RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 16/09/2026 | aceito: 23/09/2026 | publicação: 28/09/2026

La seguridad de los datos en la cadena de custodia digital y archivística del Derecho Procesal Penal con énfasis en la Ley del Paquete Anticrimen

A segurança de dados na cadeia de custódia digital e arquivística do Direito Processual Penal com enfoque na Lei do Pacote Anticrime

Data security in the digital and archival chain of custody in Criminal Procedural Law with a focus on the Anti-Crime Package Act

João Pedro Prucoli Cortes – Faculdade de Direito de Cachoeiro de Itapemirim (FDCI), joao.cortes@aluno.fdci.edu.br – Estudiante de grado en Derecho.
Ticiano Yazegy Perim – Faculdade de Direito de Cachoeiro de Itapemirim (FDCI), ticianoperim@hotmail.com – Doctorando en Educación por la Universidad Estácio de Sá (UNESA); Magíster en Ciencias Jurídicas y Sociales por la Universidad Federal Fluminense (UFF); Especialista en Derecho Público por la Universidad Candido Mendes (UCAM); Profesor universitario de la FDCI | ORCID: 0000-0003-2761-1824.

Resumen:

La cadena de custodia de pruebas periciales es un instituto del Derecho penal de total relevancia a los resultados procesales, y como tal, se adecuó a los avances tecnológicos de punta para actuar con mayor agilidad, precisión, transparencia y eficiencia en las operaciones que involucran los procedimientos concernientes a las pruebas criminales. De ese modo, este estudio se objetivó a estudiar la relevancia y desafíos a la seguridad de datos de la cadena de custodia digital y arquivística discrepando sobre sus peculiaridades, normativas legales, procedimientos periciales, aplicaciones y almacenamientos, identificando los principales desafíos a la preservación de sus archivos, a la quiebra de la cadena y a las posibles brechas en la Ley n. 13.964/19 -Pacote Anticrime. Se trata de una revisión de literatura con abordaje cualitativo y carácter exploratorio-narrativo embasada en un recorte temporal que consideró los años de 2015 a 2026, teniendo como base de recolección el CAPES, el Google Académico, la SciELo y plataformas jurídicas. Los resultados alcanzados indican un gran volumen de regulaciones y desafíos especialmente dirigidos a la quiebra de la cadena de custodia digital, lo que hace que el tema sea más interesante y relevante de ser profundizado. Se concluye que el paquete Anticrime es integrado a la cadena de custodia pena, digital y digital archivada que necesita seguir rayando las normas legales y estándares específicos con el fin de garantizar la seguridad de los datos de pruebas leales responsables de los resultados judiciales.
Palabras clave: Cadena de Custódia. Derecho penal. Ley n. 13.964/2019. Seguridad de datos. Tecnologías de Ponta.

Resumo:

A cadeia de custódia de provas periciais é um instituto do Direito Processual Penal de total relevância aos resultados processuais, e como tal, se adequou aos avanços tecnológicos de ponta para atuar com maior agilidade, precisão, transparência e eficiência nas operações que envolvem os procedimentos concernentes às provas criminais. Desse modo, esse estudo se objetivou a estudar a relevância e desafios à segurança de dados da cadeia de custódia digital e arquivística discorrendo sobre suas peculiaridades, normativas legais, procedimentos periciais, aplicações e armazenamentos, identificando os principais desafios à preservação dos seus arquivos, à quebra da cadeia e às possíveis brechas na Lei n. 13.964/19 -Pacote Anticrime. Se trata de uma revisão de literatura com abordagem qualitativa e caráter exploratório-narrativo embasada em um recorte temporal que considerou os anos de 2015 a 2026, tendo como base de

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 16/09/2026 | aceito: 23/09/2026 | publicação: 28/09/2026

coleta o CAPES, o Google Acadêmico, a SciELo e plataformas jurídicas. Os resultados alcançados denotam um grande volume de regulamentações e aos desafios especialmente direcionados à quebra da cadeia de custódia digital, o que torna o tema mais interessante e relevante de ser aprofundado. Conclui-se que o Pacote Anticrime é integrado à cadeia de custódia pena, digital e digital arquivística que precisa seguir à risca as normatizações legais e padrões específicos com vistas a garantir a segurança de dados de provas cabais responsáveis pelos resultados judiciais.
Palavras-chave: Cadeia de Custódia. Direito Processual Penal. Lei n. 13.964/2019. Segurança de Dados. Tecnologias de Ponta.

