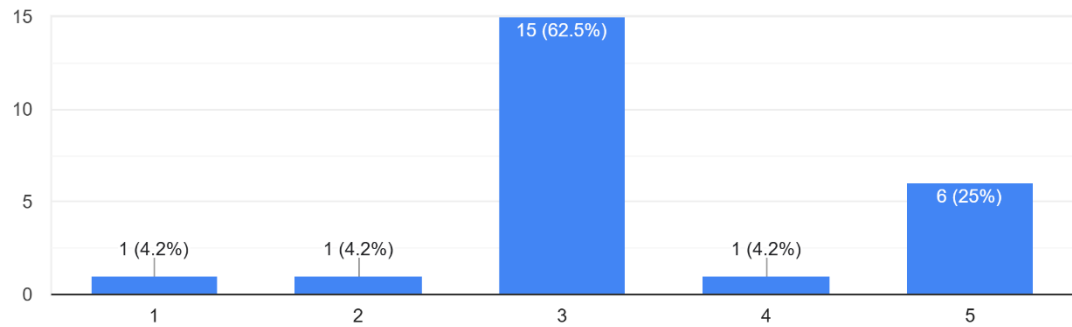
Errores humanos en la custodia y trazabilidad.

24 responses



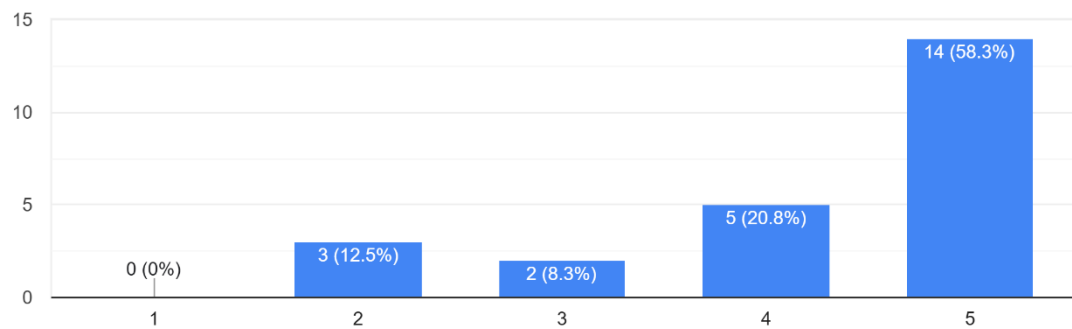
Dificultad para localizar evidencias almacenadas físicamente.

24 responses



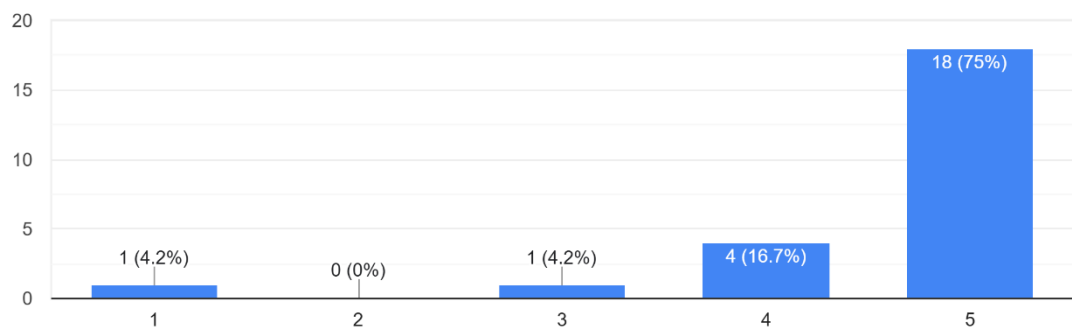
Retrasos en la remisión a instancias judiciales.

24 responses



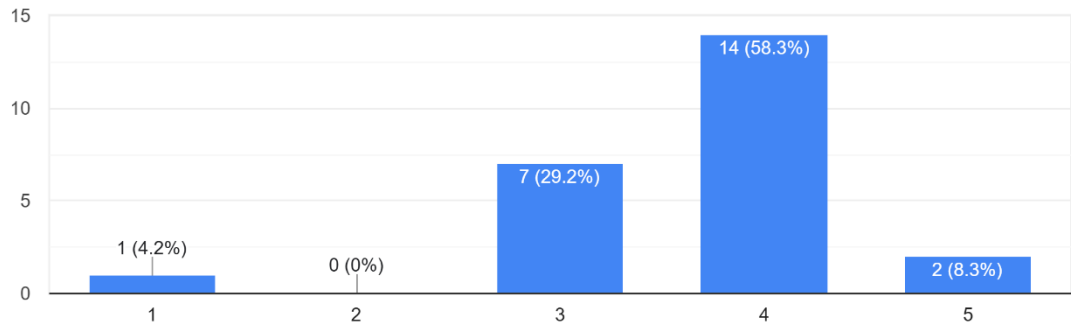
Falta de formación adecuada del personal.

24 responses



Dificultad para coordinar con otras unidades o instituciones.

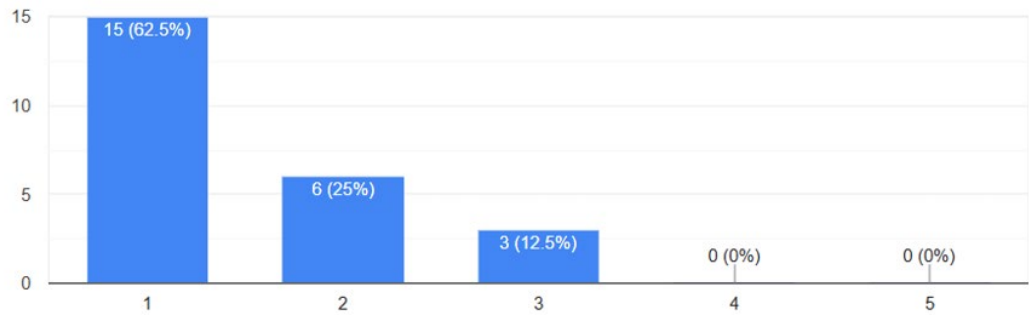
24 responses



Valore de 1 a 5 la **probabilidad de suceso** de las siguientes acciones en la gestión de las evidencias digitales (siendo 1 muy poco habitual y 5 bastante común)

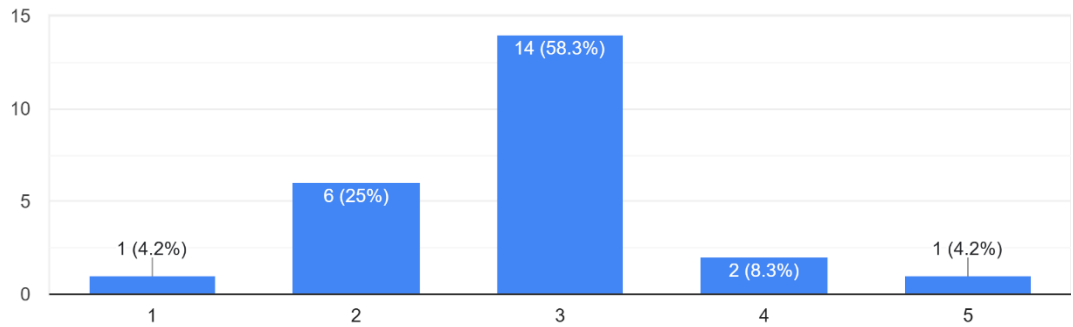
Pérdida de integridad en las evidencias durante su traslado o manipulación.

24 responses



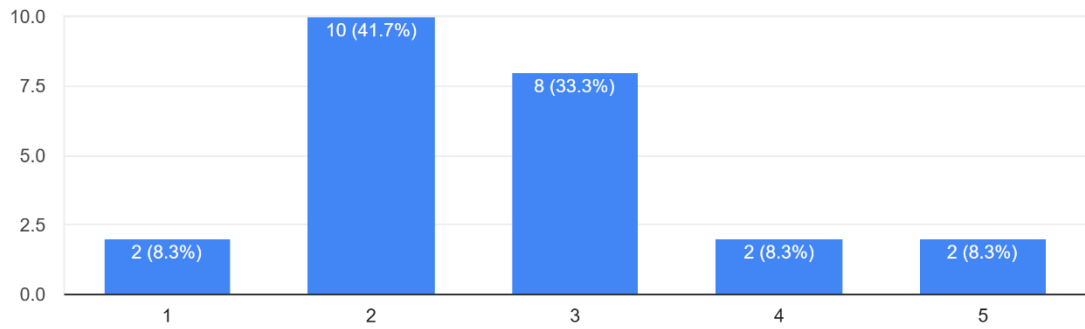
Errores humanos en la custodia y trazabilidad.

24 responses



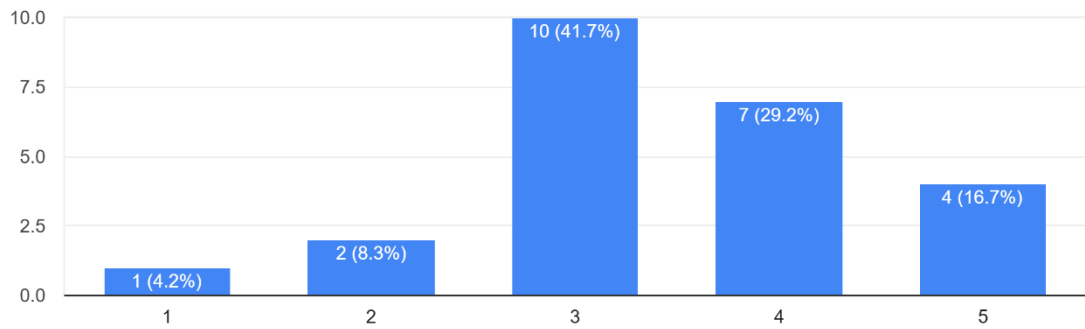
Dificultad para localizar evidencias almacenadas físicamente.

24 responses



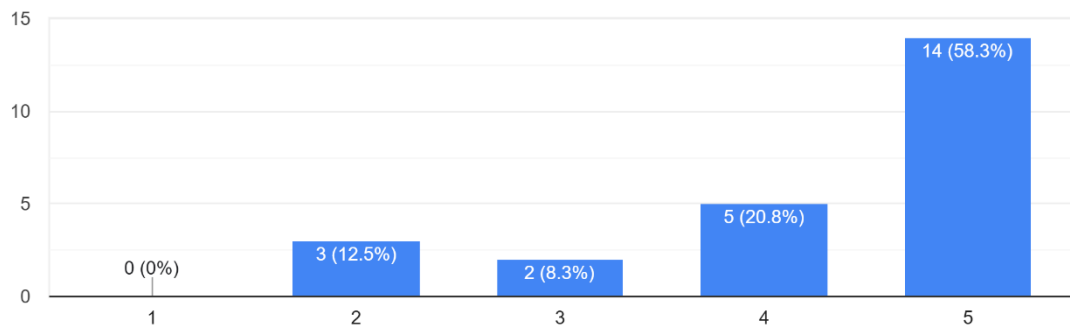
Retrasos en la remisión a instancias judiciales.

24 responses



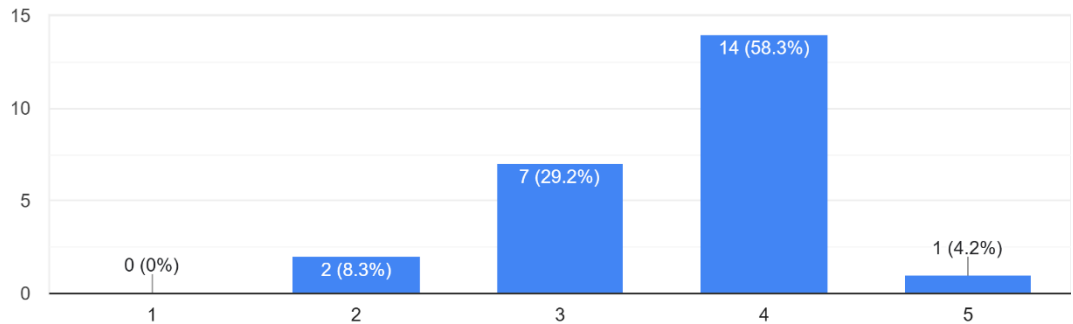
Falta de formación adecuada del personal.

24 responses



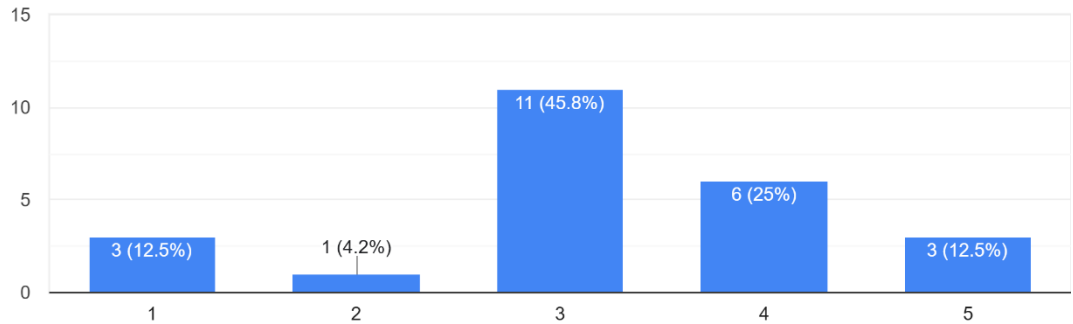
Dificultad para coordinar con otras unidades o instituciones

24 responses



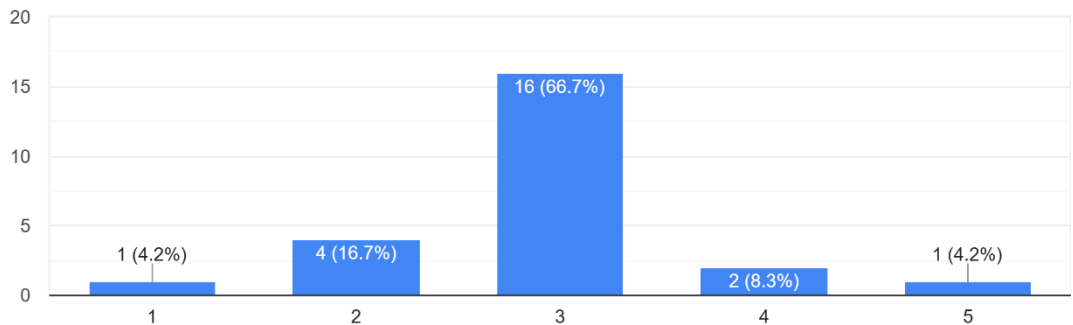
Valore de 1 a 5 el nivel de acceso que tiene a las herramientas digitales actuales para gestionar evidencias (siendo 1 muy bajo y 5 muy alto)

24 responses



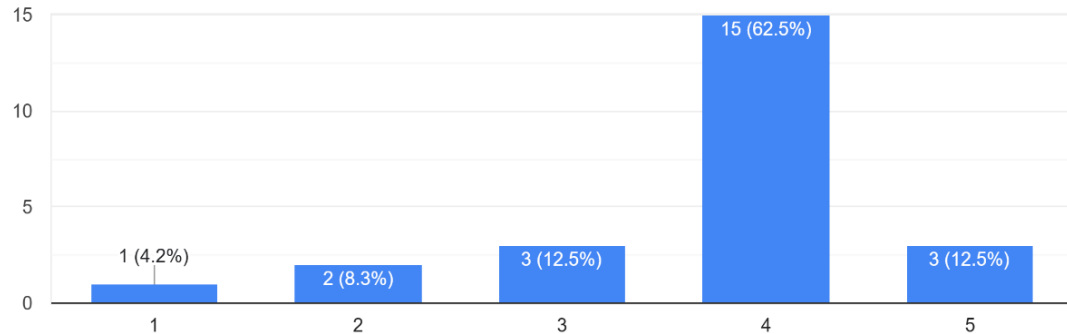
Valore de 1 a 5 la frecuencia con que se encuentra problemas de trazabilidad en las evidencias (siendo 1 nunca y 5 muy frecuentemente)

24 responses



Valore de 1 a 5 el nivel de impacto que considera que el factor humano puede tener como error en la custodia de evidencias (siendo 1 bajo y 5 crítico)

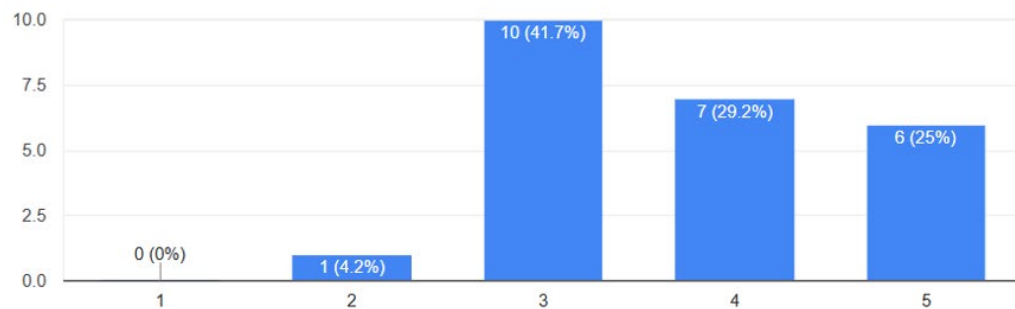
24 respuestas



Valore de 1 a 5 según **prioridad** las opciones mostradas en un sistema de Gestión Digital de Evidencias (siendo 1 bajo y 5 crítico)

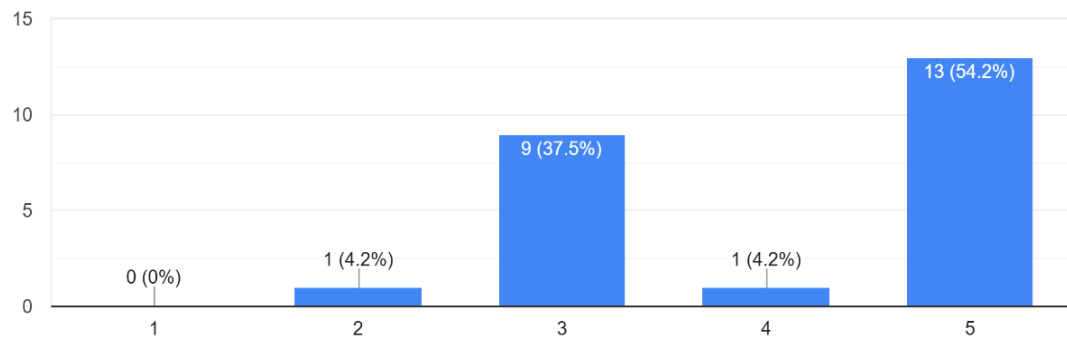
Mayor automatización del seguimiento y trazabilidad.

