Revista Iberoamericana de Derecho, Cultura y Ambiente

Edición Nº 9 – Julio de 2026

Capítulo de Derecho Penal y Criminología

www.aidca.org/revista

MÁS ALLÁ DEL HASH: CADENA DE CUSTODIA DIGITAL Y VALIDEZ PROBATORIA

Por Maite Muiña Ruiz[1]

RESUMEN

La progresiva digitalización de la sociedad ha transformado de forma profunda el sistema probatorio, situando a la evidencia digital en el centro del proceso judicial contemporáneo. La generalización del uso de dispositivos electrónicos, especialmente teléfonos inteligentes, así como la expansión de

[1] Profesora del Grado de Criminología y Ciencias Forenses, Universidad Nebrija. Personal investigador, Universidad Complutense de Madrid. ORCID: https://orcid.org/0009-0005-5224-5530 Correo: maitemuina@gmail.com Maite Muiña Ruiz es doctoranda en Medicina Legal y Criminalística por la Universidad Complutense de Madrid. Profesora universitaria en el ámbito de la Criminología y Ciencias Forenses, desarrolla su actividad docente en instituciones como la Universidad Nebrija, la Universidad Complutense de Madrid y la Universidad Internacional de Valencia. Perito judicial, criminóloga, victimóloga y detective privado, cuenta con una sólida trayectoria en el ámbito de la informática forense, la investigación criminal y la cadena de custodia de la evidencia digital. Es investigadora en diversas líneas vinculadas a la seguridad, la inteligencia y la criminología aplicada, así como directora académica del Instituto Internacional de Victimología INDUPROVIC. Ha participado en congresos y actividades internacionales en materia de criminalística, prueba digital y análisis forense, y es autora de publicaciones especializadas en revistas jurídicas y científicas.

servicios en la nube y plataformas digitales, ha convertido a la prueba electrónica en un elemento determinante para la reconstrucción de hechos con relevancia jurídico-penal. Sin embargo, esta centralidad viene acompañada de una problemática técnica y jurídica de especial complejidad, derivada de la naturaleza mutable, volátil y altamente dependiente del entorno tecnológico de la evidencia digital.

En este contexto, la cadena de custodia adquiere una relevancia estructural como mecanismo de garantía de la autenticidad, integridad y trazabilidad de la prueba, permitiendo asegurar su validez en sede judicial (González Reyes, 2021; International Organization for Standardization [ISO], 2012). No obstante, en la práctica forense contemporánea se observa una tendencia reduccionista que identifica erróneamente la integridad probatoria con la existencia de un valor hash coincidente. Este trabajo parte de la premisa de que dicha concepción resulta insuficiente desde una perspectiva técnico-jurídica.

A través de un análisis sistemático de la cadena de custodia digital, sus fases técnicas, metodologías de adquisición y estándares normativos, se sostiene que la validez de la prueba digital no puede fundamentarse exclusivamente en la verificación criptográfica, sino que requiere un modelo integral que combine procedimiento, documentación y control metodológico. En definitiva, se propone una evolución conceptual desde la cadena de custodia tradicional hacia una verdadera cadena de valor probatorio.

1. INTRODUCCIÓN

La transformación tecnológica de las últimas décadas ha redefinido la naturaleza de la prueba en el proceso judicial. En el contexto actual, una parte significativa de las actividades humanas deja rastro en entornos digitales, generando información susceptible de ser utilizada como medio probatorio. Desde conversaciones mantenidas en aplicaciones de mensajería instantánea hasta registros de actividad en sistemas informáticos, pasando por datos de geolocalización o contenidos almacenados en dispositivos electrónicos, la

evidencia digital se ha consolidado como un elemento esencial en la investigación de hechos jurídicamente relevantes (González Reyes, 2021).

Este cambio no es meramente cuantitativo, en el sentido de que existan más datos disponibles, sino cualitativo, en la medida en que la propia configuración de la prueba ha mutado. A diferencia de la evidencia física tradicional, la evidencia digital no constituye un objeto tangible e inmutable, sino que se presenta como información dependiente de sistemas tecnológicos complejos, susceptible de modificación sin dejar rastros perceptibles y, en muchos casos, sometida a procesos automáticos de actualización, sincronización o sobreescritura (ISO, 2012).

