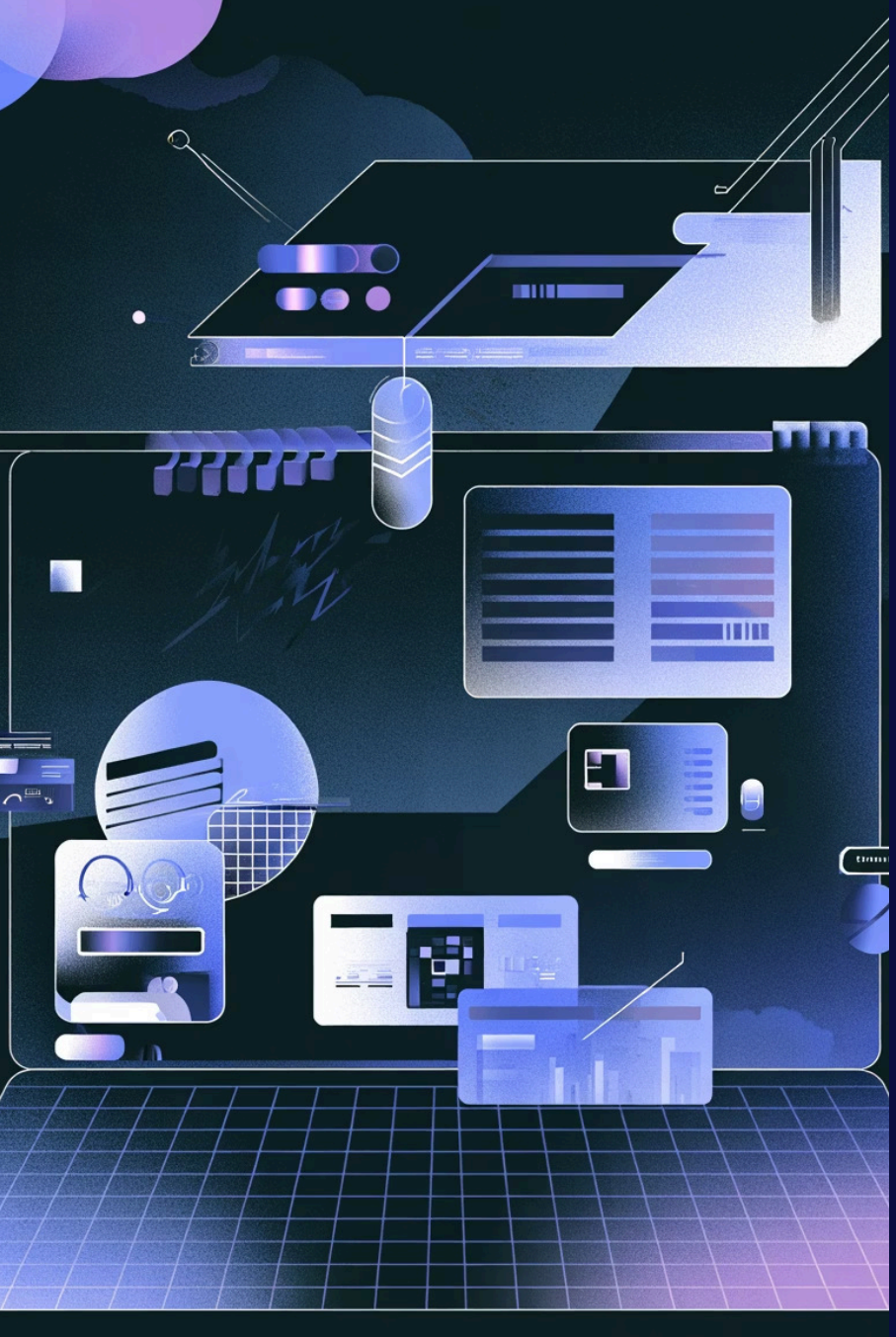


# Metodología Forense Digital Corporativa

La digitalización masiva de los últimos años ha transformado radicalmente el panorama de la seguridad empresarial. Este cambio ha traído consigo un incremento exponencial en la frecuencia y sofisticación de los incidentes de ciberseguridad, obligando a las organizaciones a fortalecer sus capacidades de respuesta y análisis forense.