Abstract:

The chain of custody of forensic evidence is an institute of criminal procedural law of total relevance to procedural results, and as such, it has adapted to cutting-edge technological advances to act with greater agility, precision, transparency and efficiency in operations involving procedures concerning criminal evidence. Thus, this study aimed to study the relevance and challenges to the data security of the digital and archival custody chain, discussing its peculiarities, legal regulations, forensic procedures, applications and storages, identifying the main challenges to the preservation of their files, the breaking of the chain and the possible loopholes in Law n. 13.964/19 - Anti-crime package. This is a literature review with a qualitative approach and exploratory-narrative character based on a time frame that considered the years 2015 to 2026, based on CAPES, Google Academic, SciELo and legal platforms. The results achieved denote a large volume of regulations and challenges especially directed at breaking the digital custody chain, which makes the issue more interesting and relevant to be deepened. It is concluded that the Anti-Crime Package is integrated into the chain of custody pen, digital and digital archival that needs to follow to the letter the legal norms and specific standards to ensure the security of data from cabal evidence responsible for the judicial results.
Keywords: Custody chain. Criminal Prosecution Law. Law No. 13.964/2019. Data security. Point Technologies.

1. Introducción

En el ámbito del Derecho penal procesal (DPP), las pruebas reales son indispensables para la conducción de los diversos procesos penales, lo que significa que dentro de la institución de la Seguridad Pública (SP) existe la propuesta de preservación de la fidelidad comprobatoria de la cadena de custodia de evidencias criminales (Stecker; Damian, 2021), utilizada en adelante por medio de la sigla CdC.

En Brasil, a lo largo de los últimos 10 años, la CdC viene comprobando su necesidad, importancia y eficiencia en la conducción de penas más justas y expresivas, así como a la aplicación de medidas protectivas más elaboradas, promoviendo mayor eficacia a la prisión y

detención de individuos criminales, además de propiciar audiencias de custodia más concisas a todo y cualquier tipo de delito criminal (Consejo Nacional de Justicia - CNJ, 2025). Su preservación configura un elemento estratégico impar a la excelencia operativa de los procesos penales, considerando sus objetivos en garantizar la integridad y autenticidad de evidencias penales periciadas, involucrando en ello, procesos que van desde la recolección a la presentación en juicio (Supremo Tribunal de Justicia - STJ, 2023).

La CdC incluye tres tipos de custodias periciales: la prueba penal, la prueba digital y la prueba digital archivada, reguladas por el Código de Procedimiento Penal (CPP) que fija los procedimientos/regulación de los procesos de recolección, almacenamiento, preservación de la integridad, mantenimiento de registros coesos, claros y precisos, así como la presentación correspondiente a los vestigios aplicables a los procesos penales en curso. La preservación de la integridad evita contaminación y/o adulteración de la prueba (Motta, 2022; Gava; Flores, 2023). La Ley n. 13.964/19 que implantó el denominado “Pacote Anticrime” (Brasil, 2019), imputa a la CdC integrativa al DPP, al uso de tecnologías diversas y específicas que involucran todos los procesos jurídicos en acción procesual y masivo uso de la ciberseguridad (Stecker; Damian, 2021).

La eficacia de la CdC como un todo requiere obligatoriamente, secreto de justicia y pruebas debidamente documentadas en registros y laudos periciales específicos y estandarizados, sean ellas físicas o digitales, considerando para ello, la preservación de divergentes factores y la ruptura de la CdC, como elementos primordiales para que se validen y preserven los vestigios de la infracción penal previamente examinados por los expertos y presentados en juicio cuando sea necesario (Supremo Tribunal de Justicia - STJ, 2023).