Esta particularidad introduce una tensión fundamental en el ámbito probatorio: la necesidad de garantizar que el material presentado ante el tribunal conserva su autenticidad e integridad, a pesar de su naturaleza inherentemente inestable. En este sentido, la cadena de custodia se configura como el instrumento que permite salvar dicha tensión, proporcionando un marco de control sobre el tratamiento de la evidencia desde su obtención hasta su incorporación al proceso.

Sin embargo, la creciente tecnificación de la prueba ha generado también simplificaciones conceptuales peligrosas. En particular, en la práctica forense se ha extendido la idea de que la coincidencia de valores hash es suficiente para acreditar la integridad de la evidencia digital. Este planteamiento, si bien parte de una herramienta técnicamente válida, resulta incompleto desde el punto de vista jurídico. El hash verifica un estado de la información, pero no permite reconstruir el camino recorrido por dicha información ni las condiciones en las que fue obtenida y tratada.

Por ello, el presente trabajo se orienta a demostrar que la cadena de custodia digital debe ser entendida como un proceso complejo y multidimensional, en el que confluyen elementos técnicos, metodológicos y jurídicos. Su finalidad no es únicamente preservar el dato, sino garantizar la fiabilidad del procedimiento en su conjunto.

2. LA CADENA DE CUSTODIA COMO GARANTÍA ESTRUCTURAL DE LA PRUEBA DIGITAL

La cadena de custodia constituye uno de los pilares fundamentales sobre los que se asienta la validez de la prueba digital en el proceso judicial. Lejos de tratarse de un mero requisito formal o de una sucesión de actuaciones administrativas, debe entenderse como una verdadera **estructura de garantía**, orientada a asegurar que la evidencia presentada conserva su autenticidad, integridad y trazabilidad desde su obtención hasta su valoración judicial *(González Reyes, 2021)*.

Desde una perspectiva clásica, la cadena de custodia se ha definido como el conjunto de actuaciones documentadas que permiten identificar a las personas que han tenido contacto con la evidencia, así como las circunstancias temporales y materiales en las que se ha producido su manipulación. No obstante, en el ámbito digital esta concepción resulta insuficiente, en tanto que la naturaleza de la evidencia electrónica exige incorporar al análisis no solo el «quién» y el «cuándo», sino también el **«cómo» y el «con qué»** se ha intervenido sobre el soporte digital *(ISO, 2012)*.

En consecuencia, una cadena de custodia digital adecuada debe incluir, al menos, la siguiente información:

-identificación precisa del dispositivo o sistema intervenido
-estado del mismo en el momento de su localización
-condiciones en las que se produce la incautación o adquisición
-medidas de aislamiento adoptadas
-técnicas empleadas para la obtención de la evidencia
-herramientas utilizadas
-operadores que intervienen en cada fase
-registros temporales de cada actuación
-condiciones de almacenamiento y acceso posterior

(ISO, 2012; Contreras Calderón, 2022)

La ausencia o defectuosa documentación de cualquiera de estos elementos no constituye una simple irregularidad formal, sino que puede afectar directamente a la **fiabilidad probatoria del material obtenido**, en la medida en que impide reconstruir el proceso de tratamiento de la evidencia y, por tanto, someterlo a contradicción en sede judicial *(Requejo Passoni, 2025)*.

En este sentido, la cadena de custodia cumple una doble función. Por un lado, opera como mecanismo de **control técnico**, en cuanto permite verificar que no se han producido alteraciones indebidas en la evidencia. Por otro, actúa como instrumento de **garantía procesal**, asegurando que la prueba puede ser impugnada, analizada y debatida por las partes en condiciones de igualdad. Esta dimensión dual la convierte en un elemento esencial del derecho de defensa.

3. PARTICULARIDADES TÉCNICAS DE LA EVIDENCIA DIGITAL

La comprensión adecuada de la cadena de custodia en el ámbito digital exige, necesariamente, atender a las características específicas de la evidencia electrónica. A diferencia de la prueba física tradicional, la evidencia digital no posee una materialidad estable, sino que se construye sobre estructuras lógicas altamente dependientes del funcionamiento del sistema tecnológico en el que se integra *(ISO, 2012)*.

En primer lugar, la evidencia digital se caracteriza por su **mutabilidad**. Cualquier interacción con el dispositivo —incluso aquellas que forman parte de su uso ordinario— puede generar modificaciones en los datos almacenados. Entre estas modificaciones se incluyen cambios en metadatos, registros de acceso, marcas temporales o estructuras internas del sistema de archivos. Esta circunstancia implica que la mera manipulación del dispositivo, incluso con fines aparentemente inocuos, puede alterar la evidencia sin dejar rastros perceptibles a simple vista.