24 respuestas



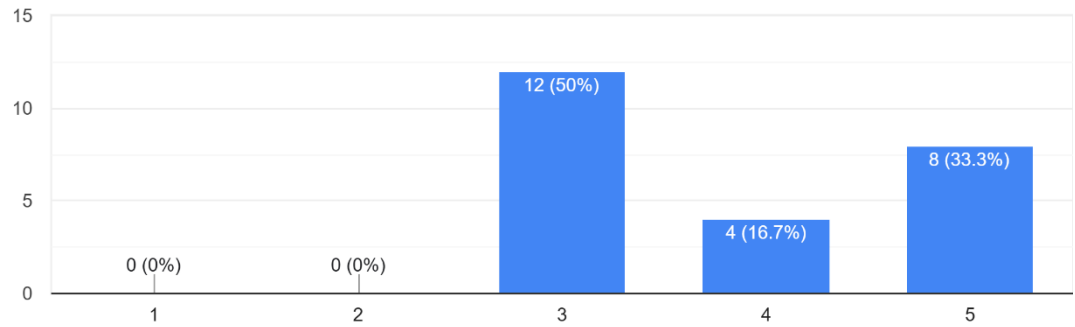
Seguridad mejorada para garantizar la integridad de las evidencias.

24 respuestas



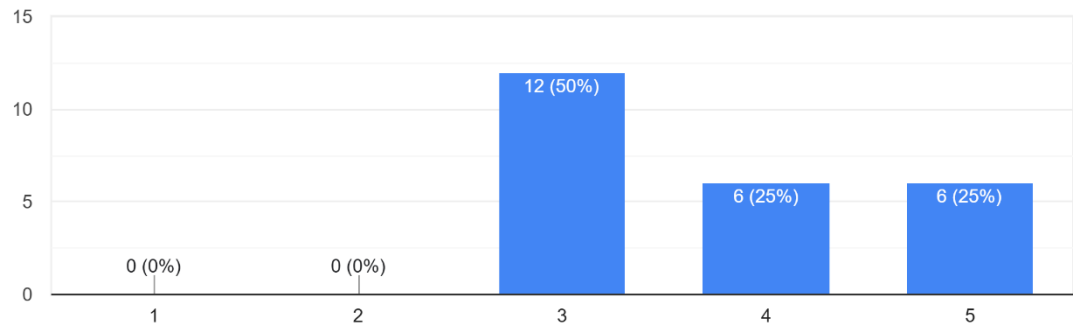
Simplificación de los procesos de remisión y consulta.

24 responses



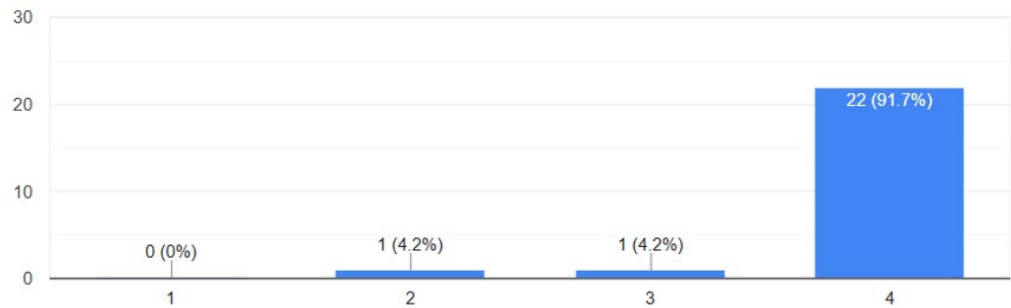
Acceso rápido y remoto a las evidencias.

24 responses



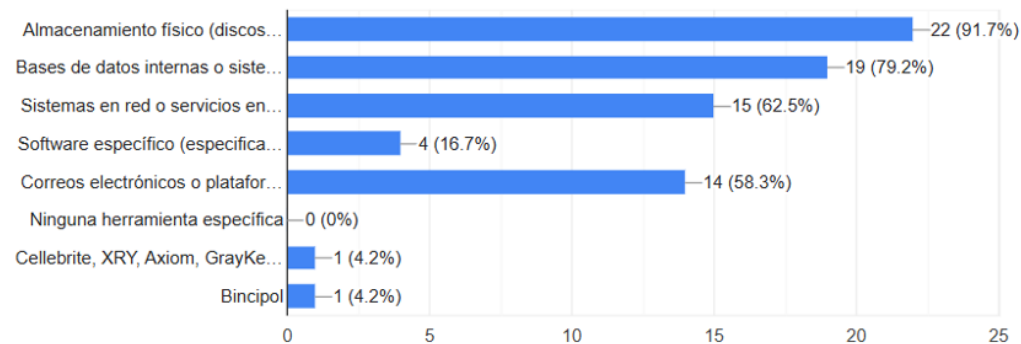
Valore de 1 a 4 cuánto **mejorarían sus labores** operativas si existiera una plataforma digital centralizada y segura para el manejo de evidencias digitales (siendo 1 no mejoraría y 4 mejoraría significativamente)

24 responses



¿Qué **herramientas** utilizas actualmente para el manejo de evidencias digitales? (opción múltiple)

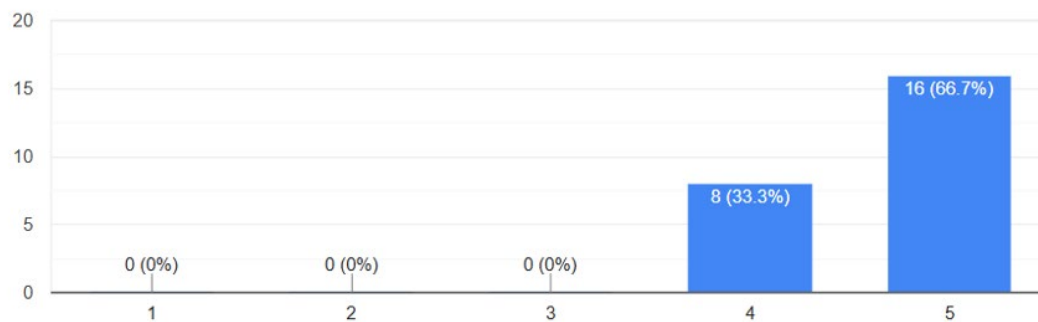
24 responses



Valore de 1 a 5 según el **grado de importancia** que considere de las siguientes características para asegurar la facilidad de uso del sistema (siendo 1 no apreciado y 5 muy importante)

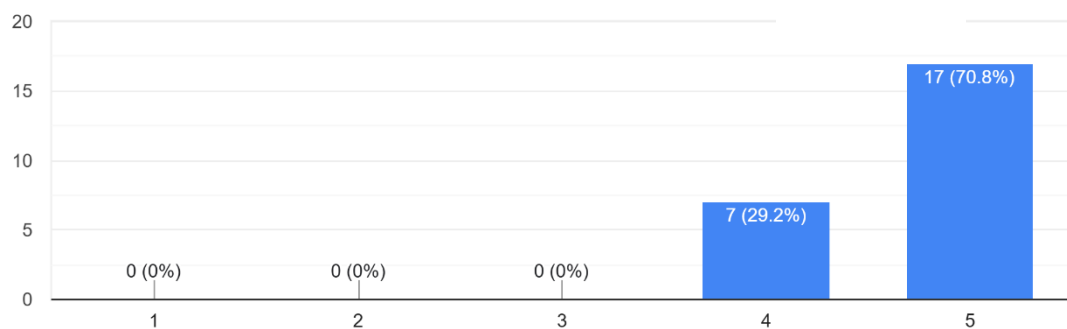
Interfaz intuitiva y amigable.

24 responses



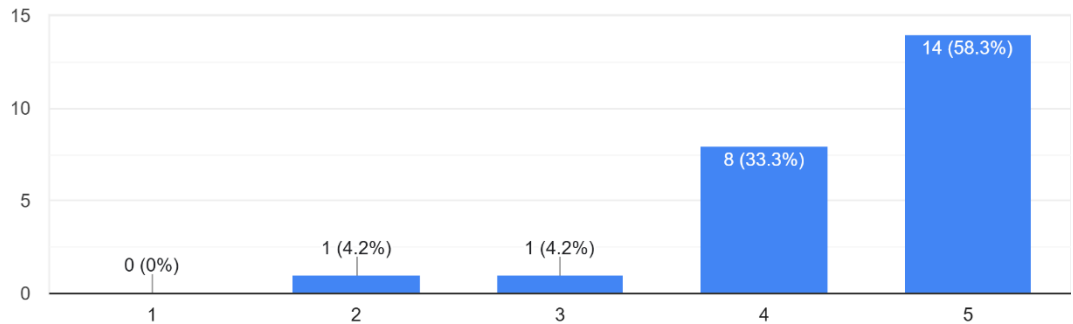
Capacitación adecuada.

24 responses



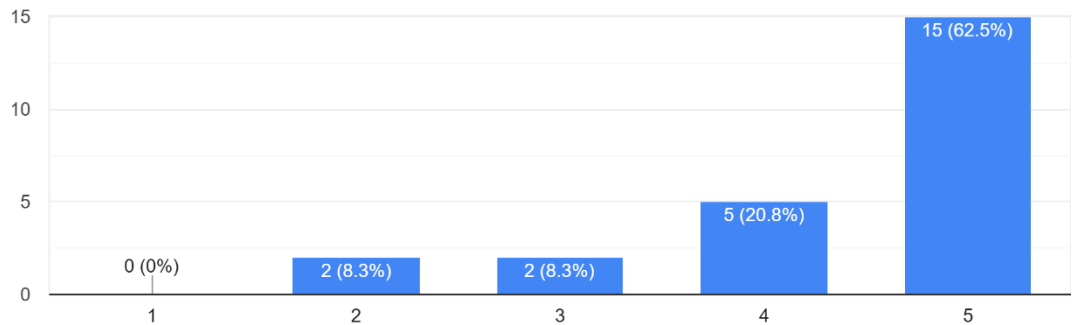
Disponibilidad de soporte técnico.

24 responses



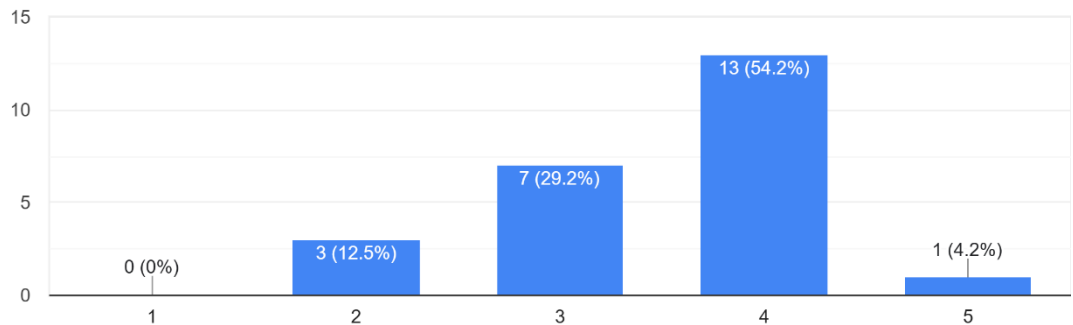
Compatibilidad con todos los dispositivos.

24 responses



Valore del 1 al 5 según considere si la seguridad lógica en las herramientas empleadas ofrecen todas las garantías deseables (siendo 1 nada seguras y 5 totalmente seguras)

24 responses



¿Recibes capacitación específica para el manejo de evidencias digitales?

24 responses

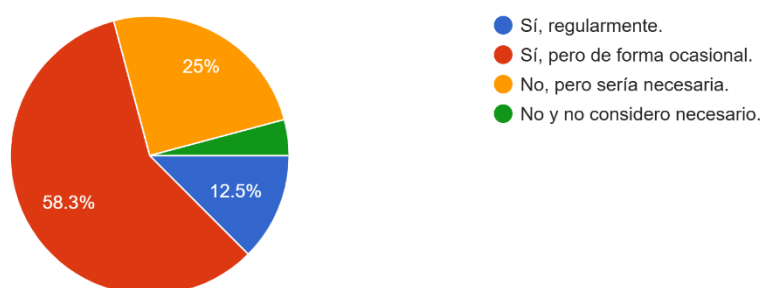


Figura 4-3 Consulta operativa

Síntesis del formulario de uso operativo

El análisis del formulario operativo resalta problemas críticos percibidos por los usuarios, como:

- La pérdida de integridad de las evidencias durante su traslado o manipulación (78.6% lo califica como muy grave).
- Retrasos en la remisión a instancias judiciales y dificultades en la localización de evidencias almacenadas físicamente.
- Un nivel bajo de acceso a herramientas digitales avanzadas, lo que limita la capacidad de los usuarios para gestionar evidencias de manera efectiva.

Los resultados indican una necesidad urgente de mayor automatización y digitalización del sistema para abordar estas deficiencias y reducir el impacto de los errores humanos. También los mismos reflejan como la implantación de una herramienta única integral de gestión de evidencias digitales facilitaría su labor elevando el nivel de eficiencia y eficacia.

4.1.4 Conclusiones

Ambas consultas subrayan la importancia de avanzar hacia la digitalización de los procedimientos. Mientras que las perspectivas estratégicas ponen énfasis en los beneficios a largo plazo, como la reducción de costes y la mejora en la trazabilidad, las operativas destacan problemas inmediatos que afectan directamente la calidad del trabajo diario. Este contraste evidencia la necesidad de una transformación digital integral, que considere tanto los objetivos organizativos como las necesidades prácticas de los usuarios finales.

5 TECNOLOGÍA, METODOLOGÍA Y ARQUITECTURA APLICADA AL DATO

En este capítulo se abordará la tecnología que se empleará para asegurar la integridad de los datos recopilados, garantizando la cadena de custodia y proporcionando una base sólida de seguridad para nuestra plataforma de intercambio de evidencias digitales. Se realizará un análisis específico e individualizado de cada una de estas tecnologías, incluyendo las modalidades de almacenamiento y la arquitectura de la plataforma, con el objetivo de ofrecer una visión amplia y detallada de su aplicación. Finalmente, en el último apartado del capítulo, se presentará la integración teórica de todas estas tecnologías en el diseño y funcionamiento de nuestro trabajo.