En consecuencia de eso, se afirma que el tema es amplio, complejo y conductor a una gama de cuestionamientos, lo que llevó a la elección del problema de investigación directriz a ese estudio, estructurado sobre la siguiente indagación: ¿En qué medida las tecnologías aplicadas a la cadena de custodia pueden garantizar la autenticidad, integridad y confiabilidad de la prueba digital en el proceso penal, y cuáles son las consecuencias jurídicas de las fallas en su preservación?

Hipoteticamente, las respuestas a esa pregunta provienen de las siguientes condiciones: (i) complejidad de la gestión y control de la CdC digital mediante la amplitud de dispositivos, leyes y especificidades subjetivas que la estructuram; (ii) susceptibilidad de alteración, reprogramación y de ataques por hackers a los procesos de levantamiento y preservación de pruebas criminales, realidad esa, crítica y desafiadora al Derecho Processual Penal; (c) posibles lagunas, en especial, las asociadas a la quiebra de la cadena que involucra cuestiones de

comunicabilidad, sigilos diversos, búsqueda y aprehensión, preservación/alteración del objeto y ambiente periciado, derechos y deberes legales, estructuras de procesos falhos, entre otras, imprescindibles a los resultados periciales y jurídicos.

Para tal finalidad, esta investigación se objetivó a estudiar aspectos de la seguridad de datos de la CdC Digital y Digital Archivística, conociendo características, legalizaciones y los principales desafíos a la preservación de sus archivos con foco en la quiebra de la cadena y posibles brechas en la Ley n. 13.964/19. Tal alcance demandó secundariamente: (i) caracterizar la seguridad de datos en el ámbito del Derecho procesal Penal; (ii) conceptualizar la cadena de custodia en las esferas de la prueba penal, prueba digital y condición archivada; iii) conocer las legislaciones concernientes a la cadena de custodia digital y las principales tecnologías aplicables; (iv) aclarar el Paquete Anticrime instituido por la Ley n. 13.964/19; (v) identificar los principales desafíos implicados en la CdC digital que afectan su seguridad de datos, según estudios comprobatorios y jurisprudencias del STJ.

Al apoyarse en la contextualización del tema ya discurrida, se comprende que la ampliación de conocimientos sobre el fenómeno de la seguridad de datos de la CdC digital, es además de actualísima, expresivamente importante para que se refleje sobre la robustez del asunto y se corrobore a la minimización de la laguna temática, todavía parcamente abordada por la academia. Delante de eso, se justifica la elección y relevancia del estudio, cuyos resultados son promotores de excelentes ganancias académicos, legales, públicos y sociales y, de exponencial aplicabilidad en la esfera del DPP.

Ese estudio se estruturó además a sus datos pretextuales y por ese capítulo introductorio, por los capítulos asociados al referencial teórico, metodología aplicada, resultados/discusiones y consideraciones finales, cerrando por el elemento posttextual que lista las referencias bibliográficas usadas. Se destaca que lo mismo siguió las normas del Manual de la FDCI para la disciplina afín, y también las disposiciones de la Asociación Brasileña de Normas Técnicas (ABNT) para trabajos académicos-científicos.

2. Marco teórico

Ese capítulo fue estructurado para mapear y dar sustanza a los objetivos propuestos por esa investigación, presentando las referencias bibliográficas correspondientes al que fue alcanzado teóricamente en publicaciones recientes, analizadas y legitimadas por fuentes académicacientíficas, del STF y del STJ.

Para la temática dirigida a la caracterización de la seguridad de datos, según Stecker y Damian (2021) ella es concerniente a un concepto valoroso y esencial en el ámbito del DPP, ya que reúne una gama de prácticas, métodos, tecnologías y políticas dirigidas a la protección de informaciones digitales en el contexto del acceso no autorizado, robo, pérdida y corrupción.