Ante esta realidad, surge la necesidad imperante de contar con metodologías forenses robustas y bien estructuradas que permitan identificar, preservar y analizar evidencias digitales con rigor técnico y validez legal. Nuestro equipo forense ha desarrollado un método propio integral que garantiza la integridad de la información, cumple con los requisitos legales vigentes y optimiza la eficiencia operativa en todas las fases del proceso investigativo.

# Objetivos Estratégicos del Proyecto

### Investigación normativa

Análisis exhaustivo de los principales estándares y normas forenses reconocidos a nivel internacional, evaluando su aplicabilidad y robustez técnica.

### Selección estratégica

Comparativa detallada de marcos normativos para identificar aquellos más adecuados al entorno empresarial y contexto legal español.

### Diseño metodológico

Desarrollo de una metodología propia integral, adaptable y escalable que integre las mejores prácticas internacionales.

### Documentación técnica

Elaboración de un resumen esquemático y operativo que facilite la aplicación práctica de la metodología en escenarios reales de investigación.

### Presentación ejecutiva

Comunicación clara y profesional de los resultados ante dirección, equipos de auditoría y organismos de cumplimiento normativo.

# Marco Normativo Internacional

La investigación se centró en los marcos de referencia más relevantes y reconocidos internacionalmente en el ámbito de la informática forense y la gestión de evidencias digitales:

### ISO/IEC 27037

Proporciona directrices detalladas para la identificación, recolección, adquisición y preservación de evidencia digital, estableciendo los fundamentos para mantener la integridad desde el primer contacto.

### ISO/IEC 27042

Define criterios específicos para el análisis e interpretación de evidencias, asegurando que los métodos aplicados sean reproducibles y científicamente válidos.

### ISO/IEC 27043

Presenta un modelo completo de investigación de incidentes que abarca desde la preparación inicial hasta la presentación final de conclusiones.

### NIST SP 800-86

Guía práctica para la integración de capacidades forenses dentro de los procesos de respuesta a incidentes de seguridad de la información.

### NIST SP 800-101 Rev.1

Metodología especializada en forense de dispositivos móviles, considerando las particularidades técnicas de smartphones y tablets.

### UNE 71506:2013

Estándar español que adapta las mejores prácticas internacionales al marco legal y procedimientos judiciales nacionales.

- **CFTT/DFRWS:** Iniciativas enfocadas en la validación técnica rigurosa de herramientas forenses, garantizando su confiabilidad y precisión en entornos de producción.

# Análisis Comparativo de Marcos Normativos

### Familia ISO/IEC

Ofrece una estructura formal y sistemática que prioriza la trazabilidad completa, reproducibilidad metodológica y validez jurídica de todos los procedimientos. Ideal para entornos donde la admisibilidad legal es crítica.

### Guías NIST

Enfoque eminentemente operativo y práctico, orientado a la respuesta inmediata ante incidentes. Proporciona procedimientos detallados y técnicamente probados en escenarios reales de ciberseguridad.

### Norma UNE 71506:2013

Perfecta alineación con la legislación procesal española y los procedimientos judiciales nacionales. Facilita la integración con requisitos legales específicos del ordenamiento jurídico español.

## Conclusión estratégica

No existe un estándar único que cubra todas las necesidades operativas, legales y técnicas. La solución óptima requiere desarrollar un **modelo híbrido** que integre las fortalezas complementarias de cada marco normativo.

DFRWS y CFTT complementan el enfoque mediante la evaluación rigurosa de la confiabilidad técnica de las herramientas forenses empleadas, proporcionando validación científica adicional.