5.1 Integridad y autenticidad

Estos dos conceptos aplicados al dato son pilares esenciales en la gestión de evidencias digitales, especialmente en ámbitos jurídicos donde la fiabilidad de la información puede influir decisivamente en el desarrollo de una investigación o un juicio. Un fallo en cualquiera de los dos no solo pondría en riesgo la utilidad del dato, sino también la confianza en el sistema y la solidez de la cadena de custodia. Estas propiedades no solo garantizan la seguridad técnica, sino que también refuerzan la validez jurídica de las evidencias digitales.

La **integridad** se refiere a la capacidad de garantizar que los datos no han sido alterados desde su creación o recopilación, asegurando que cualquier cambio, intencionado o accidental, sea detectable. Técnicamente, esto se logra mediante el uso de funciones hash criptográficas, que generan un identificador único del contenido original.

La **autenticidad** implica confirmar la procedencia y legitimidad del dato, verificando que este proviene de una fuente confiable y que no ha sido manipulado en el tránsito, lo cual se puede garantizar mediante firmas digitales o certificados emitidos por una autoridad confiable.

En los siguientes subapartados vamos a describir unos sistemas que nos permiten garantizar los términos que se han descrito.

5.1.1 Sistema de gestión de certificados PKI

Un sistema de gestión de certificados PKI (*Public Key Infrastructure*) es una infraestructura tecnológica que permite la emisión, gestión, revocación y uso de certificados digitales. Los certificados digitales son documentos electrónicos que asocian una clave pública con una identidad, como una persona, organización o dispositivo, y están firmados por una autoridad de certificación (CA, por sus siglas en inglés).

Esta tecnología permite gestionar de forma segura certificados digitales y claves criptográficas, asegurando las propiedades esenciales de autenticación, confidencialidad, integridad y no repudio en entornos digitales.

Normalmente se utiliza para proteger comunicaciones digitales, como correos electrónicos, conexiones web seguras (HTTPS) o redes privadas virtuales (VPN), además de habilitar la firma digital de documentos con validez legal. También se utiliza en la gestión de identidades y accesos, en la seguridad de dispositivos IoT y en la transmisión segura de datos.

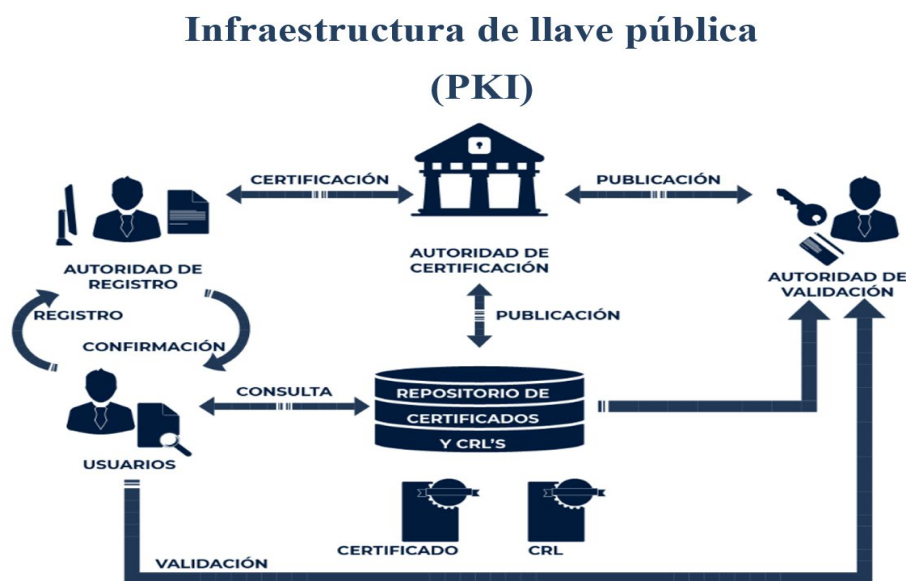


Figura 5-1 Infraestructura de llave pública PKI

La imagen representa la arquitectura básica de una Infraestructura de Llave Pública (PKI), mostrando cómo se interconectan sus principales componentes para gestionar certificados digitales.¹⁶

1. **Autoridad de Certificación (CA):** es el núcleo del sistema, responsable de emitir y publicar certificados digitales. Estos se almacenan en un **repositorio de certificados y listas de revocación (CRLs)**, que los usuarios y otros componentes pueden consultar.
2. **Autoridad de Registro (RA):** se encarga de verificar la identidad de los usuarios que solicitan certificados antes de enviar la solicitud a la CA. Una vez confirmada, la CA emite el certificado.
3. **Usuarios:** consultan el repositorio para validar certificados o acceder a las CRLs en caso de que un certificado haya sido revocado.
4. **Autoridad de Validación:** se encarga de confirmar la validez de los certificados en tiempo real, utilizando listas CRL como alternativa el protocolo de Estado de Certificados Online (OCSP) que proporciona un método en tiempo real para verificar el estado de un certificado.

¹⁶ <https://www.cegasecurity.com/landings/solicitud-de-información-pki/>

El flujo general incluye la emisión, validación, publicación y uso de certificados digitales, garantizando la autenticidad, integridad y seguridad de las comunicaciones digitales.

5.1.2 Tecnología Blockchain, Smart Contract y NFTs

La **tecnología blockchain** [25] o cadena de bloques es un sistema descentralizado de registros digitales que permite el almacenamiento seguro, transparente e inalterable de datos. Surgió con la publicación del artículo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" en 2009, por Satoshi Nakamoto [26], quien propuso su aplicación inicial como base para la criptomoneda **Bitcoin**.

El blockchain elimina la necesidad de intermediarios al validar transacciones mediante consenso distribuido entre los nodos de la red. Cada transacción queda registrada en bloques que, una vez validados, se añaden a una cadena criptográficamente segura. Su gran contribución es que elimina la necesidad de un tercero fiable para la validación de las operaciones.

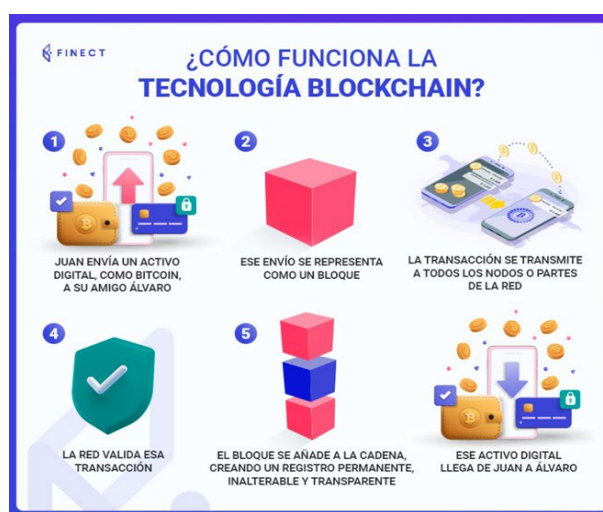


Figura 5-2 Funcionamiento Blockchain

En la figura 5-2, se describe de manera visual cómo funciona la tecnología blockchain en seis sencillos pasos: ¹⁷

1. **Envío** de un activo digital.
2. **Representación** como bloque.
3. **Distribución** en la red a todos los nodos.
4. **Validación** de la transacción por la red de nodos mediante algoritmos de consenso.
5. **Incorporación a la cadena** del bloque validado creando un registro **permanente, inalterable y transparente**.
6. **Entrega** del activo digital a su destinatario, completando la transacción.

Un **smart contract (o contrato inteligente)** es un programa o protocolo informático que se ejecuta automáticamente en una blockchain al cumplirse ciertas condiciones previamente definidas. Destacaremos sus características principales debido a su relevancia en este trabajo:

- Automatización: acciones definidas cuando se cumplen las condiciones establecidas.
- Transparencia: la lógica del contrato es pública y verificable por sus términos.
- Inmutabilidad: una vez implementado no se pueden alterar, lo que garantiza su integridad.
- Sin intermediarios: garantiza la ejecución del acuerdo, reduciendo costos y tiempos.

¹⁷ <https://statics.teams.cdn.office.net/evergreen-assets/safelinks/1/atp-safelinks.html>

Funcionamiento



Figura 5-3 Funcionamiento Smart contract

A continuación, se describe el flujo de trabajo según la imagen anterior:

1. Identificar el acuerdo:

Las partes involucradas identifican la oportunidad de colaboración y los resultados deseados. Esto implica definir los términos y condiciones que regirán el contrato.

2. Establecer las condiciones:

Se determinan las condiciones específicas bajo las cuales el contrato inteligente se ejecutará automáticamente. Estas condiciones deben ser claras y acordadas por todas las partes.

3. Codificar la lógica empresarial:

La lógica del contrato (las reglas y condiciones definidas) se traducen en un programa informático. Este programa es desarrollado como un código que será ejecutado en una blockchain.

4. Tecnología de encriptación y blockchain:

La tecnología de encriptación asegura la transferencia segura de datos entre las partes, mientras que la blockchain registra el contrato y sus transacciones, proporcionando un entorno seguro, descentralizado y transparente.

5. Ejecución y procesamiento:

Una vez que las condiciones del contrato se cumplen, el código se ejecuta automáticamente, y los resultados (como transferencias de activos o cambios de estado) se graban en la blockchain.

6. Actualización de la red:

Todos los nodos de la red blockchain se actualizan para reflejar la ejecución y los resultados del contrato, asegurando la consistencia y trazabilidad de los registros.

Los **NFTs o Token no fungibles**, es una manera sofisticada de expresar que algo es absolutamente único y no puede ser reemplazado por otro elemento. Ampliando esta definición, se conocen como activos digitales únicos que representan la propiedad o autenticidad de un objeto específico, ya sea digital o físico. A diferencia de las criptomonedas como Bitcoin o Ethereum, que son fungibles e intercambiables entre sí, cada NFT posee características distintivas que lo hacen irrepetible. Esta singularidad permite que los NFTs se utilicen para certificar la propiedad de obras de arte digitales, coleccionables, música, videos y otros contenidos digitales.

La mayoría de las personas relaciona el término NFT con tarjetas coleccionables, obras de arte digitales u objetos y personajes de videojuegos. Es muy importante comprender que los NFT no son los activos en sí mismos, sino representaciones de dichos activos (cadenas de datos codificados) registradas en la **blockchain**.

Funcionamiento

La mayoría de los NFTs operan sobre la tecnología blockchain, principalmente en la red Ethereum, aunque también en otras blockchains que soportan contratos inteligentes (*smart contracts*). El proceso general de creación y transacción de un NFT se puede resumir en los siguientes pasos:

1. **Creación**

El creador genera un NFT mediante un contrato inteligente, que asigna un identificador único al activo y lo registra en la blockchain. Este proceso incluye la incorporación de metadatos que describen las propiedades del NFT, como nombre, descripción y enlace al propio activo.

2. **Registro**

Una vez creado, el NFT se almacena en la blockchain, garantizando su inmutabilidad y propiedad verificable. La descentralización de la blockchain asegura que el registro no pueda ser alterado ni eliminado, proporcionando confianza en la autenticidad del activo.

3. **Compra/Venta**

Los NFTs pueden comprarse y venderse en mercados digitales especializados. Las transacciones se registran en la blockchain, transfiriendo la propiedad del NFT al nuevo propietario y manteniendo un historial transparente de todas las operaciones realizadas.

4. **Acceso**

Aunque el NFT certifica la propiedad de un activo digital, el contenido generalmente se almacena fuera de la blockchain, en sistemas de almacenamiento descentralizados o servidores tradicionales. El NFT contiene enlaces o referencias a este contenido, permitiendo su visualización o descarga según los términos establecidos por el creador.

5.2 Modalidades de almacenamiento

En este apartado vamos a describir las diferentes tecnologías que se pueden llegar a contemplar para el manejo eficiente y seguro de evidencias digitales y que requieren de una infraestructura de almacenamiento que se adapte a las necesidades específicas de la plataforma, considerando factores como la sensibilidad de los datos, la escalabilidad requerida, el cumplimiento normativo y los costos operativos.

A continuación, se describen las principales modalidades de almacenamiento: **nube privada**, **nube pública**, **nube híbrida** y **on-premise**, destacando sus características, ventajas, desventajas y su relevancia para la plataforma de evidencias digitales.

Nube Privada

La infraestructura es exclusiva para la plataforma, ya sea gestionada internamente o por un proveedor externo, pero aislada de otros usuarios.

Características

- Permite cumplir estrictamente con normativas legales sobre custodia y protección de datos.
- Control absoluto sobre la infraestructura y el acceso a las evidencias.
- Alta seguridad, ya que no se comparte con otras organizaciones.

Nube Pública

Los servicios se alojan en servidores gestionados por proveedores externos (como AWS, Azure, o Google Cloud), compartiendo recursos con otros usuarios.

Características

- Escalabilidad inmediata para almacenar grandes volúmenes de evidencias digitales.
- Costos operativos bajos gracias al modelo de pago por uso.

- Beneficios de redundancia y recuperación ante desastres proporcionados por los proveedores.

Nube Híbrida

Integra la nube privada para datos sensibles con la nube pública para almacenamiento no crítico.

Características

- Combina la seguridad de la nube privada para evidencias críticas con la flexibilidad de la nube pública para datos secundarios.
- Permite escalar rápidamente en picos de uso, como durante investigaciones con grandes volúmenes de evidencia digital.

On-Premise

Toda la infraestructura se aloja y gestiona dentro de las instalaciones físicas de la organización.

Características

- Control total sobre la custodia de las evidencias y la infraestructura.
- No depende de terceros para la gestión o almacenamiento de los datos.
- Permite operar sin conectividad a internet, crucial para entornos de alta seguridad.

Modalidad	Ventajas	Desventajas
Nube Privada	- Alta seguridad y cumplimiento normativo. - Control total de las evidencias y trazabilidad. - Personalización completa.	- Costos iniciales elevados. - Gestión y mantenimiento especializado. - Escalabilidad limitada.
Nube Pública	- Escalabilidad rápida. - Costos bajos por uso. - Infraestructura y respaldo gestionados por el proveedor.	- Riesgo de brechas de seguridad. - Dependencia de proveedores externos. - Menor control directo.
Nube Híbrida	- Flexibilidad entre control y escalabilidad. - Optimización de costos. - Integración de sistemas redundantes.	- Complejidad de integración. - Costos de herramientas híbridas. - Requiere personal técnico especializado.
On-Premise	- Máximo control sobre la custodia de evidencias. - Sin dependencia de terceros. - Operación offline posible.	- Costos iniciales y operativos altos. - Menor escalabilidad. - Tiempo de implementación más largo.

Tabla 5-1 – Modalidades de almacenamiento

Existen diversas empresas cuyos productos o servicios están diseñados para depender directamente del almacenamiento en la nube. Estas soluciones suelen clasificarse en tres categorías principales:

1. **IaaS (Infrastructure-as-a-Service):** ofrecen una infraestructura básica, con servidores de alta capacidad, utilizados como base para otros servicios (AWS, Rackspace y Flexiscale).
2. **PaaS (Platform-as-a-Service):** proveen sistemas operativos, lenguajes de programación y bases de datos que facilitan el desarrollo y la administración de aplicaciones (Microsoft Azure y Salesforce).
3. **SaaS (Software-as-a-Service):** ofrecen aplicaciones accesibles vía internet, eliminando la necesidad de adquirir licencias (Hubspot y Pipedrive).

Un desafío adicional significativo es el conjunto de políticas de seguridad implementadas por las Fuerzas y Cuerpos de Seguridad (FCS) en su infraestructura tecnológica. Estas políticas, en ocasiones, dificultan la adopción de soluciones tecnológicas de vanguardia, ya que no siempre se ajustan a los estándares de seguridad establecidos. Como resultado, a menudo se opta por soluciones más

conservadoras o intermedias que equilibran la innovación tecnológica con las normativas de seguridad vigentes.

5.3 Arquitectura

En este apartado se detallará la arquitectura general que soportará la plataforma de intercambio de evidencias digitales. Esta arquitectura debe garantizar la seguridad, la escalabilidad y la integridad de los datos, integrando las tecnologías y métodos mencionados en los apartados anteriores.