En segundo lugar, la evidencia digital presenta un alto grado de **volatilidad**. Determinados datos, como los contenidos en memoria RAM o registros temporales del sistema, desaparecen automáticamente al apagar el dispositivo o

al reiniciar un proceso. Esto obliga a tomar decisiones inmediatas en el momento de la intervención, ya que la inacción o una actuación incorrecta pueden conducir a la pérdida irreversible de información relevante.

En tercer lugar, destaca su **fragmentación**. La información no se encuentra necesariamente concentrada en un único soporte, sino que puede estar distribuida entre el dispositivo físico, aplicaciones, bases de datos, copias de seguridad y servicios en la nube. Este fenómeno implica que el análisis de un único dispositivo puede resultar insuficiente para reconstruir la totalidad de la actividad digital relevante.

A estas características se suman factores adicionales, como la **automatización de procesos**, la **sincronización constante con servidores externos**, y la **existencia de mecanismos de seguridad avanzados** (cifrado, autenticación biométrica, arranque seguro), que dificultan el acceso a la información y condicionan las decisiones técnicas del perito *(Contreras Calderón, 2022)*.

Todo ello conduce a una conclusión fundamental: la evidencia digital no puede ser tratada como un objeto estático, sino como un sistema dinámico cuya integridad depende del modo en que se interviene sobre él. En este contexto, la cadena de custodia adquiere una dimensión reforzada, al convertirse en el instrumento que permite documentar y controlar dicha intervención.

4. METODOLOGÍA FORENSE EN EL TRATAMIENTO DE LA EVIDENCIA DIGITAL

La práctica de la informática forense ha desarrollado una metodología específica orientada a garantizar la correcta obtención, preservación y análisis de la evidencia digital. Esta metodología no constituye un protocolo rígido, sino un conjunto de principios y fases que deben adaptarse a las circunstancias concretas de cada caso, manteniendo en todo momento la coherencia con las exigencias de integridad y trazabilidad *(ISO, 2012)*.

De forma general, pueden identificarse las siguientes fases:

4.1 Identificación y documentación inicial

La primera actuación consiste en identificar el dispositivo o sistema objeto de análisis y documentar su estado en el momento de la intervención. Este momento es crítico, ya que constituye el punto de partida de toda la cadena de custodia. La documentación debe recoger aspectos como:

-si el dispositivo se encuentra encendido o apagado

-si está bloqueado o desbloqueado

-si se encuentra conectado a redes

-condiciones físicas visibles

Una documentación deficiente en esta fase compromete la capacidad de reconstruir posteriormente el estado original de la evidencia.

4.2 Aislamiento del dispositivo

El aislamiento tiene como finalidad evitar cualquier alteración externa de la evidencia. En la práctica, esto implica impedir que el dispositivo pueda establecer comunicaciones con redes externas que modifiquen su contenido.

Es habitual, por ejemplo, que dispositivos móviles permanezcan conectados a internet o a servicios en la nube que sincronizan automáticamente datos. Si no se interrumpe esta conectividad, pueden producirse modificaciones no controladas, como:

-actualización de archivos

-eliminación remota de información

-sobrescritura de registros

Por ello, se emplean técnicas como el modo avión o el uso de dispositivos de aislamiento físico.

4.3 Adquisición de la evidencia

La fase de adquisición constituye el núcleo técnico del proceso forense. En ella se obtiene una copia de la información contenida en el dispositivo para su análisis posterior.

Se distinguen, de manera general, tres tipos de adquisición:

a) Extracción manual

Consiste en la obtención de información mediante la interacción directa con el dispositivo (capturas de pantalla, fotografías). Su valor es limitado, ya que no garantiza una imagen completa del sistema.

b) Extracción lógica

Permite acceder a los datos visibles del sistema mediante herramientas específicas. Ofrece un mayor volumen de información, pero puede excluir áreas protegidas o datos eliminados.

c) Extracción física

Consiste en una copia bit a bit del almacenamiento. Es el método más completo, ya que permite acceder a la totalidad de los datos, incluyendo restos de información borrada. Su valor probatorio es, en general, superior *(Contreras Calderón, 2022)*.

La elección del método no es neutra: determina el alcance de la evidencia y condiciona su defensa en sede judicial.