Se enfoca en la defensa técnica exigida a la garantía de la confidencialidad, integridad y disponibilidad de datos, y la legitimidad de los usuarios a los accesos, objetivando la protección contra amenazas externas/internas provenientes de fallas humanas, virus digitales y hackers, haciendo uso de herramientas como criptografía, autenticaciones faciales y biométricas, rigor en el control de accesos y monitoreo multifactorial continuo, intuyendo minimizar la ocurrencia de riesgos en ambientes físicos, digitales y en la nube (Lucas et al., 2023).

Cabe destacar que en Brasil, la seguridad de datos personales, se alicerza previamente en las égides de la Ley no 13.709/2018 (Ley General de Protección de Datos - LGPD) regulando el tratamiento de datos digitales en general, sin embargo, con enfoque dirigido más expresivamente a la privacidad de los datos. En lo que se refiere a las acciones de persecución y represión de infracciones penales cabibles al DPP, la seguridad de datos sigue las disposiciones del art. 4o, caput III, "a" - seguridad pública y "d" - actividades de investigación y represión de infracciones penales), c/c §1o de la LGPD (Brasil, 2018), el cual determina:

> § 1o El tratamiento de datos personales previsto en el inciso III se regirá por una legislación específica, que deberá prever medidas proporcionales y estrictamente necesarias para la atención del interés público, observadas el debido proceso legal, los principios generales de protección y los derechos del titular previstos en esta Ley (Brasil, 2018 p. 1).

En ese escenario, la Enmienda Constitucional EC en el 115/2022 acresció el inciso LXXIX al artículo 5o de la CF de 88 dispondo sobre la protección general de datos, incluyendo los de orden digital, como derecho fundamental, debidamente garantizado en la forma de la ley. Su embasamiento jurídico implica los ejes abajo:

(i) Autodeterminación Informativa - derecho fundamental que garantiza al ciudadano el control sobre sus datos personales, limitando la actuación del Estado y evitando abusos o selectividad en la persecución penal; (ii) Crime de Invasión de Dispositivo Informático - el art. 154-A del CP (según Ley no 14.155/2021), tipifica el crimen de invasión de dispositivo informático de uso ajeno para obtener, adulterar o destruir datos o informaciones sin autorización, o para instalar vulnerabilidades objetivando ventajas ilícitas, y; (iii) Exigencia de Ley Específica: el tratamiento de datos personales dado por las autoridades públicas, observa los principios de legalidad, proporcionalidad, necesidad y proceso legal existente, objetivando

la adopción de medidas necesarias al interés público, incluso cuando no haya aplicación directa de la LGPD (Souza, 2022). El concepto del término “cadea de custodia” utilizado en el ámbito jurídico y en el ámbito del DPP y, en las palabras de los Exmos. Promotores de Justicia Levy E. Magnus y Mylene Comploier (2021, p. 196) la CdC está constituida por "[...] una sistematización de procedimientos que objetivan la preservación del valor probatorio de la prueba pericial, más precisamente, de su autenticidad".

Esto significa que a partir de la inclusión del art. 158-A y art. 158-B al CPP por la Ley n. 13.964/19, se trata de la colección de todos los procedimientos que mantienen y documentan la historia cronológica de un vestigio bruto, visible o no, percibido, constatado y/o recogido en locales o, en las víctimas de crímenes, exigible para que se rastrean factores como posesión y manejo, envolviendo en eso, las etapas que van desde sus reconocimientos hasta sus descartes (Brasil, 2019).