5.3.1 Descripción general

La arquitectura general de la plataforma de intercambio de evidencias digitales adopta un enfoque híbrido, combinando entornos de nube híbrida y on-premise para maximizar la seguridad, escalabilidad, y flexibilidad. Este diseño permite la coexistencia de sistemas locales (on-premise) para garantizar el control total sobre datos sensibles y sistemas basados en la nube para ofrecer escalabilidad y accesibilidad.

A continuación, se detalla cada componente y capa de la arquitectura, incluyendo la interacción entre los entornos híbridos:

- **Capa de acceso/presentación:** interfaz que conecta a los usuarios con el sistema. Este componente se despliega tanto en entornos locales como en la nube, permitiendo una interacción fluida y segura desde cualquier lugar. Se puede acceder a interfaces instaladas en servidores on-premise, mientras que los usuarios remotos tienen acceso a un portal web seguro en la nube. Esta capa ofrece funcionalidades como el registro de evidencias digitales, la visualización de la trazabilidad de cada evidencia y la capacidad de realizar transferencias de propiedad con total seguridad. Además, se integra con sistemas de autenticación avanzada, como la infraestructura de clave pública (PKI), para garantizar la identidad de los usuarios.
- **Capa de lógica empresarial:** gestiona los procesos críticos mediante contratos inteligentes. Estas herramientas permiten automatizar la gestión de permisos, asegurar la trazabilidad de las evidencias y realizar transferencias de propiedad de manera verificable e inmutable. La lógica empresarial está diseñada para operar de forma híbrida: procesos sensibles y críticos, como la validación de identidades, se gestionan en sistemas locales, mientras que las tareas que requieren mayor escalabilidad, como la sincronización de datos entre múltiples ubicaciones, se manejan en la nube. Un middleware asegura la orquestación fluida de las operaciones entre los entornos locales y remotos, garantizando que los procesos sean coherentes y eficientes.
- **Capa de seguridad:** incorporación de un sistema de gestión de certificados PKI para validar la identidad de los actores y garantizar la autenticidad de las transacciones. Valida las identidades y protege las comunicaciones mediante cifrado de extremo a extremo. Esta capa se despliega en ambos entornos: en los sistemas locales para proteger datos altamente sensibles, y en la nube para supervisar amenazas de manera proactiva y proteger los accesos remotos. Además, se emplea autenticación multifactor y registros detallados de auditoría para reforzar la protección del sistema.
- **Capa de almacenamiento:** combina blockchain y almacenamiento descentralizado. Los datos más sensibles se almacenan en servidores locales bajo control físico directo, mientras que las evidencias menos críticas o de acceso frecuente se alojan en la nube. La blockchain se utiliza para registrar los hashes de las evidencias, asegurando su integridad y trazabilidad de forma inmutable, mientras que soluciones como IPFS o Piñata garantizan la distribución y redundancia de los archivos digitales en entornos

descentralizados. Este enfoque asegura que la información esté disponible globalmente, manteniendo la seguridad y el control local en casos sensibles.

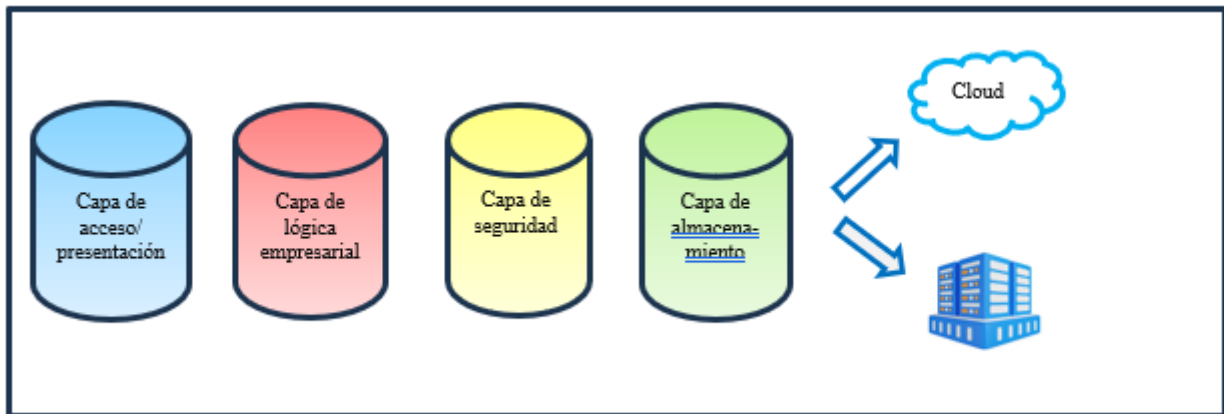


Figura 5-4 Arquitectura en capas de plataforma

Interacciones y Flujo de Trabajo

1. Registro de Evidencias:

- Un usuario local registra la evidencia en la capa de presentación on-premise.
- Los datos sensibles se almacenan localmente, mientras que los metadatos y hashes se registran en la blockchain.
- Si es necesario, los archivos son replicados en IPFS para accesibilidad.

2. Consulta y Transferencia:

- Los usuarios autorizados acceden a la plataforma mediante la interfaz local o en la nube.
- Las transacciones son validadas por el sistema PKI y los contratos inteligentes.

3. Sincronización Híbrida:

- Los sistemas on-premise sincronizan los eventos relevantes con la nube para garantizar que la plataforma opere como un entorno unificado.

5.3.2 Componentes técnicos

1. Blockchain:

El uso de la tecnología blockchain constituye el núcleo de la plataforma, proporcionando inmutabilidad y trazabilidad para las evidencias digitales. Este componente asegura que cada registro, transferencia o modificación en las evidencias sea almacenado de manera permanente y verificable, eliminando el riesgo de alteración malintencionada. Dependiendo de los requisitos de privacidad y escalabilidad del sistema, se contempla el uso de **Ethereum o Hyperledger**, aunque en nuestro caso hemos optado por la primera opción.

- **Ethereum:** es ideal para casos donde la transparencia es prioritaria, ya que opera como una red pública y descentralizada. Su capacidad para ejecutar contratos inteligentes lo hace altamente funcional para automatizar procesos.

2. Sistemas descentralizados de almacenamiento:

La gestión de los archivos digitales asociados a las evidencias utiliza un modelo descentralizado, que combina IPFS y Piñata para garantizar disponibilidad, redundancia y seguridad:

- **IPFS:** sistema de almacenamiento distribuido en el que los archivos digitales no se alojan en un único servidor, sino en nodos interconectados. Esto mejora la resiliencia y refuerza la protección contra pérdida o alteración de datos.
- **Piñata:** como un servicio complementario que facilita la gestión y el acceso a los datos almacenados en IPFS. Además, establece una conexión con la blockchain, lo que permite registrar hashes de los archivos en el blockchain para garantizar su integridad y vinculación con las evidencias.

3. Módulo PKI (Public Key Infrastructure):

La infraestructura de clave pública es un componente esencial para garantizar la autenticidad y la seguridad de las transacciones dentro de la plataforma. Este módulo se encarga de la gestión de claves y certificados digitales, lo que permite:

- **Validación de identidad:** de cada usuario, dispositivo o sistema involucrado en la plataforma que sea auténtico y esté autorizado.
- **Cifrado y firmas digitales:** protege la confidencialidad de las transacciones y garantiza la integridad de los datos mediante técnicas criptográficas avanzadas.

4. Contratos inteligentes:

Como ya se ha mencionado anteriormente, los contratos inteligentes son programas autoejecutables que automatizan tareas dentro de la plataforma, mejorando su eficiencia y confiabilidad. Entre las funciones clave que van a realizar se incluyen:

- **Gestión de permisos de acceso:** controlan y regulan quién tiene derecho a acceder o analizar una evidencia, asegurándose de que solo usuarios autorizados puedan interactuar con los datos.
- **Transferencia de custodia:** automatizan el cambio de propiedad o custodia de las evidencias, registrando cada transferencia en la blockchain para mantener una trazabilidad inmutable.

5. Plataforma de usuario:

La interacción con la plataforma se facilita a través de una interfaz web o móvil, diseñada para ser segura, intuitiva y accesible. Este componente sirve como el punto de entrada para los usuarios, ofreciendo las siguientes funcionalidades:

- Registro y consulta de evidencias digitales.
- Visualización de la trazabilidad completa de las evidencias.
- Ejecución de transferencias de custodia con validación de identidad.
- Integración con sistemas de autenticación robusta, como el módulo PKI.

5.4 Aplicación tecnológica a nuestra plataforma

5.4.1 Relación Blockchain-NFT-Evidencias Digitales

En primer lugar, vamos a ver como relacionamos estos 3 entes. La combinación de blockchain, NFTs y evidencias digitales ofrece un sistema técnico y seguro para gestionar evidencias. Estas tecnologías garantizan trazabilidad, integridad y control, aspectos fundamentales en un entorno judicial o forense.

Con esta combinación, cada **evidencia digital** puede representarse como un **NFT** único, garantizando su identificación, integridad y trazabilidad.

La **blockchain** registra todas las interacciones de manera inmutable, mientras que los **smart contracts** automatizan procesos como la transferencia de permisos y el control de acceso, asegurando

que solo usuarios autorizados puedan consultar o modificar las evidencias, mejorando la eficiencia y reduciendo el riesgo de errores.

Además, esta tecnología facilita la disponibilidad de los archivos mediante sistemas de almacenamiento descentralizado, como **IPFS**, y asegura que no se alteren gracias al uso de hashes criptográficos.

De una manera más esquemática se resumirían en las siguientes acciones:

Gestión de permisos automatizada

Los smart contracts permiten definir y ejecutar automáticamente reglas de acceso o transferencia de las evidencias representadas por NFTs.

- **Funcionamiento:** los contratos contienen las condiciones predefinidas (por ejemplo, "solo fiscales pueden acceder a esta evidencia"). Al cumplirse estas condiciones, el contrato concede el permiso o transfiere el NFT.

Control de acceso exclusivo

El sistema garantiza que solo usuarios autorizados puedan interactuar con el NFT asociado a una evidencia.

- **Funcionamiento:** los usuarios deben autenticarse mediante certificados digitales y claves privadas antes de acceder al NFT o modificar permisos.

Registro automático de interacciones

Cada interacción con una evidencia (consulta, transferencia, actualización) se registra automáticamente en la blockchain.

- **Funcionamiento:** El contrato genera un registro inmutable en la blockchain, que incluye detalles como la acción realizada, el usuario que la ejecutó y el momento en que ocurrió.

Relación entre Blockchain, NFTs y Evidencias

- **Trazabilidad:** La blockchain asegura que todas las acciones relacionadas con una evidencia sean registradas de forma permanente e inalterable.
- **Identificación única:** Los NFTs vinculan cada evidencia a un identificador único, que incluye metadatos como su hash criptográfico, fecha de creación y número de caso.
- **Integridad:** Los hashes almacenados en los NFTs permiten verificar que el archivo digital no ha sido modificado.
- **Accesibilidad controlada:** Los NFTs contienen enlaces a sistemas de almacenamiento descentralizado, como IPFS, que garantizan la disponibilidad del archivo y detectan alteraciones mediante CIDs.
- **Automatización:** Los procesos de acceso y transferencia se gestionan de forma automática, reduciendo costos y tiempos.
- **Trazabilidad y control:** Todas las interacciones se registran en la blockchain, eliminando riesgos de pérdida o manipulación.
- **Cumplimiento legal:** La estructura técnica de blockchain y NFTs asegura que las evidencias cumplan con los requisitos legales de integridad y custodia.

5.4.2 Ejemplo práctico

En este epígrafe vamos a desarrollar un ejemplo, en cinco pasos, sobre el uso de blockchain en el registro de evidencias forenses digitales y como su aplicación real ya es vinculante y operativo en países como China.¹⁸

1. Registro inicial de la Evidencia

Una unidad policial captura una evidencia digital relevante, como un video de vigilancia relacionado con un caso de robo. Este video se carga en la plataforma a través de la capa de acceso/presentación. Al registrarse, la plataforma genera un hash criptográfico (utilizando SHA-256) que actúa como un identificador único del contenido. Por ejemplo, un hash podría ser: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855.

Este hash se almacena inmediatamente en la blockchain para garantizar su trazabilidad y autenticidad.

2. Creación del NFT

Simultáneamente, la plataforma genera un NFT que representa esta evidencia. El NFT incluye:

- El hash criptográfico del video.
- Metadatos básicos como el número de atestado, la fecha de captura y la clave pública del agente que subió la evidencia.
- Enlace al contenido digital, almacenado en un sistema descentralizado como IPFS o Piñata. Por ejemplo, un CID (Identificador de contenido) asociado al archivo podría ser: QmXjAfSUviJ98JSYmKXAqxWTX14tpnW8R35.

Este NFT se registra en la blockchain, vinculando de manera inmutable el hash, los metadatos y el CID.

3. Almacenamiento seguro

El archivo original del video no se almacena directamente en la blockchain debido a restricciones de tamaño y costo. En su lugar, se emplea un sistema híbrido de almacenamiento que combina el uso de IPFS y un Centro de Procesamiento de Datos (CPD). El archivo se guarda en IPFS, un sistema de almacenamiento descentralizado que utiliza nodos distribuidos para garantizar su disponibilidad y resiliencia.

El CID que identifica de manera única el archivo en IPFS, se vincula al NFT registrado en la blockchain, asegurando la integridad del contenido mediante un mecanismo de validación criptográfica.

Adicionalmente, el archivo se almacena duplicado en el CPD, proporcionando redundancia y un acceso seguro en un entorno controlado. Esta fórmula híbrida refuerza la resiliencia del sistema al combinar las ventajas de la descentralización con la confiabilidad de una infraestructura física crítica.

4. Transferencia de custodia

Durante el proceso de investigación, la custodia de la evidencia puede transferirse entre actores (por ejemplo, de la policía a la fiscalía). Esta transferencia se realiza mediante un contrato inteligente preprogramado con reglas específicas para garantizar transparencia y trazabilidad.

Cada vez que se transfiere el NFT, la blockchain registra automáticamente la operación, incluyendo:

- Fecha y hora.
- Identidad de los actores involucrados, verificada a través del sistema PKI.
- Estado actualizado de la evidencia.

¹⁸ <https://es.cointelegraph.com/news/chinas-supreme-court-rules-that-blockchain-can-legally-authenticate-evidence>

5. Verificación en un juicio

En el juicio, el juez o las partes interesadas pueden acceder al NFT y verificar su autenticidad mediante el hash registrado en la blockchain. Además, el archivo se descarga desde IPFS utilizando el CID asociado. Para confirmar que el archivo no ha sido manipulado, se genera un nuevo hash del contenido descargado y se compara con el registrado en el NFT. Si ambos coinciden, se garantiza la integridad de la evidencia.

5.4.3 Detalles Técnicos y ventajas de implementación.

Blockchain como base de trazabilidad:

La blockchain funciona como un registro distribuido e inmutable donde cada interacción con las evidencias queda almacenada de manera permanente y verificable. Cada transacción registrada asegura que no haya alteraciones y garantiza la trazabilidad de la cadena de custodia.

- Tecnología utilizada: mediante la implementación de bloques enlazados criptográficamente y verificados mediante protocolos de consenso como Prueba de Autoridad (PoA-Proof of Authority) debido a los validadores como autoridades judiciales y policiales.

NFTs para certificar propiedad y metadatos:

Los NFTs permiten asociar cada evidencia digital a un identificador único. Estos incluyen metadatos que detallan su origen, fecha de creación, hash criptográfico y otros datos relevantes.

- Tecnología utilizada: gestión mediante estándares en blockchain como ERC-721 (compatible con IPFS), que asegura la singularidad y la inmutabilidad de los datos asociados al NFT, mediante un identificador único (*tokenId*).

Almacenamiento descentralizado en IPFS:

IPFS permite almacenar los archivos digitales de forma distribuida. Los archivos son identificados mediante un CID, que es un hash único generado en función del contenido. Este sistema asegura disponibilidad continua incluso en caso de fallos de nodos y que cualquier modificación en el archivo sea detectable.

- Tecnología utilizada: red de nodos distribuidos que permite acceder a los datos almacenados utilizando su CID.

Contratos inteligentes para automatización:

Los contratos inteligentes automatizan procesos relacionados con la gestión de evidencias, como la transferencia de custodia y la asignación de permisos. Su ejecución está programada para ocurrir automáticamente al cumplirse ciertas condiciones.

- Tecnología utilizada: código escrito en lenguajes específicos como *Solidity*, implementado en la blockchain.