4.4 Verificación y análisis

Una vez obtenida la evidencia, se procede a verificar su integridad mediante el cálculo de valores hash. Este proceso permite confirmar que la copia obtenida no ha sido alterada desde su creación.

Posteriormente, se realiza el análisis de la información, utilizando herramientas específicas que permiten examinar archivos, bases de datos, registros y metadatos.

4.5 Conservación

Finalmente, la evidencia debe ser almacenada en condiciones que garanticen su preservación a largo plazo, evitando accesos no autorizados y posibles alteraciones.

5. HERRAMIENTAS FORENSES Y NECESIDAD DE VALIDACIÓN

El uso de herramientas informáticas es inherente al análisis forense digital. Sin embargo, su utilización no constituye por sí misma una garantía de validez. Lo relevante no es la herramienta en sí, sino el modo en que se utiliza.

Desde una perspectiva jurídica, resulta imprescindible documentar:

-qué herramienta se ha utilizado

-versión concreta

-configuración aplicada

-finalidad de su uso

(ISO, 2012)

Asimismo, el entorno en el que se realiza la intervención adquiere especial relevancia. La norma IRAM-ISO/IEC 17025 establece requisitos de calidad aplicables a laboratorios, incluyendo aspectos como la competencia del personal, la trazabilidad de los procesos y el control de los equipos *(IRAM, 2017)*.

En este contexto, la calidad institucional no es una cuestión accesoria, sino un factor determinante en la credibilidad de la prueba digital.

6. LA FALACIA DEL HASH COMO GARANTÍA AUTÓNOMA DE INTEGRIDAD PROBATORIA

En el ámbito de la informática forense, el uso del hash criptográfico se ha consolidado como una herramienta técnica de referencia para verificar la integridad de la evidencia digital. Su funcionamiento descansa en la generación de una huella única asociada a un conjunto de datos determinado, de modo que cualquier alteración en dichos datos implica necesariamente la modificación del valor obtenido. Desde esta perspectiva, el hash permite afirmar, con un alto grado

de certeza matemática, que dos archivos son idénticos o que, por el contrario, han sufrido algún tipo de modificación *(Rubio Alamillo, 2016)*.

No obstante, la práctica forense contemporánea ha tendido a sobredimensionar el alcance de esta herramienta, hasta el punto de convertirla, en muchos casos, en un criterio aparentemente suficiente para sostener la integridad probatoria. Esta reducción conceptual resulta problemática. El hash acredita la coincidencia entre dos estados de la información, pero no proporciona información alguna sobre el procedimiento mediante el cual se ha obtenido dicha información ni sobre las condiciones en que se ha producido su tratamiento *(Jamardo Lorenzo, 2025)*.

Así, puede darse la situación —no infrecuente en la práctica— de que una copia forense presente un valor hash correcto respecto de un determinado estado del dispositivo, pero que dicho estado se haya visto previamente alterado como consecuencia de una intervención inadecuada. En tales casos, la integridad criptográfica no compensa la deficiencia metodológica. La prueba no es fiable porque, aun siendo técnicamente idéntica en el momento de la verificación, no existe garantía de que represente fielmente la información original existente en el momento de la incautación.

Este fenómeno pone de manifiesto una distinción esencial: el hash verifica el resultado, pero no valida el proceso. La cadena de custodia, sin embargo, se construye precisamente sobre la necesidad de documentar y controlar ese proceso. De ahí que la identificación entre ambos conceptos resulte no solo técnicamente incorrecta, sino jurídicamente insuficiente.

En consecuencia, debe afirmarse que el hash constituye un instrumento necesario en el ámbito de la verificación técnica, pero en ningún caso puede erigirse en elemento autónomo de garantía probatoria. Su valor solo adquiere pleno sentido cuando se integra en un contexto metodológico más amplio que permita explicar, justificar y reproducir las condiciones en las que se ha obtenido la evidencia.

7. CONSECUENCIAS PROCESALES DE UNA CADENA DE CUSTODIA DEFECTUOSA

La relevancia de la cadena de custodia no se agota en el plano técnico, sino que proyecta efectos directos sobre la validez jurídica de la prueba. Las deficiencias en su configuración pueden traducirse en una pérdida de credibilidad del material probatorio, en su impugnación por las partes e incluso, en supuestos extremos, en la declaración de nulidad.