Indo al encuentro del contexto arriba, la CdC se alicerza mínimamente sobre cuatro principios fundamentales regidos por el Art. 158-A del CPP. El primero, condice con la “autenticidad” refiriéndose a la originalidad del objeto en análisis pericial, oriundo de fuentes actuales y anunciadas en la etapa de la recolección, sin cualquier tipo de adulteración a lo largo de un proceso, garantizando de esa forma, la identificación y la seguridad en el origen de la información, lo que requiere la tutela del agente perito. El segundo, a su vez, corresponde a la “integridad” que valida la evidencia criminal desde su reconocimiento hasta su tránsito en juzgado, garantizando así su mérito como prueba procesual mantenida en las mismas condiciones en que fue identificada (Ramalho et al., 2023). En complemento, se tiene el principio de “confiabilidad o fiabilidad” como criterio de valorización de la prueba criminal en términos de su idoneidad, el cual es relevante al fundamentamiento del argumento judicial y, posibilita la verificación de terceros a despecho de la adecuación de los procedimientos adoptados. También existe el principio de “mesmidad” asociado a la formación de la convicción del juez sobre la prueba criminal que debe obligatoriamente ser idéntica al vestigio identificado y recogido en la escena del crimen, tornándose así, la base que garantiza los principios de identidad y trazabilidad de la evidencia (Fischer, 2025).

Además del ya descrito, la CdC involucra tres agrupaciones: (i) la cadena de Custódia de la Prueba Penal (CdCPP); (ii) la cadena de Custódia de la Prueba Digital (CdCPD) y; (iii) la cadena de Custódia Digital Archivística (CCDA), cada cual con sus especificidades y fines jurídicos conforme presentado en el Cuadro 1.

Cuadro 1 - Las agrupaciones de la cadena de custodia en el ordenamiento jurídico

Grupo	Características legales

Cadena de Custódia de la Prueba Penal (CdCPP)	Sigue las disposiciones de las Artes. 158-A a 158-F del CPP que tratan de la exigencia legal de admisibilidad en el proceso penal, objetivando la garantía de la idoneidad, trazabilidad y autenticidad de todo y cualquier vestigio, en todas las etapas procesuales, indiferentemente de su estructura física o digital. Engloba la documentación cronológica, detallada y completa de la historicidad del vestígio intuyendo cuestionamientos sobre posibles adulteraciones y/o contaminaciones, teniendo en cuenta la quiebra de la cadena y sus consecuencias que tienden a la conducción de la inadmisibilidad o nulidad de la prueba, frente a los principios de la integridad y de la garantía del proceso legal afil.
Cadena de custódia de la prueba digital (CdCPD)	Asociado a la aplicación específica de los principios de la cadena arriba presentada, a las posibilidades electrónicas, intuyendo el reconocimiento de la naturaleza volátil y mutable de la prueba digital, y con eso, garantizar que la copia anexada a los autos de un proceso sea idéntica al vestígio original aprendido, preservando la integridad del contenido y de los metadados.
Cadena de Custódia Digital Arquivística (CCDA)	Referencia al concepto arquitectónico fundamentado en la gestión del ciclo de vida del documento digital, así como de su preservación a largo plazo, garantizando sus principios legales de autenticidad y confiabilidad y, además, la no quiebra de su custodia arquitectónica. Se centra en las elecciones y en la integridad técnica y jurídica de documentos cuyos fines son la memoria, la transparencia y la prueba futura.

Fuente: Adaptado por el autor de Matida (2020); Motta (2022); Gava y Flores (2023); Fischer (2025).

En el contexto de la complejidad de la triple categoría de la CdC como visto en el Cuadro1, contexto, importante observar lo que Santos (2022) resalta, al afirmar que, a pesar de que las pruebas periciales pasaron a ser inseridas en la CdC por la Portería SNSP 82/14, su efectivación en ese instituto ocurrió solamente cuando del aumento de los Arts. 158-A a 158-F, dispuestos por la Ley 13.964/2019.

Con referencia a los procesos adoptados por las CdCs sean ellas físicas, digitalizadas o archivadas, se observa en las investigaciones conducidas por Gava y Flores (2020) y Lima y Romanelli (2023), que estos necesitan ser auditados por procedimientos de preservación, requeridos a la atención de su capacidad en garantizar la genuidad y fidedignidad de pruebas periciales provenientes de un ambiente digital, que por naturaleza, ya son potencialmente complejas y vulnerables dado el hecho de sus tramitaciones entre sectores. Se Clarifica que delante de la amplitud, complejidad y detalle a la construcción de la CdC, cada vestigio dentro de una única escena criminal, demanda que se atiendan las diez etapas dispuestas en el CPP y la Ley. n. 13.964/19, constituidas en el cuadro 2.