Validación con PKI:

El sistema PKI autentica a los usuarios y garantiza la legitimidad de las interacciones mediante certificados digitales. Estos certificados aseguran la identidad del usuario y protegen las transacciones con firmas digitales.

- Tecnología utilizada: emisión de certificados mediante una Autoridad de Certificación y validación de identidad a través de claves públicas y privadas.

6 PROPUESTA DE PLATAFORMA DE INTERCAMBIO DE EVIDENCIAS DIGITALES

6.1 Introducción

En el contexto actual de transformación digital en las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y la Administración de Justicia, surge la necesidad de abordar los desafíos asociados al manejo de evidencias digitales mediante una solución integral. La propuesta que se presenta en este capítulo se centra en el diseño y desarrollo de una plataforma de intercambio de evidencias digitales con el objetivo de superar las limitaciones del sistema actual y ofrecer garantías adicionales en términos de seguridad, integridad y trazabilidad de las evidencias. La plataforma será denominada **EviCloud**.

EviCloud busca revolucionar la manera en que se manejan las evidencias digitales, integrando tecnologías avanzadas como blockchain y NFTs para garantizar su integridad y trazabilidad desde el momento de su obtención hasta su presentación en juicio. Además, se prevé la creación de un sistema robusto y escalable, diseñado para responder a las exigencias actuales y futuras del ámbito jurídico y policial, facilitando la colaboración interinstitucional y minimizando los riesgos asociados al factor humano.

Además del desarrollo de la propuesta y sus funcionalidades, se presenta una maqueta o mockup de un prototipo inicial que ilustra el diseño de la interfaz y algunas de sus funcionalidades básicas. (Ver Anexo II)

La gestión de evidencias digitales plantea retos únicos, desde la preservación de su integridad y autenticidad hasta la necesidad de facilitar su intercambio entre diversas entidades implicadas en el proceso judicial. Como se ha descrito en capítulos anteriores, el crecimiento exponencial del volumen de ciberdelitos y la diversidad de formatos en los que se presentan las evidencias digitales han puesto de manifiesto la insuficiencia de los métodos tradicionales de almacenamiento y transferencia. En este sentido, las limitaciones en capacidad de almacenamiento, la dependencia de soportes físicos y las demoras en la cadena de custodia evidencian la necesidad de un sistema más eficiente y confiable.

En este capítulo se describirán, en detalle, los principales componentes y funcionalidades de la plataforma, incluyendo los casos de uso previstos, los diseños del backend y frontend, las funcionalidades asignadas a los diferentes roles de usuario, así como los mecanismos de auditoría y control de datos. También se abordará la infraestructura física y tecnológica necesaria para su implementación, con el fin de garantizar la disponibilidad y seguridad del sistema. Este enfoque integral permitirá no solo modernizar los procedimientos actuales, sino también establecer un nuevo estándar en la gestión de evidencias digitales en España.

6.2 Casos de uso

Este apartado presenta un caso de uso genérico en el que recoge la totalidad de las funciones que contempla de manera inicial la plataforma y que el mismo sirve como base para el diseño y desarrollo de esta.

Aunque se describen diversas funcionalidades, el acceso a las mismas dependerá del rol del usuario, garantizando que los privilegios sean asignados de manera adecuada para proteger la integridad y la seguridad del sistema.

Las funciones iniciales diseñadas para la plataforma son las siguientes:

1. Oficios Policiales

Gestión de oficios relacionados con investigaciones policiales:

- **Todos los oficios:** Acceso completo a todos los oficios registrados para una visión integral del estado de los casos.
- **Oficios policiales pendientes:** Identificación de oficios que requieren gestión inmediata para priorizar tareas.
- **Oficios policiales tramitados:** Historial de oficios finalizados, útil para auditorías y revisiones.

2. Mandamientos Judiciales

Gestión de mandatos emitidos por las autoridades judiciales:

- **Todos los mandamientos:** Registro de todos los mandamientos, independientemente de su estado.
- **Pendientes de evidenciar:** Mandatos que necesitan evidencias asociadas, destacando los pendientes de gestión.

3. Evidencias Digitales

Módulo para la gestión y análisis de evidencias digitales:

- **Crear Evidencia Digital:** Registro de nuevas evidencias con metadatos y vinculación a casos.
- **Árbol Judicial:** Representación visual y jerárquica de evidencias relacionadas en un caso.

4. Conservación de Datos

Gestión de las solicitudes relacionadas con la retención de información:

- **Todas las solicitudes:** Centralización de solicitudes para asegurar su rastreabilidad.
- **Pendientes de evidenciar:** Solicitudes sin evidencias asociadas, priorizando su resolución.

5. Sistema de Incidencias

Gestión estructurada de problemas y fallos detectados en el sistema:

- **Crear incidencia:** Registro de problemas por parte de los usuarios.
- **Todas las incidencias:** Listado general para auditorías y análisis.
- **Incidencias abiertas:** Problemas pendientes de resolución.
- **Incidencias en trámite:** Seguimiento de incidencias en proceso de gestión.
- **Incidencias cerradas:** Historial de problemas solucionados.
- **Incidencias rechazadas:** Registro de problemas descartados con su justificación.

Las funcionalidades que hemos descrito anteriormente serían las iniciales que aparecerían en una primera versión de la plataforma, aunque también se barajan otras opciones que deben ser añadidas en versiones posteriores o evolutivos desarrollados ad-hoc con los usuarios. Estas funcionalidades añadidas deberán estar listas una vez la plataforma entre en la fase de producción.

Casos de Uso Adicionales

1. Gestión de Usuarios y Roles

- **Crear usuarios:** Registro de nuevos usuarios para definir su acceso y funciones.
- **Asignar roles:** Configuración y modificación de permisos según necesidades.
- **Revisar actividad de usuarios:** Auditoría de acciones realizadas para garantizar transparencia.

2. Auditorías y Reportes

- **Generar reportes:** Creación de informes detallados sobre evidencias, mandamientos, incidencias y más.
- **Revisión de auditorías:** Validación de trazabilidad e integridad de la información registrada.

3. Notificaciones y Alertas

- **Alertas automáticas:** Notificaciones sobre plazos críticos, incidencias o vencimientos.
- **Notificaciones personalizadas:** Configuración de avisos adaptados a los roles y preferencias del usuario.

6.3 Diseño de sistema BACKEND

El diseño del sistema *back-end* para la plataforma se basará en tecnologías robustas, flexibles y escalables que aseguren la correcta gestión y operación de evidencias digitales. Se han elegido una serie de tecnologías de manera que se garantice el cumplimiento de los requerimientos funcionales y técnicos, además de preparar la plataforma para futuras expansiones y actualizaciones. Destacamos los siguientes componentes clave del sistema con algunas de las ventajas que aporta cada uno:

Lenguaje de programación - Java 8

- Compatibilidad con J2EE para una integración escalable y estandarizada.
- Rendimiento y estabilidad, además de compatibilidad con bibliotecas y frameworks necesarios.
- Amplio soporte.

Framework - Spring Boot

- Desarrollo ágil en la creación de microservicios modulares.
- Facilidad de configuración centralizada para la gestión de dependencias y seguridad.
- Escalabilidad.

Microservicios bajo un modelo Software-as-a-Service (SaaS)

- Modularidad, así cada funcionalidad estará encapsulada en un servicio independiente.
- Despliegue, desarrollo y escalabilidad independiente.
- Recuperación rápida en caso de fallos de componentes individuales, garantizando la continuidad del servicio.

Blockchain – Ethereum

- Transparencia y descentralización que garantiza un registro inmutable y seguro de las operaciones, esencial para la cadena de custodia de evidencias.
- Contratos inteligentes para la automatización de procesos como el registro y transferencia de evidencias, cumpliendo con las reglas establecidas.

- Compatibilidad y escalabilidad:
 - o Implementación de estándares como **ERC-721**, que encapsulan las evidencias y su metadata, asegurando su integridad.
 - o Uso de almacenamiento descentralizado para datos asociados a las evidencias que no se registran directamente en la blockchain, optimizando el uso de recursos y manteniendo la privacidad.
 - o Preparación para **Ethereum 2.0**, que introduce mejoras en escalabilidad y eficiencia energética.

Comunicación entre los componentes del sistema mediante **API REST**

- Interoperabilidad con otros sistemas externos utilizados por las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).
- Seguridad: autenticación mediante **OAuth 2.0** y cifrado de datos mediante **HTTPS**.
- Los endpoints optimizados para manejar grandes volúmenes de datos de manera eficiente.

Bases de Datos Oracle 19 o superior

- Replicación, respaldo y recuperación, para la integridad y disponibilidad de las evidencias digitales.
- Volumen de rendimiento alto para transacciones y consultas complejas.
- Escalabilidad.

Infraestructura

- **Sistema Operativo - Red Hat 7**, para un entorno estable para aplicaciones empresariales.
- **Virtualización - VMware 6.5**, para la gestión eficiente de recursos de hardware subyacentes y con una alta disponibilidad.
- **Servidor Web - Apache**, utilizado para manejar solicitudes web y proporcionar una base robusta para la capa de presentación.
- **Servidor de Aplicación - JBoss 7.0.4 EAP**, con un entorno optimizado para la ejecución de aplicaciones Java y asegura la estabilidad de los servicios.

Arquitectura modular y abierta

- Flexibilidad, que permita la integración de nuevos módulos sin interrupciones.
- Mantenimiento simplificado, facilitando las actualizaciones y la resolución de problemas sin afectar la operación continua.
- Escalabilidad.

Calidad del desarrollo

- Siguiendo las mejores prácticas de ingeniería de software, garantizando código limpio, seguro y eficiente a través de los estándares de calidad.
- Compatibilidad, para que las aplicaciones desarrolladas cumplan con las políticas y estándares establecidos para asegurar la integración homogénea en los sistemas de las FCSE.

6.4 Diseño de sistema FRONT

El diseño del *front* de la plataforma tiene como objetivo principal proporcionar una experiencia de usuario intuitiva y eficiente, alineada con los requisitos específicos de los actores que participan en la gestión de evidencias digitales (investigadores forenses, autoridades judiciales, administradores y auditores). Este apartado se enfoca en la creación de una interfaz gráfica (UI) funcional y accesible, garantizando que los usuarios puedan navegar y operar fácilmente mientras mantienen los más altos estándares de seguridad.

Para desarrollar el diseño, se adoptaron principios de diseño centrado en el usuario priorizando accesibilidad, usabilidad y simplicidad. El diseño responde también a las exigencias legales y técnicas, como el cumplimiento de la trazabilidad en la cadena de custodia y la protección de datos sensibles.

6.4.1 Elementos principales del diseño

Los elementos del front están organizados en módulos funcionales para cada tipo de usuario. Cada módulo está diseñado para cumplir con los roles y responsabilidades asignados. A continuación, se detallan los componentes principales:

- **Dashboard principal:**
 - Vista general para cada usuario con datos clave (número de evidencias gestionadas, incidencias pendientes, actividades recientes).
 - Indicadores visuales y notificaciones para resaltar aspectos críticos.
 - Barra lateral para acceso rápido a las principales funciones de la plataforma.
- **Carga de evidencias:**
 - Formularios sencillos para cargar archivos digitales.
 - Campos predefinidos con metadatos obligatorios (tipo de evidencia, fecha, caso asociado).
 - Indicadores de carga exitosa y validación automática del hash.
- **Gestión de usuarios:**
 - Pantalla de administración de roles y permisos.
 - Función de búsqueda avanzada por nombre, rol, o unidad de pertenencia.
 - Opciones para añadir, editar o desactivar usuarios según las jerarquías establecidas.
- **Visualización y búsqueda de evidencias:**
 - Motor de búsqueda con filtros avanzados (por tipo, caso, fecha, usuario, entre otros).
 - Vista previa de documentos y archivos multimedia directamente en la plataforma.
 - Función de exportación de registros con permisos controlados.
- **Historial y cadena de custodia:**
 - Interfaz cronológica que muestra cada acción realizada sobre las evidencias.
 - Integración con gráficos y tablas que representen visualmente los cambios realizados.
 - Indicadores de auditoría para identificar irregularidades de forma rápida.

6.4.2 Herramientas utilizadas

Para crear los *mockups*¹⁹ y prototipo del diseño del *front*, se ha utilizado como herramienta especializada que permiten simular el funcionamiento real de la plataforma:

Canva, creando pantallas estáticas que representan de manera visual detallada y funcional los diferentes roles diseñados para una versión inicial de la plataforma en etapa de preproducción. Estas representaciones gráficas sirven como una aproximación conceptual y deberán ser trabajadas en mayor profundidad en fases posteriores. En esas etapas, el diseño será adaptado específicamente a las necesidades de cada rol y usuario mediante un enfoque *ad hoc*.

La siguiente herramienta que se utilizaría para tener una maqueta ya funcional para el front-end sería **Angular**, cuyo enfoque estructurado y escalable lo convierte en una buena opción ya que aporta un rendimiento óptimo y una experiencia de usuario fluida.

6.4.3 Mockups y estructura visual

El diseño del *front* ²⁰ incluye capturas de pantallas representativas que serán anexadas al trabajo. Estas imágenes se organizan en las siguientes categorías:

1. **Pantalla principal:** resumen inicial que incluye accesos rápidos y notificaciones.
2. **Módulo de carga:** campos clave para registrar una nueva evidencia digital.

¹⁹ Mockup: representación virtual de un prototipo del proyecto, como un fotomontaje o maquetación virtual.

²⁰ Ver Anexo II

3. **Motor de búsqueda:** ejemplo de uso con filtros aplicados.
4. **Trazabilidad:** vista cronológica de las acciones realizadas sobre una evidencia.
5. **Informes:** plantilla de un reporte automatizado sobre el cumplimiento.

El diseño visual prioriza colores neutros para transmitir profesionalidad (azul, negro, blanco y gris) con acentos de colores distintivos (como naranja y rojo para alertas).

6.5 Usuarios, roles y funciones

La plataforma soportará una estructura jerárquica de roles que define los permisos y accesos de cada usuario, garantizando que cada actor involucrado en la cadena de custodia cumpla con sus funciones específicas dentro de un marco seguro y controlado. Los roles principales son los siguientes:

Administrador del Sistema

El administrador del sistema tiene la responsabilidad de gestionar los aspectos técnicos y organizativos de la plataforma, asegurando su correcto funcionamiento y seguridad.

- **Funciones principales:**

1. **Gestión de usuarios y roles:**

- Crear, modificar o eliminar perfiles de usuario.
- Asignar roles y permisos específicos según las necesidades operativas.
- Configurar las políticas de acceso para garantizar el cumplimiento normativo.

2. **Configuración de permisos:**

- Definir niveles de acceso y acciones permitidas para cada rol.
- Establecer restricciones sobre la visualización y manejo de evidencias.

3. **Mantenimiento y seguridad:**

- Realizar actualizaciones del sistema y aplicar parches de seguridad.
- Gestionar copias de seguridad para prevenir pérdida de datos.
- Supervisar la infraestructura técnica para evitar vulnerabilidades.

4. **Supervisión del uso:**

- Monitorear las actividades de los usuarios en la plataforma.
- Detectar accesos no autorizados o comportamientos anómalos.
- Generar alertas sobre posibles violaciones de seguridad.

5. **Control de logs de actividad:**

- Acceso y supervisión detallada de los registros de actividad de los usuarios para identificar posibles anomalías.
- Generación de reportes periódicos sobre el uso del sistema.

Investigador Forense

El investigador forense es responsable de registrar, analizar y documentar evidencias digitales, actuando como el enlace técnico entre las evidencias y los casos judiciales.

- **Funciones principales:**

1. **Registro de nuevas evidencias:**

- Ingresar evidencias digitales en el sistema.
- Asociar metadatos relevantes (fecha, tipo de archivo, caso relacionado, etc.).
- Garantizar la trazabilidad de las evidencias desde su registro.

2. Generación de informes y solicitudes judiciales:

- Elaborar informes técnicos detallados sobre los análisis realizados.
- Preparar solicitudes judiciales relacionadas con los hallazgos obtenidos.

3. Remisión de oficios:

- Solicitar autorizaciones judiciales para análisis específicos.
- Emitir peticiones formales para la realización de pruebas o peritajes adicionales.

4. Colaboración con otros investigadores:

- Compartir análisis o hallazgos con otros investigadores (si fuera necesario) en casos conjuntos, manteniendo trazabilidad de las interacciones.