La doctrina ha puesto de relieve que no toda irregularidad en la cadena de custodia conlleva necesariamente la invalidez de la prueba. Sin embargo, sí resulta determinante en la medida en que afecta a la posibilidad de verificar la autenticidad y la integridad del material aportado. Como señala Requejo Passoni (2025), la ruptura relevante de la cadena de custodia se produce cuando las deficiencias impiden sostener de forma razonable la correspondencia entre la evidencia presentada y su supuesto origen o cuando generan dudas suficientes sobre su manipulación indebida.

En este contexto, adquiere especial importancia el principio de contradicción. La prueba digital, al igual que cualquier otro medio probatorio, debe poder ser sometida a examen por las partes, lo que implica la posibilidad de analizar tanto su contenido como el procedimiento seguido para su obtención. Una cadena de custodia incompleta o defectuosa limita esta capacidad de control, debilitando el derecho de defensa y comprometiendo la equidad del proceso.

Debe añadirse que, en la práctica judicial, no es infrecuente que la discusión sobre la validez de la prueba digital se desplace desde el plano del contenido al del procedimiento. Es decir, el debate ya no gira únicamente en torno a “qué dice la evidencia”, sino a “cómo se ha obtenido”. En este sentido, la cadena de custodia se convierte en el eje central del conflicto probatorio, especialmente en aquellos supuestos en los que el contenido de la prueba resulta determinante para la resolución del caso.

Por ello, la correcta documentación de cada fase del tratamiento de la evidencia no constituye una mera exigencia formal, sino una condición necesaria

para sostener su defensa en sede judicial. La ausencia de información sobre aspectos como el aislamiento, la adquisición o el almacenamiento no solo debilita la prueba, sino que puede generar una presunción de irregularidad difícilmente superable.

8. LA CALIDAD INSTITUCIONAL COMO ELEMENTO DE VALIDEZ PROBATORIA

Otro aspecto frecuentemente infravalorado en el análisis de la cadena de custodia es el relativo al entorno institucional en el que se desarrolla la actividad forense. La fiabilidad de la prueba digital no depende exclusivamente de la actuación individual del perito, sino también de las condiciones organizativas, técnicas y metodológicas del laboratorio o entidad responsable del análisis.

En este sentido, la norma ISO/IEC 17025:2017, adoptada en el ámbito argentino como IRAM-ISO/IEC 17025:2017, establece un marco de referencia para la competencia de los laboratorios de ensayo y calibración, incluyendo aspectos como la formación del personal, el control de los equipos, la trazabilidad de las mediciones y la gestión de la calidad *(IRAM, 2017)*.

La aplicación de estos estándares al ámbito de la informática forense implica reconocer que la calidad del procedimiento no se limita a la intervención técnica sobre el dispositivo, sino que se extiende a todo el sistema de gestión en el que dicha intervención se inscribe. La existencia de protocolos documentados, la validación de herramientas, el control de accesos y la formación continua del personal constituyen elementos que contribuyen de manera directa a la credibilidad del resultado pericial *(Di Iorio et al., 2023)*.

Desde una perspectiva jurídica, esta dimensión institucional adquiere especial relevancia, en la medida en que permite reforzar la confianza en el procedimiento seguido. No se trata únicamente de acreditar que el perito ha actuado correctamente, sino de demostrar que dicha actuación se ha desarrollado en un entorno que minimiza los riesgos de error, manipulación o contaminación de la evidencia.

En este sentido, puede afirmarse que la cadena de custodia no se limita al recorrido físico o lógico de la evidencia, sino que incluye también el conjunto de condiciones organizativas que hacen posible su tratamiento adecuado. La prueba digital, en consecuencia, no es solo un producto técnico, sino el resultado de un sistema de calidad.

9. DE LA CADENA DE CUSTODIA A LA CADENA DE VALOR PROBATORIO

La evolución tecnológica y la creciente complejidad de la evidencia digital obligan a replantear el alcance del concepto tradicional de cadena de custodia. La mera documentación del recorrido de la evidencia resulta insuficiente para dar respuesta a las exigencias actuales de fiabilidad probatoria. Por ello, resulta conveniente avanzar hacia una concepción más amplia, que puede denominarse **cadena de valor probatorio***(Jamardo Lorenzo, 2025)*.

Este enfoque parte de la idea de que la validez de la prueba digital no depende de un único elemento, sino de un conjunto de actuaciones interrelacionadas que, en su conjunto, proporcionan garantías de autenticidad y fiabilidad. Cada fase del proceso —desde la identificación del dispositivo hasta la presentación de los resultados— añade o resta valor probatorio en función de su correcta ejecución.

