Gestión y análisis de evidencias digitales para investigadores, analistas y peritos

Guía docente de la edición de enero de 2027

Inicio · 15 de enero de 2027
Coordinación y docencia · Alejandro Maestre
Modalidad · Online asíncrona en castellano
Dedicación orientativa · 12 horas
Matrícula · 250 € general. Gratuita para miembros de la AEICF.

Presentación

Este curso ofrece una introducción estructurada a la gestión de evidencias digitales desde una perspectiva jurídica, técnica y operativa. Su planteamiento parte de un problema central: en el entorno digital no basta con disponer de un dato, un archivo o una captura; es necesario poder defender su origen, su integridad, su contexto y la corrección del proceso seguido hasta su incorporación en un informe o procedimiento.

La propuesta formativa se organiza en tres partes complementarias. La primera estudia la problemática de la evidencia digital y los errores más frecuentes en su valoración. La segunda traduce ese problema a un marco metodológico concreto mediante UNE-EN ISO/IEC 27037. La tercera lleva ese marco a una ejecución trazable dentro de Probatia, conectando caso, actuación, evidencia, informe y certificación.

Destinatarios y conocimientos previos

Peritos informáticos, investigadores, analistas de seguridad, profesionales jurídicos y responsables de cumplimiento que deban documentar o revisar evidencias digitales. Se recomienda familiaridad básica con la gestión documental o la actuación pericial. El nivel es introductorio profesional.

Itinerario

1. Problemática de la evidencia digital
2. La norma UNE-EN ISO/IEC 27037
3. Implementación operativa con PROBATIA (material docente en preparación).

Finalidad, objetivos y competencias

La finalidad del curso es que el alumnado comprenda por qué la evidencia digital presenta riesgos específicos de admisibilidad, fiabilidad y trazabilidad, y que sea capaz de aplicar un flujo de trabajo defendible desde la identificación de la evidencia hasta su integración final en un informe y, en su caso, en un proceso de certificación.

Objetivo general

Capacitar al alumnado para analizar, documentar y gestionar evidencias digitales con un criterio metodológico consistente, alineado con UNE-EN ISO/IEC 27037 y materializado en un flujo operativo completo dentro de Probatia.

Objetivos específicos

- Diferenciar evidencia digital, prueba digital, soporte electrónico y documento electrónico.
- Identificar los riesgos jurídicos y técnicos que debilitan la fuerza probatoria de una evidencia.
- Comprender el alcance, los límites y la utilidad práctica de UNE-EN ISO/IEC 27037.
- Aplicar criterios de relevancia, fiabilidad, suficiencia, auditabilidad, justificabilidad y reproducibilidad.
- Tomar decisiones básicas de identificación, recogida, adquisición y preservación con documentación suficiente.
- Ejecutar en Probatia un flujo coherente de caso, actuaciones, operaciones, unidades, evidencias, informe y certificación.
- Revisar la trazabilidad y la calidad documental de un expediente digital antes de su cierre.

Resultados de aprendizaje

- Explicar por qué la evidencia digital es intangible, replicable, volátil, contextual y potencialmente manipulable.
- Valorar críticamente capturas, impresiones, exportaciones y otras representaciones parciales de datos digitales.
- Reconocer los principales focos de ilicitud o debilidad probatoria en actuaciones sobre evidencia digital.
- Aplicar el vocabulario operativo esencial de ISO/IEC 27037 y distinguir roles como DEFR y DES.
- Justificar decisiones de recogida o adquisición en función del riesgo de pérdida, la volatilidad y la relevancia del material.
- Documentar una cadena de custodia básica y describir qué información mínima debe quedar registrada.
- Operar con criterio en Probatia para registrar contexto, asociar evidencias, generar el informe y cerrar la certificación conforme al flujo de la plataforma.

Metodología y actividades

Progresión del aprendizaje

La metodología del curso sigue una progresión deliberada de lo conceptual a lo operativo:

1. Comprender el problema.
2. Interiorizar el estándar metodológico.
3. Aplicarlo en una herramienta real de trabajo.

Este orden evita un error frecuente en la formación sobre evidencia digital: aprender funciones de plataforma o técnicas aisladas sin haber fijado antes el criterio jurídico-técnico que da sentido a cada decisión.