5. Restricción de acciones:

- No tienen permisos para modificar o eliminar registros existentes.
- No pueden transferir evidencias fuera de los límites definidos por su jurisdicción.
- Sus acciones están limitadas al análisis técnico y la generación de reportes.

Autoridad Judicial

La autoridad judicial tiene un rol clave en la toma de decisiones sobre las evidencias digitales y la supervisión del cumplimiento de la cadena de custodia.

• **Funciones principales:**

1. Acceso ilimitado a casos relevantes:

- Visualizar todas las evidencias vinculadas a un caso específico.
- Garantizar que ningún elemento probatorio quede fuera de su análisis.

2. Ordenar acciones específicas:

- Emitir instrucciones como congelar evidencias para evitar su modificación.
- Solicitar la entrega de evidencias originales.
- Autorizar el acceso a nuevos investigadores o peritos.

3. Consulta de informes y remisión de autorizaciones:

- Revisar análisis técnicos e informes forenses.
- Emitir autorizaciones necesarias para continuar con el manejo de evidencias.

4. Garantía de la cadena de custodia:

- Supervisar que las evidencias no sean manipuladas indebidamente.
- Asegurar la integridad y trazabilidad de las evidencias desde su origen hasta su uso en procesos judiciales.

5. Priorizar casos críticos:

- Identificar y marcar casos como prioritarios, asignando mayor urgencia a su gestión dentro de la plataforma.

6. Historial de decisiones:

- Consultar un registro de las decisiones tomadas en relación con las evidencias de un caso, incluyendo autorizaciones, rechazos y observaciones.

Auditor

El auditor es el responsable de revisar y validar los procesos relacionados con las evidencias digitales, asegurando que se cumplan los protocolos establecidos.

- **Funciones principales:**

- 1. Revisión de registros:**

- Inspeccionar el historial de transacciones relacionadas con evidencias.
- Verificar la trazabilidad en la cadena de custodia.

- 2. Verificación de integridad:**

- Validar que las evidencias no hayan sido alteradas desde su registro en el sistema.
- Realizar comprobaciones técnicas, como la verificación de hash de los archivos.

- 3. Informes de cumplimiento:**

- Preparar reportes sobre la adherencia a los procedimientos establecidos.
- Utilizar herramientas para identificar patrones de comportamiento inusuales en el acceso y manejo de evidencias.
- Identificar y documentar posibles irregularidades o desviaciones.
- Verificar que las incidencias críticas relacionadas con evidencias sean atendidas dentro de los plazos adecuados.

- 4. Restricciones operativas:**

- No tiene permisos para modificar, eliminar o añadir evidencias.
- Su rol es exclusivamente de supervisión, garantizando la independencia de sus evaluaciones.

Estructura de Permisos

Cada rol tendrá un conjunto de permisos predefinidos que se alinean con sus funciones específicas. Esta segmentación asegura que:

- Los usuarios accedan únicamente a la información y funcionalidades necesarias para sus responsabilidades.
- La seguridad e integridad de la información estén protegidas en todo momento.
- Se cumplan las normativas legales y de la cadena de custodia.

Para el **Acceso y la Autenticación**, la plataforma deberá incorporar controles de acceso avanzados, incluyendo la autenticación multifactor (MFA) obligatoria para todos los usuarios. Este método combinará al menos dos factores de autenticación, como contraseñas y códigos de un solo uso (OTP), y podrá ampliarse en futuros evolutivos para integrar métodos adicionales, como autenticación biométrica, según sea necesario. Las políticas de permisos basadas en roles garantizarán que solo los usuarios autorizados accedan a las funcionalidades y datos correspondientes.

Además, será esencial implementar un plan de contingencia que contemple políticas de respaldo y recuperación de datos, con pruebas periódicas para validar su eficacia. Cualquier intento de acceso no autorizado deberá ser detectado y gestionado mediante alertas automáticas, bloqueos preventivos y medidas de recuperación para asegurar la continuidad del sistema y la protección de la información.

6.6 Auditoría y control de datos

En este apartado se detalla la implementación de procesos de auditoría y control de datos para garantizar la integridad, trazabilidad y confiabilidad de las evidencias digitales. Utilizando tecnologías

de sellado de tiempo, hash criptográfico, blockchain y NFT, se garantiza que las evidencias cumplan con los estándares legales y los protocolos de cadena de custodia.

Los objetivos prioritarios de esta funcionalidad implementada en la plataforma son principalmente:

- Garantizar la **integridad** de las evidencias digitales a lo largo de su ciclo de vida.
- Verificar la **trazabilidad** en la cadena de custodia mediante registros inmutables.
- Detectar **irregularidades** o desviaciones en los procesos de manejo y acceso.
- Generar informes de cumplimiento que respalden la validez de las evidencias ante autoridades judiciales.

Para alcanzar estos objetivos, utilizaremos una serie de herramientas tecnológicas mencionadas en el capítulo 5, cada una de las cuales tiene una aplicación directa y específica en relación con dichos objetivos, es decir:

Herramienta tecnológica	Objetivo
Blockchain	Integridad y trazabilidad
Hash criptográfico (SHA-256)	Integridad
NFT	Asociación de metadatos y trazabilidad única
Sellado de Tiempo	Certificación de fecha y hora exacta
Sistemas de Monitorización	Herramientas de auditoría y generación de informes

Tabla 6-1 – Herramientas Tecnológicas

La metodología que utilizaremos con cada una de las herramientas será la siguiente:

Blockchain

Proceso: cada evidencia digital se registra en la blockchain mediante un **hash criptográfico único**, generado a partir del contenido íntegro de la evidencia digital. Además, el registro incluye información complementaria, como datos de la cadena de custodia (identificación del custodio, fecha y hora de transferencias). Este diseño asegura que los registros sean inmutables y verificables, protegiéndolos contra alteraciones. Durante auditorías y movimientos dentro de la plataforma, el hash se compara con el contenido original de la evidencia para confirmar su integridad.

Hash Criptográfico

Proceso: en la recogida de la evidencia, se genera un **hash criptográfico único (SHA-256)** que actúa como identificador inmutable de la evidencia. Este hash no se registra como un elemento separado en la blockchain, sino que se integra como un **atributo interno del NFT** asociado a la evidencia, formando parte de sus metadatos.

Durante el proceso de auditoría, se compara el hash registrado en el NFT con el hash recalculado a partir de la evidencia. Si ambos coinciden, se confirma que no ha habido alteraciones en la evidencia, garantizando su integridad. Este diseño permite que el hash y el NFT estén intrínsecamente vinculados, optimizando el registro y garantizando la trazabilidad y seguridad de las evidencias.

NFT

Proceso: cada evidencia digital se vincula a un NFT único, que contiene metadatos relevantes como la identificación de la evidencia, el hash original, información de la cadena de custodia y roles asociados. Esto permitirá auditar en tiempo real cualquier transferencia o modificación.

Sellado de Tiempo

Proceso: en el momento del registro, se aplica un sellado de tiempo certificado a la evidencia, que se almacena junto con su hash en la blockchain. Con esto se asegura y demuestra su existencia en un momento concreto, respaldando la cadena de custodia.

Sistemas de Monitorización

Proceso: El sistema de monitorización implementado tiene como objetivo registrar y auditar de forma segura todas las actividades relevantes en la plataforma, garantizando tanto la integridad de los datos como la privacidad de la información. Las principales funciones incluyen:

- **Registro de accesos:** se almacenan datos sobre los accesos de usuarios autorizados, incluyendo la fecha, hora y las operaciones realizadas.
- **Detección de actividades anómalas:** se generan alertas automáticas en caso de accesos no autorizados o comportamientos sospechosos, permitiendo una respuesta ágil ante posibles incidentes de seguridad.
- **Integración con blockchain:** todos los registros se integran en la blockchain como bloques adicionales, asegurando su integridad y trazabilidad. Esto permite que los nodos participantes verifiquen la validez de los registros sin comprometer la privacidad de los datos sensibles.
- **Generación de informes:** el sistema genera informes automatizados en formatos estándar (PDF y CSV), documentando información clave como:
 - Transacciones verificadas.
 - Cumplimiento de la cadena de custodia.
 - Análisis de anomalías y recomendaciones de mejora.

Para garantizar que los nodos puedan verificar los registros almacenados en la blockchain sin comprometer la confidencialidad de los datos sensibles, se han implementado las siguientes soluciones:

- Cifrado de datos sensibles: los registros se almacenan cifrados en los bloques de la blockchain, permitiendo que los nodos validen la integridad de los bloques (a través de hashes o firmas digitales) sin tener acceso al contenido cifrado.
- Zero-Knowledge Proofs (ZKP): estas pruebas permiten que los nodos verifiquen que los registros cumplen con los criterios de validez (como accesos legítimos o alertas reales) sin revelar la información subyacente.
- Control de acceso basado en roles: se definen roles específicos para los nodos y los usuarios, asignando permisos según sus responsabilidades. Por ejemplo, los nodos auditores tienen permisos adicionales para acceder a ciertos datos, mientras que otros nodos solo verifican integridad sin acceso al contenido.
- Uso de datos fuera de la blockchain (off-chain): en algunos casos, los datos más sensibles se almacenan fuera de la blockchain en sistemas externos seguros. La blockchain registra solo referencias (hashes) que permiten verificar la integridad sin exponer directamente el contenido.

Las funciones asociadas para cada uno de los roles y responsabilidades que se han definido en el apartado anterior referentes a esta parte de control de datos y auditoría serían:

Auditor:

- Revisa los registros blockchain y valida los hashes.
- Genera informes de cumplimiento.

Investigador Forense:

- Integra las evidencias digitales en la plataforma.

Autoridad Judicial:

- Evalúa los informes de auditoría para validar la cadena de custodia.

6.7 Infraestructura física y hardware

Como se mencionó brevemente en el apartado 3.3 sobre la Seguridad de la Información, para abordar este punto es esencial remitirnos al Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS). En su artículo 40, este decreto establece las diferentes categorías de seguridad para los sistemas de información. De acuerdo con este esquema, el sistema objeto de este trabajo se clasifica con un nivel de seguridad **ALTO**, dada la criticidad de los datos y procesos que maneja.

6.7.1 Infraestructura física

El Centro de Procesamiento de Datos (CPD), que aloja los servidores de la plataforma de gestión digital de evidencias, se clasifica como una **infraestructura crítica** debido al nivel de seguridad requerido. Cualquier incidente o ataque podría comprometer la disponibilidad, integridad y accesibilidad de las evidencias digitales, afectando directamente procesos judiciales y de seguridad pública. Por este motivo, su diseño y operación se basan en estándares estrictos que garantizan la protección de los datos, la confidencialidad y la continuidad del servicio.

Características principales del CPD

En una blockchain híbrida como la que se plantea, los nodos pueden operar tanto en infraestructuras internas (CPD) como externas (Nube). No todos los nodos necesitan estar ubicados físicamente en el CPD, pero sí que el CPD desempeña un papel crucial en la configuración de nodos clave para garantizar:

- Control y seguridad local: nodos críticos pueden alojarse en el CPD para mantener un control físico y asegurar el cumplimiento normativo.
- Interoperabilidad: el diseño híbrido permite que otros nodos estén distribuidos en la nube, beneficiándose de la escalabilidad y redundancia que ofrece este modelo.

Por tanto, la infraestructura física asegura que los nodos en el CPD mantengan la capacidad de respaldo y garantizan una conexión segura con los nodos externos, fortaleciendo la resiliencia del sistema.

- **Topología:** TIER III plus (99,982%) - mantenimiento concurrente:
 - Redundancia en componentes esenciales N+1 (alimentación, refrigeración).
 - Mantenimiento sin afectar a la continuidad de los equipos IT.
- **Distribución geográfica:** sistema redundado en dos sitios físicos con diferente ubicación geográfica, operando en un modelo Activo-Activo.
- Solución técnicamente eficiente además de **segura, escalable y modular**.
- **Reducción de tiempos** para la realización de cambios/actualizaciones.
- Mayor eficiencia en la **gestión y monitorización** para detectar comportamientos anómalos y resolver problemas.

Sistema eléctrico

El sistema eléctrico está diseñado con alta redundancia para garantizar un suministro confiable. Incluye:

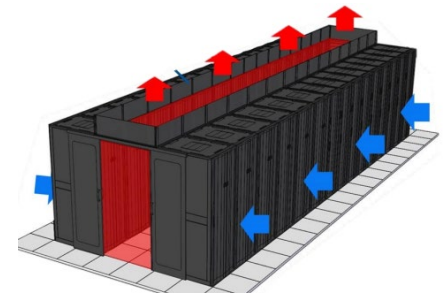
- Dos centros de seccionamiento en superficie y líneas subterráneas de 20 kV para conectar con los centros de distribución.

- Dos centros de distribución en superficie, con celdas de protección y medida para cada centro de transformación.
- Dos centros de transformación soterrados (1250 kVA cada uno), que funcionan de forma independiente y pueden asumir toda la carga en caso de fallo.
- Dos grupos electrógenos (1600 kVA cada uno) para respaldar el sistema en caso de corte eléctrico.
- Dos cuadros generales de baja tensión (CGBT), sistemas de alimentación ininterrumpida (SAIs) y baterías de ion-litio para garantizar la operación continua.

Climatización

El sistema de climatización está diseñado con alta eficiencia y redundancia, asegurando un control climático fiable y continuo en todas las zonas críticas. Incluye:

- Producción de **agua enfriada**: una central con tres enfriadoras (chillers) equipadas con freecooling directo, configuradas en anillo para optimizar el rendimiento.
- **Distribución**: dos ramas hidráulicas independientes garantizando continuidad en caso de fallo.
- **Climatización de salas IT**: climatizadores In-Row integrados en las filas de racks, conectados a ambas ramas de agua para asegurar suministro continuo.
- **Redundancia**:
 - N+1 enfriadoras.
 - 2N grupos de bombeo con N+1 bombas en cada uno.
 - 2N depósitos de seguridad para la conmutación red-grupo.
- **Unidades CRAH**: con impulsión de aire para mantener un ambiente estable en salas de SAIs.
- **Cerramiento de pasillo caliente**: Para optimizar la gestión térmica y mejorar la eficiencia energética en las áreas críticas.



Sistema de Protección contra incendios

El sistema de extinción de incendios NOVEC, utiliza el agente químico **Novec 1230**, que se vaporiza rápidamente para enfriar y sofocar el fuego sin dejar residuos. Es seguro para entornos sensibles como centros de datos, ya que no conduce electricidad, es incoloro e inodoro. Su liberación en forma de niebla asegura una supresión rápida y efectiva de las llamas.

Modelo de Servicio

Nube híbrida: El modelo de servicio sobre nube híbrida permite al organismo interesado mantener el control sobre la implementación y administración de sus aplicaciones y datos, utilizando un portal de autoaprovisionamiento que facilita el acceso a los recursos necesarios en tiempo real.

Por otro lado, el CPD centralizado asume la responsabilidad de gestionar la infraestructura subyacente, incluyendo el mantenimiento del software, la redundancia en el almacenamiento de datos, y el soporte técnico. Este enfoque asegura un entorno robusto, seguro y eficiente para la ejecución de las aplicaciones, maximizando la disponibilidad y el rendimiento.

En la figura se puede observar la distribución de responsabilidades:

- En naranja, se destacan las capas gestionadas directamente por el organismo, correspondientes a las aplicaciones y los datos.
- En azul, se representan las capas gestionadas desde el CPD, que abarcan los elementos fundamentales de infraestructura, como la virtualización,



cómputo, almacenamiento, networking, monitorización, seguridad física, electricidad y refrigeración.

Centro de Supervisión y Control

El Centro de Supervisión y Control se encarga de prevenir, detectar y gestionar incidentes que afecten la infraestructura, seguridad y comunicaciones del CPD. Utiliza un **sistema de gestión BMS** que centraliza y controla de manera integral todos los sistemas, como iluminación, energía, seguridad, incendios y climatización. Este sistema permite el monitoreo en tiempo real, optimiza la operación, reduce costos y facilita el tratamiento ágil de incidencias. Además, contribuye al rendimiento energético al monitorear emisiones de CO₂ y consumo de energía, ayudando a reducir la huella de carbono y mejorar la sostenibilidad del CPD.