# Integración Estratégica de Estándares

La metodología forense desarrollada se fundamenta en una integración estratégica y complementaria de los marcos normativos más robustos, combinando sus fortalezas para crear un modelo híbrido superior:

### ISO/IEC 27037–27043

Marco estructural internacional que proporciona la base metodológica formal, garantizando trazabilidad, reproducibilidad y reconocimiento global de los procedimientos aplicados.

### NIST SP 800-86 / 800-101

Guía operativa y técnica que aporta procedimientos específicos, técnicas probadas y mejores prácticas para la ejecución práctica de actividades forenses en diversos escenarios.

### UNE 71506:2013

Referencia legal y documental nacional que asegura el cumplimiento de requisitos procesales españoles y facilita la admisibilidad de evidencias ante tribunales.

Esta combinación estratégica asegura simultáneamente tres pilares fundamentales: **admisibilidad legal** en procedimientos judiciales, **consistencia técnica** en la ejecución de análisis forenses, y **flexibilidad práctica** para adaptarse a diferentes tipos de incidentes y contextos organizacionales.

# Metodología Forense: Visión General

Hemos desarrollado una metodología integral y sistemática estructurada en **siete fases secuenciales** que cubren el ciclo completo de una investigación forense digital, desde la preparación inicial hasta la presentación formal de resultados:

### Fase 0: Preparación

Planificación estratégica y preparación del entorno forense.

### Fase 1: Identificación

Identificación de sistemas afectados y recolección preliminar de información relevante.

### Fase 2: Adquisición

Obtención de copias forenses exactas de las evidencias digitales.

### Fase 3: Preservación

Almacenamiento seguro y mantenimiento de la integridad de evidencias.

### Fase 4: Análisis

Examen técnico detallado y extracción de información relevante.

### Fase 5: Documentación

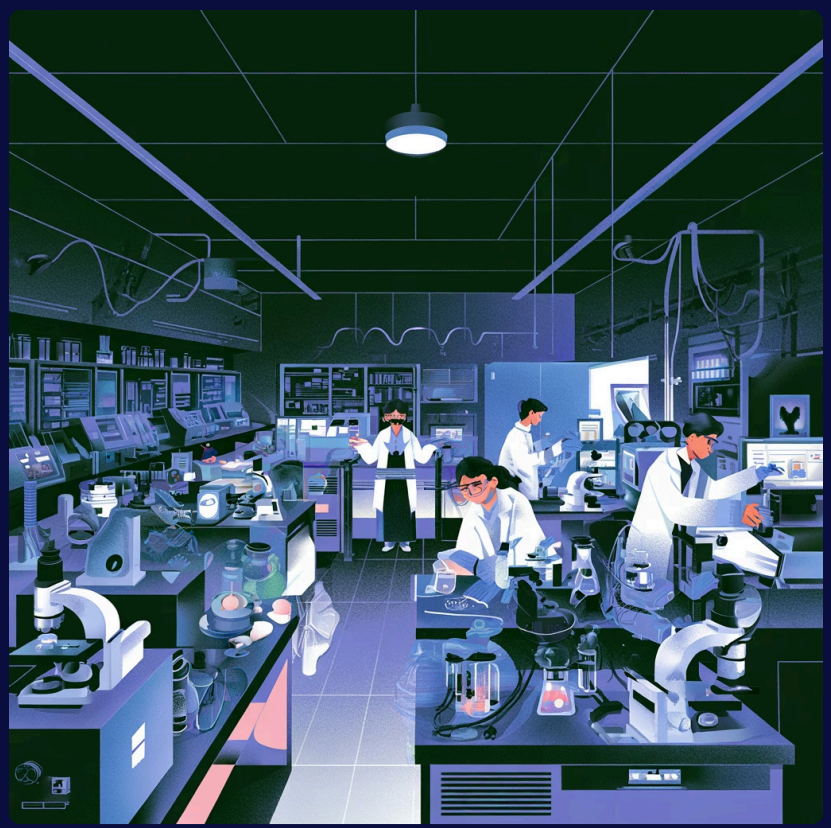
Elaboración de informes técnicos y ejecutivos completos.