Así, la identificación precisa del soporte, la adecuada documentación inicial, el aislamiento oportuno, la selección del método de adquisición, la utilización de herramientas validadas, la verificación de integridad, el análisis técnico y la conservación segura constituyen eslabones de una cadena en la que cada elemento resulta imprescindible. La ausencia o debilidad de alguno de ellos no puede ser compensada por la corrección de los restantes.

Esta visión permite superar la concepción reduccionista de la cadena de custodia como un simple registro para entenderla como un sistema dinámico de construcción de fiabilidad. La prueba digital deja de ser un dato aislado para convertirse en el resultado de un proceso verificable.

10. CONCLUSIONES

La evidencia digital ha adquirido una relevancia indiscutible en el proceso judicial contemporáneo, planteando al mismo tiempo desafíos técnicos y jurídicos sin precedentes. Su naturaleza mutable, volátil y fragmentada exige la adopción de mecanismos de control reforzados que permitan garantizar su autenticidad, integridad y trazabilidad.

En este contexto, la cadena de custodia se configura como una herramienta esencial, no solo en términos técnicos, sino también como garantía procesal vinculada al derecho de defensa. Su correcta implementación permite asegurar que la prueba puede ser sometida a contradicción y valorada racionalmente por el órgano jurisdiccional.

El análisis desarrollado en este trabajo permite afirmar que la integridad de la evidencia digital no puede reducirse al cálculo de un hash criptográfico. Esta herramienta, si bien resulta necesaria para verificar la identidad técnica de los datos, no sustituye la necesidad de documentar el procedimiento ni garantiza por sí sola la fiabilidad de la prueba. El hash acredita un estado de la información, pero no permite reconstruir el camino seguido para obtenerla.

Por ello, la validez probatoria de la evidencia digital exige un enfoque integral en el que converjan técnica, metodología, documentación y calidad institucional. La propuesta de avanzar hacia una cadena de valor probatorio permite integrar estos elementos en un modelo coherente, capaz de responder a las exigencias de la práctica judicial actual.

En definitiva, la prueba digital no se legitima únicamente por su contenido, sino por la forma en que dicho contenido ha sido obtenido, tratado y conservado. En este sentido, puede afirmarse que:

No es el dato lo que prueba, sino el camino que recorre hasta el proceso.

Esta afirmación resume la idea central del presente trabajo: la fiabilidad de la prueba digital no es una propiedad inherente al dato, sino el resultado de un proceso técnicamente adecuado y jurídicamente defendible.

REFERENCIAS BIBLIOGRÁFICAS

Contreras Calderón, C. A. (2022). Buenas prácticas en informática forense para el procesamiento de evidencia digital o información electrónicamente almacenada. Publicaciones e Investigación, 15(2). https://doi.org/10.22490/25394088.5245

Di Iorio, A. H., Ambrústolo, M., et al. (2023). Guía técnica para el diseño y la implementación de un sistema de gestión de calidad en laboratorios de informática forense. Universidad FASTA / Universidad Nacional de Mar del Plata.

González Reyes, J. M. (2021). La prueba pericial digital y la cadena de custodia. Anales de la Facultad de Derecho, 38, 43–79. https://doi.org/10.25145/j.anfade.2021.38.03

Instituto Argentino de Normalización y Certificación (IRAM). (2017). IRAM-ISO/IEC 17025:2017. Requisitos generales para la competencia de los laboratorios de ensayo y calibración.

International Organization for Standardization (ISO). (2012). ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.

Jamardo Lorenzo, A. (2025). La dimensión tecnológica de la cadena de custodia: algunas claves. InDret, 2. https://doi.org/10.31009/InDret.2025.i2.07

Requejo Passoni, W. (2025). La nulidad procesal por ruptura de la cadena de custodia digital: estándares comparados en la jurisprudencia argentina y española. Estudios sobre jurisprudencia, 326–345.

Rubio Alamillo, J. (2016). Conservación de la cadena de custodia de una evidencia informática. *Diario La Ley*, (8859).

Nota de transparencia editorial

El presente manuscrito constituye una reelaboración sustancial de un trabajo previo de la autora, incorporando una reformulación integral del texto, una nueva sistematización argumental y una actualización técnico-jurídica conforme a estándares normativos y doctrina reciente. La presente versión ha sido

específicamente desarrollada para esta publicación y no se encuentra sometida simultáneamente a evaluación en otra revista.