Servicio de Seguridad TIC

En el que podemos ver los siguientes niveles de servicio:

- **Niveles I y II - Monitorización y Detección:**
 - Soporte presencial 24x7 en las instalaciones.
- **Nivel III - Servicios Especializados:**
 - Soporte especializado 8x5 en las instalaciones.
 - Soporte adicional bajo demanda.
- **Servicios de Prevención de Incidentes** como: análisis automatizado de vulnerabilidades, pentesting, análisis de seguridad de código, vigilancia digital, capacitación y concienciación en seguridad.
- **Servicios de Detección de Incidentes** como: Sistema EDR (Endpoint Detection and Response), monitorización de eventos de seguridad, detección de incidentes (nivel I), búsqueda proactiva de amenazas (Threat Hunting), detección de fugas de información, alerta temprana ante amenazas.
- **Servicios de Protección de Seguridad** como: seguridad perimetral, navegación y trabajo remoto protegido.
- **Gestión y Respuesta ante Incidentes de Seguridad TIC** como: análisis y respuesta a incidentes (niveles II y III), gestión de crisis, análisis forense, laboratorio especializado en análisis de malware.

6.7.2 Hardware

Para aproximar el alcance necesario sobre este apartado, en la parte que afecta a las FCSE, teniendo en consideración el crecimiento mensual de almacenamiento del Sistema, sería necesario disponer de cabinas de almacenamiento, junto con su electrónica de red, con un crecimiento de 40 terabytes mensuales por Cuerpo a lo cual habría que sumar el sistema de gestión de evidencias compuesto 4/4 *blades* de servidores con su licenciamiento.

Para el cálculo de almacenamiento para los datos recibidos, en el caso de Policía Nacional, se reciben una media de 40TB/mes que deberán ser evidenciados. Incluye información de informes periciales de la Comisaría General de Policía Científica y las intervenciones de las Comisarias General de Policía Judicial e Información. Se estimaría un alcance similar para las Unidades de Guardia Civil.

A continuación, se presenta una propuesta de hardware viable para el despliegue de nuestro sistema, garantizando calidad y un funcionamiento óptimo:

- **Chasis y servidores tipo “Blade”**
 - **Chasis Blade:** HPE Synergy 12000 o Dell PowerEdge MX7000, con alta densidad y escalabilidad.
 - **Servidores Blade:** 4 iniciales (expansibles a 6 u 8), con:
 - Procesadores: Intel Xeon Scalable o AMD EPYC (16 núcleos, doble socket).
 - Memoria RAM: 512 GB (expandible a 1 TB).
 - Almacenamiento local SSD: 2 TB NVMe.
 - Conectividad: Fibra (10/25 Gbps) y Ethernet (1/10 Gbps).
- **Controladoras de almacenamiento**
 - Modelos: NetApp AFF A250 o Dell EMC PowerStore.
 - Soporte para alta disponibilidad y replicación en tiempo real.
 - Interfaces: FC, iSCSI, NVMe-oF.
- **Cabinas de disco de distintas capacidades**
 - Capacidades: Desde 100 TB hasta 500 TB, para datos secundarios.
 - Modelo sugerido: HPE MSA 2060 o Synology FS6400.
 - Tipo de discos: HDD SAS con caché SSD.
- **Cabinas de almacenamiento principales (1 PB cada una)**
 - Modelos: Dell EMC Unity XT 680F o Pure Storage FlashArray//C.
 - Capacidad inicial: 1 PB por cabina, sincronizadas para alta disponibilidad.
 - Discos: SSD NVMe para máximo rendimiento.
- **Switches de fibra y Ethernet**
 - **Fibra:** Brocade G630 o Cisco MDS 9148T, con soporte para 32 Gbps por puerto.
 - **Ethernet:** Cisco Catalyst 9500 o Arista 7050X3, con puertos de 1/10 Gbps y uplinks de 25/100 Gbps.
- **Firewalls de perímetro redundados**
 - Modelos: Palo Alto Networks PA-3250 o Fortinet FortiGate 600E.
 - Configuración: Redundancia activa-activa.
 - Funcionalidades: Inspección en tiempo real, IPS, segmentación de red, y VPN.
- **Licenciamiento de aplicativos de intercambio**
 - Licencias para 100 usuarios concurrentes, escalables.
 - Soluciones compatibles: Elastic Stack o Microsoft Azure Data Share.

6.8 Plan de formación

Dentro de los objetivos globales de la plataforma de intercambio de evidencias digitales, se incluye la implementación de un **plan de formación continuo y estructurado**. Este plan tiene como finalidad dotar a los integrantes de las Fuerzas y Cuerpos de Seguridad (FCS), autoridad judicial y demás actores relevantes de los conocimientos, habilidades y recursos necesarios para adoptar y optimizar el uso de la plataforma. Además, busca fomentar un entorno de compartición del conocimiento que permita establecer pautas comunes, mejorar la operativa y garantizar la sostenibilidad del proyecto a lo largo del tiempo.



Figura 6-1 Plan de Formación

6.8.1 Diseño del plan de formación

El plan de formación se diseñará en varias fases, asegurando la alineación con los objetivos definidos para la plataforma y las necesidades específicas de cada perfil involucrado. El proceso incluye:

1. **Identificación de perfiles formativos:** se reconocerán los actores clave del sistema, como agentes de FCSE, personal técnico y administrativo, y operadores judiciales. Para cada perfil se identificarán objetivos formativos específicos, atendiendo a sus responsabilidades dentro del ciclo de vida de las evidencias digitales.
2. **Elaboración de contenidos:** se desarrollarán cursos, manuales, tutoriales y otros materiales adaptados a cada perfil. Los contenidos incluirán temas como:
 - Uso operativo de la plataforma.
 - Seguridad en la gestión de evidencias.
 - Procedimientos asociados a la cadena de custodia.
 - Actualización en normativas y mejores prácticas.
3. **Creación de un calendario de ejecución:** al principio se intensificarán las actividades formativas para asegurar la adopción inicial de la plataforma. En los meses siguientes, se realizarán acciones de refuerzo, revisiones periódicas y formación continua, adaptándose a las necesidades emergentes, como la incorporación de nuevos usuarios.

6.8.2 Métodos de seguimiento y evaluación

La eficacia del plan de formación se monitorizará a través de mecanismos de seguimiento y evaluación, que garantizarán la consecución de los objetivos y permitirán realizar ajustes según sea necesario:

1. **Cuestionarios de evaluación:**
 - Tras cada sesión formativa, los asistentes evaluarán la calidad del contenido, los materiales y el desempeño del formador.
 - Cuestionarios específicos que midan el nivel de conocimiento adquirido y detectar áreas de mejora.
2. **Indicadores de desempeño,** mediante métricas clave para analizar el progreso, como:
 - Porcentaje medio de aciertos en evaluaciones.
 - Valoración media de los formadores.
 - Número de sesiones realizadas frente a las planificadas.
 - Porcentaje de asistencia por perfil.
 - Número de riesgos identificados en el proceso formativo.

3. **Cuadro de mando:** como sistema visual que permita realizar un análisis global y detallado del progreso, con datos segmentados por perfiles, áreas y objetivos. Este recurso facilitará la toma de decisiones orientadas a la mejora continua.

6.8.3 Recursos necesarios

Para el correcto desempeño y realización de este plan de formación son necesarios principalmente los siguientes recursos:

- **Recursos humanos:** el equipo de formación estará compuesto por personal especializado en la plataforma, tanto interno como externo. Además, se involucrará a miembros de FCSE, autoridad judicial y proveedores de la plataforma en las actividades formativas.
- **Recursos materiales:**
 - **Documentos y presentaciones:** procedimientos, manuales y plantillas diseñados para consulta continua.
 - **Material audiovisual:** videos formativos que expliquen procesos clave de manera visual y accesible.
 - **Píldoras formativas:** envío periódico de boletines con novedades y recordatorios clave.
 - **Portal del conocimiento:** plataforma colaborativa que centralice todos los recursos formativos, organizados por perfil y con permisos de acceso controlados.
 - **FAQs:** listas de preguntas frecuentes para resolver dudas habituales rápidamente.
 - **Cuadro de mando:** herramienta para visualizar métricas del proceso formativo.

Este plan de formación no solo garantizará que los usuarios adquieran las habilidades necesarias para operar la plataforma de manera eficiente, sino que también contribuirá a crear un entorno de trabajo colaborativo y orientado a la mejora continua. La integración de un enfoque basado en seguimiento, evaluación y mejora permitirá alinear las capacidades formativas con las necesidades dinámicas de la plataforma y sus usuarios, asegurando el éxito a largo plazo.

7 CONCLUSIONES

El análisis realizado en el TFM destaca que el sistema actual para la gestión de evidencias digitales en las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y el ámbito judicial español enfrenta retos importantes. Entre ellos, el manejo manual de evidencias, el almacenamiento en soportes físicos, la falta de trazabilidad en la cadena de custodia y las demoras en la remisión y consulta de evidencias. Estas limitaciones comprometen la integridad de las pruebas y dificultan su manejo ágil y seguro.

Este trabajo ha permitido alcanzar los objetivos secundarios definidos al inicio:

- **Estudio de la situación actual (OS1):** para ello se realizó un análisis exhaustivo de los procesos actuales de intercambio de evidencias digitales entre las unidades centrales y periféricas de las FCSE y la administración de justicia. Este estudio permitió identificar las principales carencias y definir los procesos críticos que deben ser digitalizados.
- **Análisis de necesidad de transformación digital en organizaciones policiales (OS2):** se ha desarrollado un estudio y análisis mediante un procedimiento de consulta a profesionales en el ámbito de la gestión y uso de evidencias digitales.
- **Diseño de una arquitectura de servicio (OS3):** se ha desarrollado una arquitectura moderna que supera el estado actual del arte, garantizando la integridad del proceso de manejo de evidencias digitales y adaptándose a los requisitos legales y procedimentales actuales.
- **Provisión de un modelo funcional (OS4):** en las secciones 5 y 6 se presenta el diseño de la plataforma **EviCloud**, definiendo roles, flujo de negocio, mecanismos de auditoría y la infraestructura tecnológica necesaria para su implementación.

La propuesta de la plataforma digital **EviCloud** busca superar estas barreras mediante la digitalización y centralización de procesos. La implementación de tecnologías como blockchain y NFTs garantiza la integridad y autenticidad de las evidencias, mientras que un diseño intuitivo optimiza el acceso y la colaboración entre las distintas entidades. Este enfoque no solo mejora la eficiencia operativa, sino que también refuerza la confianza en el sistema judicial.

Una de las metodologías clave que ha facilitado el desarrollo de las conclusiones de este trabajo ha sido el análisis previo de la situación actual, no solo mediante la revisión documental y procedimental, sino también a través de un estudio basado en las aportaciones de los usuarios. Este enfoque ha permitido comprender con mayor precisión las necesidades presentes, así como las perspectivas y el conocimiento de los profesionales involucrados en la gestión de evidencias digitales.

Como se ha expuesto a lo largo del trabajo, la situación actual en el manejo de evidencias digitales presenta múltiples desafíos, desde la falta de herramientas tecnológicas adecuadas hasta problemas estructurales como la dependencia de soportes físicos y la carencia de trazabilidad confiable. Estas carencias no solo afectan la eficiencia operativa, sino que también generan riesgos de invalidación de pruebas esenciales para los procesos judiciales.

La plataforma propuesta en este TFM aporta una solución integral que:

1. Mejora la seguridad y la integridad mediante blockchain y NFTs.
2. Reduce los tiempos de respuesta y errores humanos con un diseño automatizado y centralizado.
3. Facilita el acceso remoto y la colaboración interinstitucional a través de un sistema moderno y escalable.

En conjunto, esta transformación digital no solo modernizará la gestión de evidencias digitales, sino que también fortalecerá la confianza en el sistema judicial, alineándolo con las demandas del entorno digital actual y futuro.

Por último, a partir de los resultados obtenidos en este trabajo, se abren diversas líneas futuras de investigación y desarrollo para fortalecer y expandir la propuesta de la plataforma EviCloud. Entre las principales, se destacan:

1. **Integración con sistemas internacionales:** explorar la interoperabilidad de EviCloud con plataformas de gestión de evidencias digitales utilizadas en otros países, lo que permitiría un intercambio transnacional de pruebas en casos de colaboración internacional, especialmente en delitos cibernéticos.
2. **Ampliación de funcionalidades basadas en IA:** incorporar el uso de herramientas de inteligencia artificial para optimizar la clasificación, búsqueda y análisis de evidencias digitales, facilitando procesos judiciales más ágiles y efectivos.
3. **Análisis de impacto social y legal:** investigar cómo la adopción de esta tecnología afecta la percepción de justicia por parte de los ciudadanos, y analizar posibles adaptaciones normativas para garantizar su correcta implementación y uso.

Estas líneas futuras no solo consolidarán el impacto del trabajo realizado, sino que también permitirán que la plataforma propuesta evolucione para enfrentar los desafíos emergentes del entorno jurídico y tecnológico.

8 BIBLIOGRAFÍA

- [1] «Web de Interior». [En línea] Disponible: <https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/seguridad-ciudadana/Policia-Cientifica-100-anos-de-Ciencia-al-servicio-de-la-justicia-NIPO-126-11-081-7.pdf>. [Último acceso: 1 septiembre 2024].
- [2] «Web de Interior». [En línea] Disponible: https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2022_126200212.pdf. [Último acceso: 1 septiembre 2024].
- [3] Ley de Enjuiciamiento Criminal (LECrim). (Última modificación por Ley Orgánica 1/2015). España.
- [4] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica el Código Penal. Boletín Oficial del Estado, núm. 77, de 31 de marzo de 2015. España.
- [5] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Boletín Oficial del Estado, núm. 251, de 19 de octubre de 2007. España.
- [6] UNE 71505:2013. Seguridad en los sistemas de información y la evidencia digital. Asociación Española de Normalización y Certificación (AENOR).
- [7] Reglamento General de Protección de Datos (RGPD). (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea, L119, 1-88.
- [8] «Web de Poder Judicial». [En línea] Disponible: <https://www.poderjudicial.es/search/AN/openDocument/07530e4a0def9b81a0a8778d75e36f0d/20240521>. [Último acceso: 15 septiembre 2024].
- [9] «Web de Consejo de Europa». [En línea] Disponible : <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>. [Último acceso: 16 septiembre 2024].
- [10] «Web de Consejo de Europa ». [En línea] Disponible : <https://www.coe.int/en/web/cybercrime/tcy-drafting-group>. [Último acceso: 16 septiembre 2024].
- [11] Diego Luis Santiago Gutiérrez, 2022-2023, Trabajo de Fin de Máster Universitario en Dirección TIC para la Defensa, “La cadena de custodia mediante tecnología Blockchain”

- [12] Javier Ángel Fernández-Gallardo, 2022, Letrado de la Administración de Justicia, Juzgado Central de Instrucción nº 4 Audiencia Nacional, “XXXIV Curso de investigación de delitos cometidos a través de las nuevas tecnologías. El papel del Letrado de la Administración de Justicia. Garantía de la evidencia”
- [13] «Web de Gobernanza de ciberseguridad nacional». [En línea] Disponible : <https://gobernanza.ccn-cert.cni.es/ens-navegable>. [Último acceso: 8 octubre 2024].
- [14] «Web de Legal Information Institute». [En línea] Disponible: <https://www.law.cornell.edu/rules/fre>. [Último acceso: 12 octubre 2024].
- [15] «Web de United States Courts». [En línea] Disponible: https://www.uscourts.gov/sites/default/files/2016-04-evidence-agenda_book_final_0.pdf. [Último acceso: 12 octubre 2024].
- [16] DI-001. (2009). Manual de buenas prácticas para el examen de evidencias digitales. Grupo de Trabajo Europeo sobre Evidencias Digitales de ENFSI. Abril.
- [17] DI-002. (2008). Normas de procedimiento de la Sección de Informática Forense de la CGPC. Diciembre.
- [18] ENFSI-BPM-FIT-01. (2015). Manual de buenas prácticas para el examen de evidencias digitales. Grupo de Trabajo Europeo de Análisis Forense Digital de ENFSI. Noviembre.
- [19] Unidad Central de Criminalística. Manual de Normas Generales. Comisaría General de Policía Científica. España.
- [20] ISO 17025. Requisitos generales para la competencia de los laboratorios de ensayo y calibración. Organización Internacional de Normalización.
- [21] ISO 17020/17025. Estándar de calidad en organismos de inspección y de competencia en laboratorios de calibración y ensayo. Organización Internacional de Normalización.
- [22] «Web de Revista Seguridad 360, "La cadena de custodia para evidencia digital"». [En línea] Disponible: <https://revistaseguridad360.com/destacados/la-cadena-de-custodia>. [Último acceso: 11 de noviembre 2024].
- [23] «Web de Ciberseguridad. "ISO/IEC 27037:2012"». [En línea] Disponible: <https://ciberseguridad.com/normativa/espana/iso-iec-27037-evidencia-digital>. [Último acceso: 16 noviembre 2024].
- [24] «Web de Security Artwork. "Análisis Forense: Cadena de Custodia de la evidencia digital"». [En línea] Disponible: <https://www.securityartwork.es/2016/02/10/analisis-forense-cadena-de-custodia-de-la-evidencia-digital>. [Último acceso: 17 noviembre 2024].
- [25] “Blockchain Technology. Beyond Bitcoin”, 16 October 2015 Berkeley, University of California. Autores: Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman.
- [26] Satoshi Nakamoto, 2009, “Bitcoin: un Sistema de dinero en efectivo electrónico peer to peer.