### Fase 6: Presentación

Comunicación formal de hallazgos, conclusiones y recomendaciones.

Cada fase incluye **controles de calidad específicos**, puntos de verificación de integridad y requisitos de documentación que garantizan la trazabilidad completa del proceso investigativo.

# Fase 0: Preparación y Planificación



## Objetivo estratégico

Garantizar un entorno controlado y certificado que permita la trazabilidad absoluta de todas las actuaciones forenses, minimizando riesgos de contaminación o alteración de evidencias.

**1**

### Definición de roles y responsabilidades

Asignación formal de funciones especializadas: Responsable Forense (dirección técnica), Analista (ejecución de análisis), Custodio (gestión de evidencias y cadena de custodia).

**2**

### Validación de herramientas forenses

Verificación y certificación de todas las herramientas de software y hardware conforme a estándares CFTT, incluyendo pruebas de precisión, reproducibilidad y ausencia de alteración.

**3**

### Preparación documental

Elaboración y revisión de formularios estandarizados de cadena de custodia, bitácoras de actuaciones, plantillas de informes y listas de verificación operativas.

**4**

### Acondicionamiento del entorno

Configuración de laboratorio forense con aislamiento de red, control de accesos físicos y lógicos, sistemas de monitorización ambiental y respaldo energético.

# Fase 1: Identificación y Recolección Preliminar

## Objetivo operativo

Determinar con precisión los sistemas, dispositivos y fuentes de información afectados por el incidente, estableciendo prioridades de actuación basadas en la volatilidad y relevancia de los datos.

### Identificación de activos digitales

Inventario completo de dispositivos involucrados (servidores, estaciones de trabajo, dispositivos móviles), usuarios implicados, servicios afectados y rutas de red relevantes.

### Documentación del estado inicial

Registro fotográfico y descriptivo detallado del estado de los sistemas en el momento del descubrimiento, incluyendo pantallas activas, conexiones físicas y configuraciones visibles.

### Priorización de datos volátiles

Recolección urgente de información temporal: contenido de memoria RAM, procesos en ejecución, conexiones de red activas, sesiones abiertas y datos en caché que se perderían con el apagado.

### Registro cronológico de actuaciones

Documentación precisa de cada acción realizada con hora exacta (sincronizada con fuente confiable), fecha, descripción de la actividad y firma del responsable ejecutor.

# Fase 2: Adquisición de Evidencia Digital

## Objetivo técnico

Obtener **copias forenses exactas y verificables** de las evidencias digitales sin alterar, modificar o comprometer el contenido original en ningún momento del proceso.

01

### Creación de imágenes forenses

Generación de copias bit a bit utilizando herramientas validadas: FTK Imager, dd/dcfldd, o Guymager. Incluye metadatos completos del proceso.

02

### Verificación criptográfica

Cálculo y registro de hashes SHA-256 (y opcionalmente MD5) antes y después de la adquisición para garantizar integridad absoluta.

03

### Adquisición de dispositivos móviles

Extracción especializada según NIST SP 800-101: aislamiento de señal, métodos lógicos o físicos según disponibilidad, preservación de datos de aplicaciones.