Principios metodológicos

• Aprendizaje secuencial: cada módulo prepara el siguiente.

• Integración de Derecho, técnica y operativa: no se tratan como planos aislados.

• Orientación a decisiones: el curso no se limita a definiciones, sino que entrena criterios de actuación.

• Trazabilidad documental: se insiste de forma transversal en quién hizo qué, cuándo, sobre qué y por qué.

• Transferencia a la práctica: el cierre del curso exige reproducir un flujo completo en Probatia.

Actividades de aprendizaje

Las actividades del curso se articulan en cuatro niveles:

• Lectura o visualización de los materiales base de cada módulo.

• Resolución de test de autoevaluación en los módulos 1 y 2.

• Ejecución de un caso práctico guiado en el módulo 3.

• Relectura final de los criterios de calidad documental y trazabilidad.

Actividades observables esperadas:

• Analizar una situación probatoria y detectar puntos de fallo.

• Justificar por escrito una decisión de recogida o adquisición.

• Completar notas de actuación u operación con la información mínima requerida.

• Clasificar evidencias y vincularlas a su contexto.

• Revisar eventos de trazabilidad y comprobar coherencia documental.

• Generar un informe final y completar correctamente el cierre de certificación.

Tema 1. Problemática de la evidencia digital

Finalidad del módulo

fijar el mapa de riesgos que explica por qué la evidencia digital requiere un tratamiento probatorio reforzado.

Programa

- Distinción entre evidencia digital y prueba digital.
- Condiciones acumulativas para pasar de dato a prueba defendible.
- Intangibilidad y visualización mediata.
- Replicabilidad, copia bit a bit, hash e integridad.
- Volatilidad, borrado, alteración y dependencia contextual.
- Función estructural de la pericial informática.
- Valor de capturas, impresiones, transcripciones y exportaciones.
- Prueba ilícita en entorno digital y derechos especialmente comprometidos.
- Cadena de custodia digital: función, requisitos y matices procesales.
- Asimetría de recursos, dimensión transnacional y errores recurrentes de valoración judicial.
- Escenarios aplicados: mensajería instantánea, correo electrónico y custodia incompleta de dispositivos.

Clases y materiales del aula

«Del dato a la prueba» (45 min 48 s) y «Acreditar la evidencia» (45 min 34 s). Apuntes de 48 páginas. Las dos clases incluyen subtítulos y transcripción. El tema dispone de una autoevaluación con un banco de 100 preguntas. En cada intento se sortean 20 preguntas y se mezcla el orden de las opciones.

Tema 2. La norma UNE-EN ISO/IEC 27037

Finalidad del módulo

traducir los riesgos del módulo 1 a un marco operativo y documentable de trabajo sobre potencial evidencia digital.

Programa

- Alcance, propósito y límites de la norma.
- Terminología esencial: evidencia digital, soporte, adquisición, preservación, imaging.
- Roles operativos y competencia: DEFR y DES.
- Principios rectores: relevancia, fiabilidad y suficiencia.
- Requisitos del proceso: auditabilidad, justificabilidad, repetibilidad y reproducibilidad.
- Reglas fundamentales de manejo del original.
- Procesos de identificación, recogida, adquisición y preservación.
- Documentación mínima, cadena de custodia, briefing y evaluación de riesgos.
- Priorización por volatilidad y riesgo de pérdida.
- Casos específicos: ordenadores encendidos o apagados, dispositivos en red y sistemas CCTV.
- Anexo A y Anexo B como apoyo a competencias y transferencias documentales.

Clases y materiales del aula

«La norma y su método» (51 min 06 s) y «Aplicación y garantías» (46 min 24 s). Apuntes de 58 páginas. Las dos clases incluyen subtítulos y transcripción. El tema dispone de una autoevaluación con un banco de 100 preguntas. En cada intento se sortean 20 preguntas y se mezcla el orden de las opciones.

Tema 3. Implementación operativa con PROBATIA

Finalidad del módulo

aplicar el criterio de los módulos anteriores dentro de un flujo real de gestión de evidencias con trazabilidad.