ANEXO I: ACRÓNIMOS UTILIZADOS

AGE: Administración General del Estado.
CA: Autoridad de Certificación
CERT: Equipo de Respuesta a Emergencias Informáticas.
CCN: Centro Criptológico Nacional.
CRLs: Repositorio de Certificados y Listas de Revocación.
ENFSI: Red Europea del Instituto de Estudio de Ciencias Forenses.
ENS: Esquema Nacional de Seguridad.
EPOC: Orden Europea de Producción.
EPOC-PR: Orden Europea de Conservación.
FCSE/FFCCSE: Fuerzas y Cuerpos de Seguridad del Estado.
GC: Guardia Civil.
GDPR: Reglamento General de Protección de Datos.
IaaS: Infraestructura Como Servicio.
IPFS: Sistema de Archivos Interplanetario.
ISO: Organización Internacional de Estandarización.
LECRIM: Ley de Enjuiciamiento Criminal.
NFT: Token no fungible.
OEDI: Observatorio Español de Delitos Informáticos.
PaaS: Plataforma Como Servicio.
PKI: Infraestructura de Clave Pública.
PN: Policía Nacional.
RA: Autoridad de Registro.
SaaS: Software Como Servicio.
SES: Secretaría de Estado de Seguridad.
STS: Sentencia del Tribunal Supremo.
TB: Terabytes.
TS: Tribunal Supremo.
VPN: Red Privada Virtual.
UE: Unión Europea.

ANEXO II: MOCKUP EVICLOUD

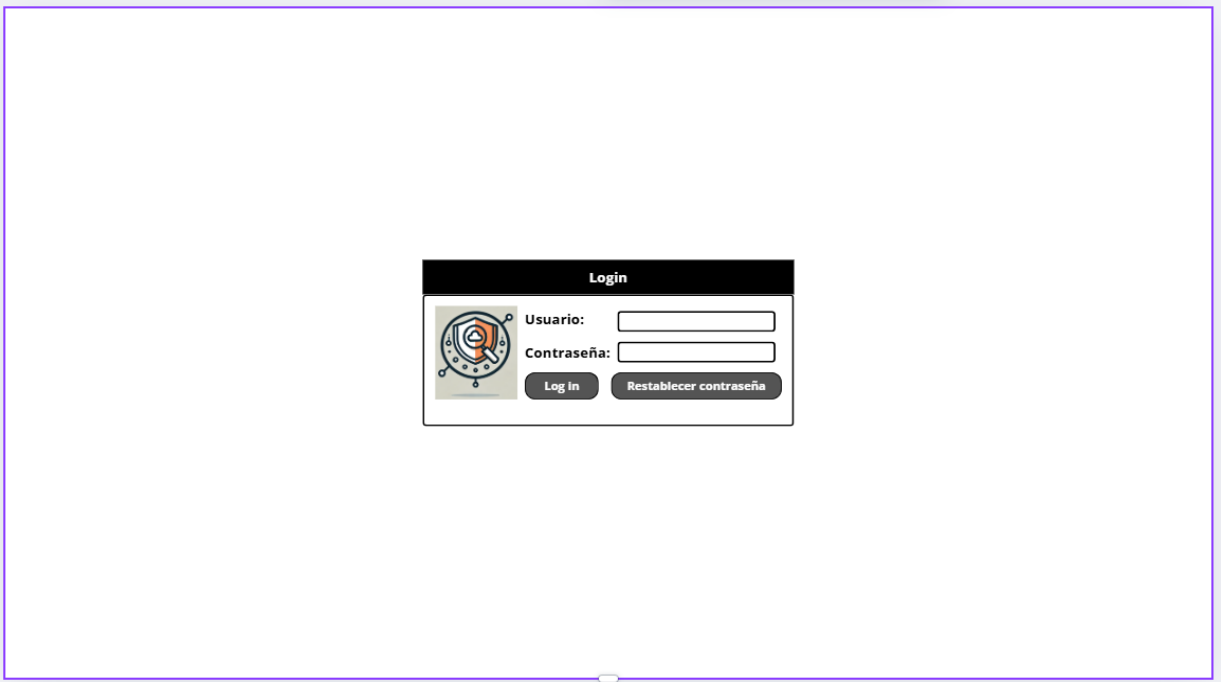


Figura A-1 Acceso a Plataforma Evicloud

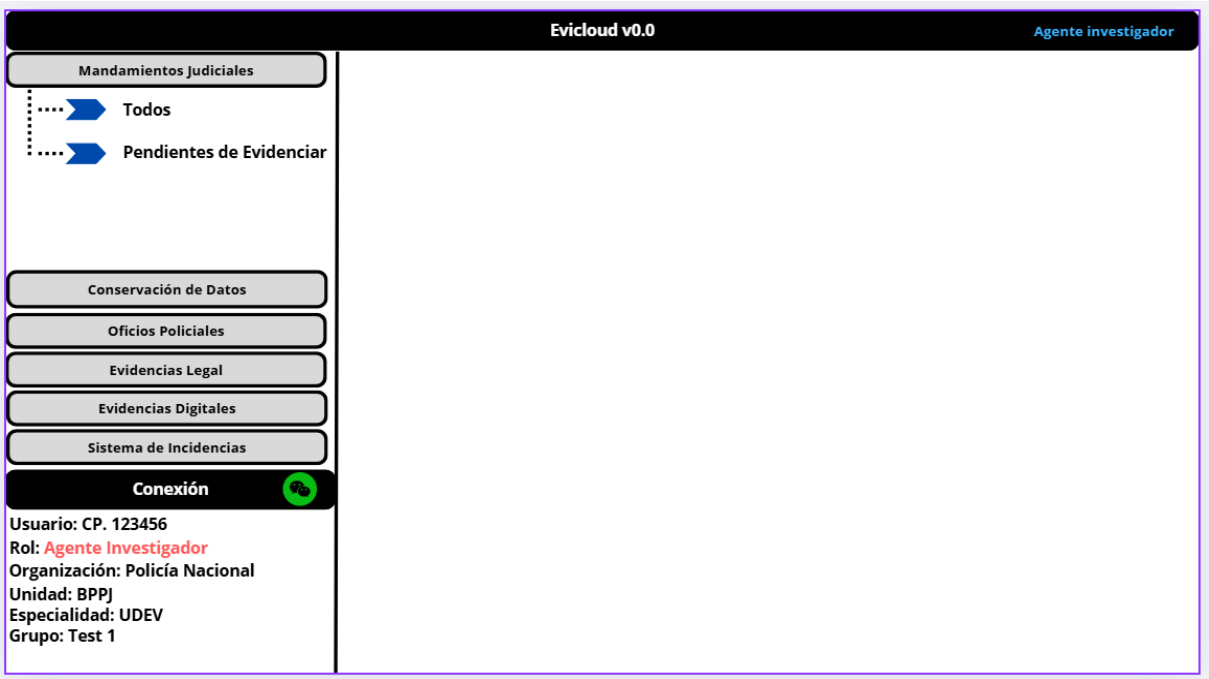


Figura A-2 Evicloud/Agente_investigador

Mandamientos Judiciales

Todos

Pendientes de Evidenciar

Conservación de Datos

Oficios Policiales

Evidencias Legal

Evidencias Digitales

Sistema de Incidencias

Conexión

Usuario: CP. 123456
Rol: **Agente Investigador**
Organización: Policía Nacional
Unidad: BPPJ
Especialidad: UDEV
Grupo: Test 1

Evicloud v0.0

Agente investigador

Código de Mandamiento	Juzgado	Tipo de procedimiento	Nº de procedimiento
GCAI6_24_0010	Audiencia Nacional	JUICIO ORDINARIO	10/2024
GCAI6_24_0010	J.I nº 1 VIGO	DIL. PREVIAS	11/2024
GCAI6_24_0010	J.I nº 8 LAS PALMAS	ASUNTO PENAL	12/2024
GCAI6_24_0010	J.I.G nº 13 MADRID	JUICIO ORDINARIO	13/2024

Figura A-3 Evicloud/Agente_investigador/Mandamientos_judiciales

Mandamientos Judiciales

Conservación de Datos

Oficios Policiales

Evidencias Legal

Evidencias Digitales

Crear Evidencia Digital

Árbol Judicial

Sistema de Incidencias

Conexión

Usuario: CP. 123456
Rol: **Agente Investigador**
Organización: Policía Nacional
Unidad: BPPJ
Especialidad: UDEV
Grupo: Test 1

Evicloud v0.0

Agente investigador

Datos del Mandamiento

Provincia:
Juzgado:
Sección:
Tipo de Procedimiento:
Grupo:
Localidad del Juzgado:
Sala:
Número de Procedimiento :
Fecha del Mandamiento:

Datos de la Evidencia Digital

Cuerpo:
Nombre del Investigado:
Tipo de Estudio:
Observaciones:
Documento ID Investigado:
Apellidos del Investigado:
Extracción:

Figura A-4 Evicloud/Agente_investigador/Evidencia_digital

Evicloud v0.0		Agente investigador
Mandamientos Judiciales Conservación de Datos Oficios Policiales Evidencias Legal Evidencias Digitales Crear Evidencia Digital Árbol Judicial Sistema de Incidencias Conexión Usuario: CP. 123456 Rol: Agente Investigador Organización: Policía Nacional Unidad: BPPJ Especialidad: UDEV Grupo: Test 1	Datos del Mandamiento Provincia: Localidad del Juzgado: Juzgado: Sala: Sección: Número de Procedimiento : Tipo de Procedimiento: Fecha del Mandamiento: Grupo: Datos de la Evidencia Digital Cuerpo: Documento ID Investigado: Nombre del Investigado: Apellidos del Investigado: Tipo de Estudio: Extracción: Observaciones: Copia Forense Evidencias Legal Clonado	

Figura A-5 Evicloud/Agente_investigador/Evidencia_digital_campo_requerido

Evicloud v0.0		Administrador del Sistema
Gestión de usuarios y roles Crear/modificar Configurar permisos Políticas de acceso Mantenimiento Seguridad Supervisión de uso Logs Sistema de Incidencias Conexión Usuario: CP.0000001 Rol: Administrador del sistema Organización: Policía Nacional Unidad: BPPJ Especialidad: UDEV Grupo: Test 1		

Figura A-6 Evicloud/Administrador_del_sistema

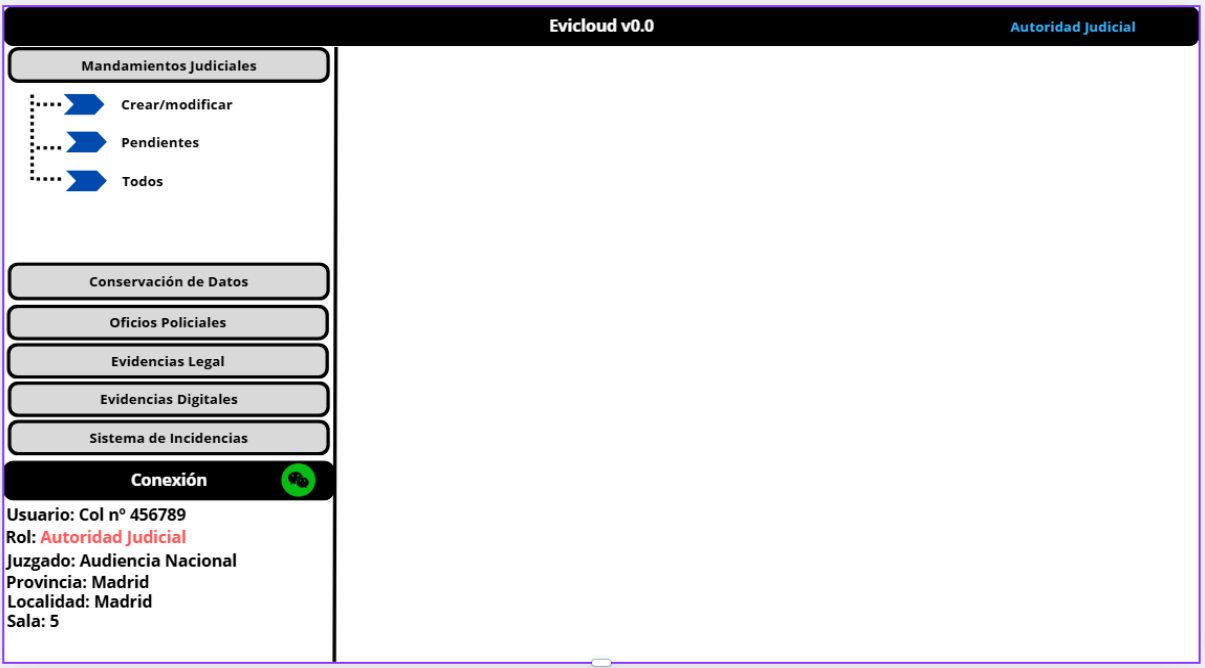


Figura A-7 Evicloud/Autoridad_judicial

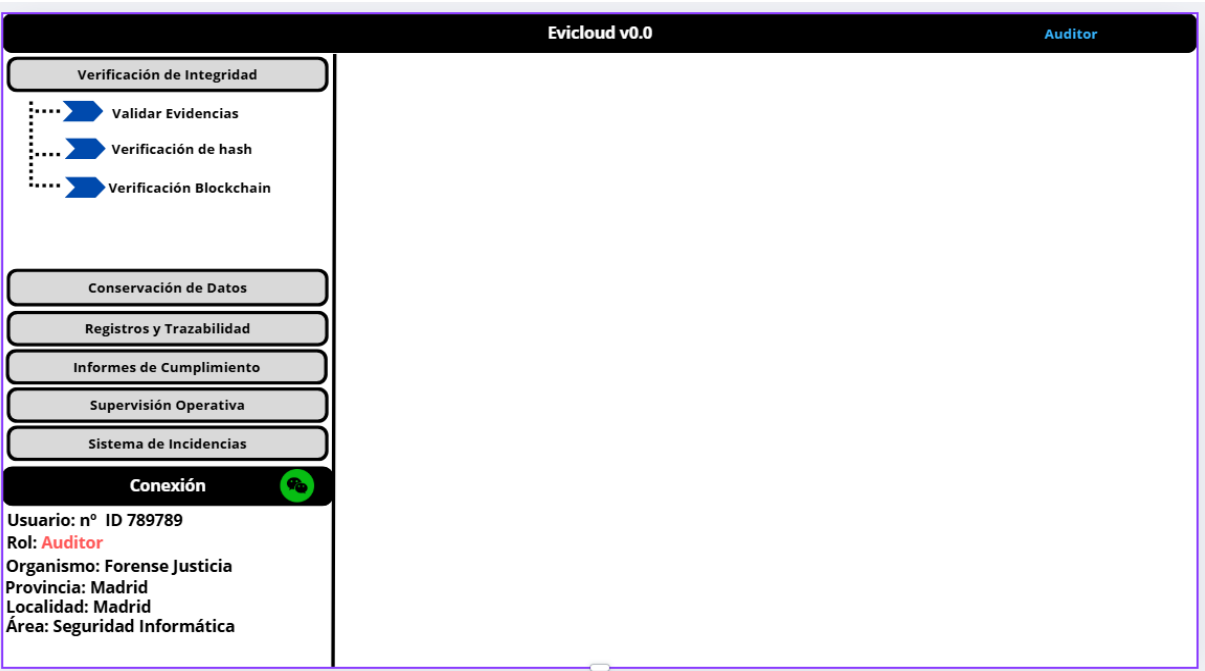


Figura A-8 Evicloud/Auditor