04

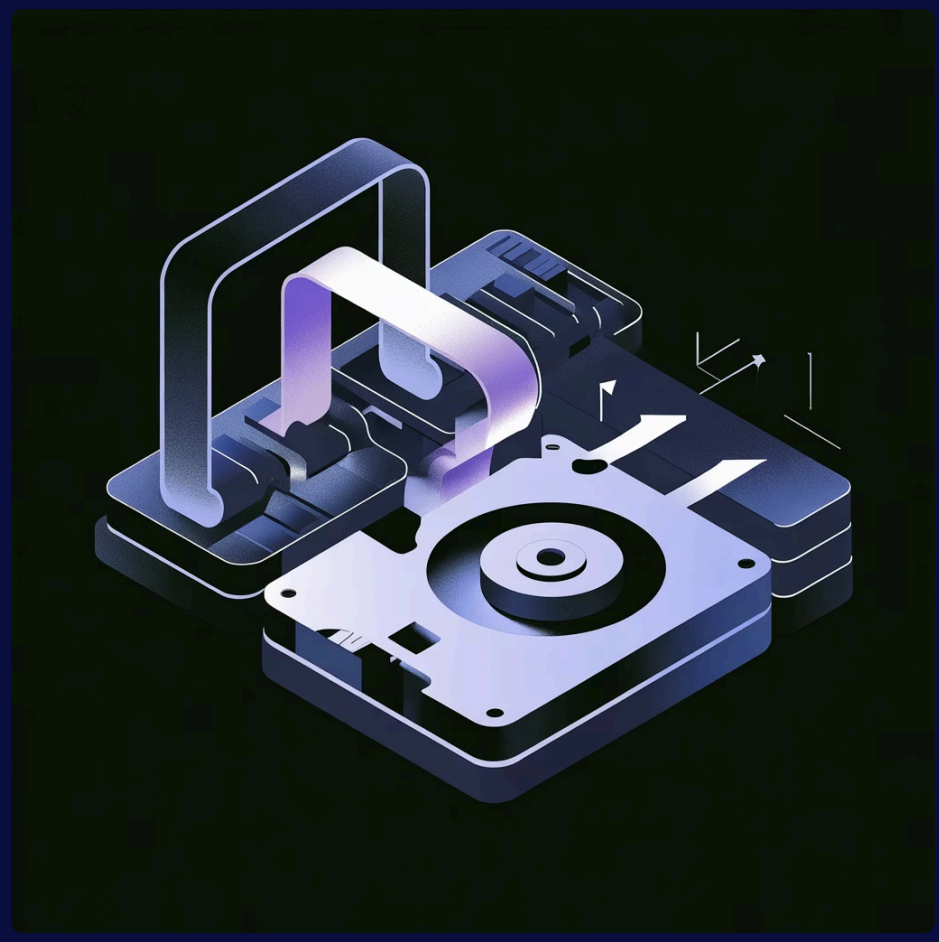
### Documentación técnica completa

Registro de versiones de software empleado, parámetros específicos de adquisición, operador responsable y observaciones relevantes.

05

### Formalización de cadena de custodia

Cumplimentación exhaustiva del formulario de custodia con firmas digitales, sellado lógico mediante hash y opcionalmente sellado físico con precintos numerados.



> **Principio fundamental:** La evidencia original nunca debe ser modificada. Todo análisis se realiza sobre copias de trabajo, manteniendo el original en estado prístino.

# Fase 3: Preservación y Almacenamiento

## Objetivo de integridad

Mantener y demostrar la integridad inmutable de las evidencias digitales durante todo el ciclo de vida de la investigación, desde la adquisición hasta la presentación final o archivo permanente.

### Almacenamiento protegido

Conservación en medios de solo lectura (write-blockers hardware) o con protección criptográfica. Ubicación en entorno con control ambiental, acceso restringido y registro automatizado.

### Trazabilidad completa de accesos

Registro detallado y firmado de cada acceso, consulta, movimiento o manipulación de las evidencias, incluyendo: quién, cuándo, por qué, qué acciones y resultados obtenidos.

### Segregación de copias

Separación estricta entre copia original maestra (intocable, solo para verificación) y copias de trabajo (para análisis activo). Etiquetado claro y distintivo de cada tipo.

### Verificación periódica de integridad

Re-cálculo programado de valores hash para confirmar que las evidencias no han sufrido degradación, corrupción o alteración involuntaria durante el almacenamiento prolongado.

**Cumplimiento normativo:** Todos los procedimientos de preservación están alineados con ISO/IEC 27037 y UNE 71506:2013, garantizando admisibilidad judicial y conformidad con requisitos de auditoría.