Programa

- Mapa funcional de Probatia y correspondencia con el flujo metodológico.
- Principios de uso, objetivos y ventajas, con sus condiciones y límites.
- Casos como contenedor principal del contexto probatorio.
- Actuaciones y operaciones: creación, relación y documentación mínima.
- Dispositivos, unidades de intervención y unidades de registro.
- Alta de evidencias, tipologías, valor probatorio y derivados.
- Metadatos, geolocalización y control de calidad previo al informe.
- Trazabilidad y auditoría de eventos.
- Selección de evidencias e inclusión en informe PDF.
- Regla operativa de certificación: solo sobre pruebas incluidas en informe.
- Contactos, cuenta, gobernanza mínima y criterios de uso consistente.
- Caso integrado final de principio a fin.
- Metodología de captura de páginas y eventos web con PROBATIA (apartado propio).

Estado del material

Este tema forma parte del programa previsto. Las prácticas y el caso integrado están en desarrollo. El aula tiene preparados los materiales de los dos primeros temas.

Evaluación y orientaciones docentes

Enfoque de evaluación

Se recomienda una evaluación continua, criterial y orientada al desempeño. El curso no debe medirse solo por memorización terminológica, sino por la capacidad de tomar decisiones justificables y de documentarlas de forma defendible.

Instrumentos previstos

- Test de autoevaluación del módulo 1.
- Test de autoevaluación del módulo 2.
- Test y caso práctico guiado del módulo 3.
- Checklist de aceptación del caso final.
- Rúbrica rápida de autoevaluación del cierre práctico.

Criterios recomendados de superación

- Comprender la diferencia entre dato, evidencia y prueba.
- Identificar riesgos jurídicos y técnicos sin confundir apariencia con autenticidad.
- Aplicar correctamente la lógica de ISO/IEC 27037 a decisiones básicas de trabajo.
- Completar el caso final con contexto, vínculos, trazabilidad e informe coherentes.
- Respetar la regla de certificación sobre evidencias incluidas en informe.

Calificación de la autoevaluación

Cada respuesta correcta suma 0,5 puntos, cada incorrecta resta 0,5 y las preguntas en blanco valen 0. Para aprobar cada test hay que obtener al menos 5 puntos sobre 10. Por ejemplo, 15 aciertos y 5 errores dan una nota de 5. El caso práctico del tercer tema continúa en preparación.

Orientaciones para la impartición

- Empezar siempre por el problema probatorio y no por la herramienta.
- Evitar presentar ISO 27037 como una lista cerrada de técnicas; debe explicarse como un marco de decisiones justificables.
- No separar el uso de Probatia de la cadena de custodia, del informe y del criterio de inclusión de evidencias.
- Utilizar los escenarios y solucionarios comentados como espacios de debate, no solo como corrección mecánica.
- Exigir narrativa documental clara: una evidencia bien cargada pero mal contextualizada sigue siendo débil.
- Reforzar la idea de que el valor probatorio depende tanto del contenido como del proceso seguido.

Recursos y bibliografía

Recorrido de estudio

Los temas 1 y 2 reúnen cuatro clases, 106 páginas de apuntes y dos autoevaluaciones con 100 preguntas en el banco de cada tema. Para cada tema, sigue las clases en orden, consulta el desarrollo en los apuntes y contrasta tus decisiones en las autoevaluaciones. Puedes volver a un pasaje concreto mediante los subtítulos y la transcripción.

Referencias recomendadas en la guía docente

- UNE-EN ISO/IEC 27037.
- Galindo, Problemática jurídica de la prueba digital y sus implicaciones.
- Rodríguez-Magarinos, Incorporación al proceso del material informático.
- López Rivera, Peritaje informático y tecnológico.

Ámbitos de consulta

- problemática jurídica de la prueba digital,
- diferencia entre soporte, documento, evidencia y prueba,
- metadatos, integridad y autenticidad,
- estructura y límites del informe pericial,
- criterios operativos de identificación, recogida, adquisición y preservación.

Alcance de la formación

Este curso tiene una finalidad formativa y metodológica. No sustituye el asesoramiento jurídico aplicable a un caso concreto ni agota las exigencias procesales o técnicas de cada jurisdicción. Su valor reside en ofrecer un itinerario coherente para pensar, documentar y ejecutar mejor el trabajo con evidencias digitales.

Ficha de la convocatoria

Consultar la ficha del curso en imagencientifica.es