Cuadro 2 - Etapas que involucran las pruebas periciales de una CdC

Paso	Correspondencia	Características
1	Reconocimiento	Identificación del vestígio como potencial prueba pericial
2	aislamiento	Preservación total del medio ambiente

		y del vestígio pericial
3	Fixación	Ato de describirse con detalles el ambiente y el vestígio pericial
4	Recolección	Recogida del vestígio sin ningún cambio de su originalidad
5	Acondicionamiento	Guarda del vestigio en recipiente propio, etiqueta de identificación, fecha y hora de la recolección
6	Transporte	Movimentación del vestígio al lugar de destino asegurando su integridad
7	Recibido	Formalización documentada de la transferencia del vestígio
8	Procesamiento	Condizente con el examen pericial y la emisión de su laudo
9	Almacenamiento	Asociado a las condiciones de guardia de la prueba pericial y su laudo
10	Descarte	Corresponde a la eliminación total de la prueba pericial según leyes y normas afines

Fuente: Adaptado por el autor de Brasil (1941; 2019).

Fundamentando en el presentado en el Cuadro 2, y para hacer jus al propósito jurídico, se cita el §1o del art.158-A del CPP instituido por la Ley n. 13.964/19, dispone que “el inicio de la cadena de custodia se da con la preservación del local de crimen o con procedimientos policiales o periciales en los cuales sea detectada la existencia de vestígio” (Brasil, 1941, p. 1). Esta premisa reconoce la relevancia de la conservación de la escena del crimen; del(s) su(s)vestígio(s); de la adopción de procedimientos de seguridad estándar y de la relevancia del perito (Cavalcanti; Silva, 2026).

Tal reconocimiento, según la concepción de la Súmula no 361 aplicada por el Supremo Tribunal Federal (STF, 2026, p.1), enuncia que: “en el proceso penal, es nulo el examen realizado por un solo experto, considerándose impedido lo que ha funcionado, anteriormente, en la diligencia de aprehensión”, cuyo embasamiento se sustenta en los Arts. 151; 159 a 160; 165; 170 a 171; 173; 177; 179, en el párrafo único del artículo. 181 y 279, II, dispuestos en el CPP. Este enunciado se basa en las tres siguientes condiciones (i) aplicación a Peritos No Oficiales; ii) inaplicabilidad a Peritos Oficiales (servidores federales y estatales) y; iii) impedimento por Participación Previa. Esto remite a la reflexión sobre la regla de la nulidad.

A título de conocimiento, Motta (2022) y Gava y Flores (2023), destacan que la CdC igital/Digital Arquivística integrativas al DPP, utilizan, particularmente, divergentes Tecnologías de Información y Comunicaciones (TICs) y de ciberseguridad, las cuales no serán discurridas en esta revisión, considerando que su objetivo es buscar respuestas a los riesgos de la seguridad de datos de las pruebas criminales mantenidas en las CdCs.

Sin embargo, es necesario que se comprenda que todas las tecnologías aplicadas en las CdCs están regidas por divergentes directrices para el respaldo legal a sus procedimientos en general. Dentro de ese escenario, se destacan: el Request for Comments RFC n.3227/02 -

documento técnico que describe patrones, protocolos, métodos e investigaciones realizadas de forma digital, definiendo la base de comunicación de Internet y compartiendo datos relevantes de la ingeniería de la computación (Motta, 2022); la Ley n. 12.965/14 - Considerada como Marco Civil de Internet una vez que dispone sobre los principios de privacidad, protección de datos y guarda de registros (Brasil, 2014); la Resolución CONARQ n. 51/23 Versión 2 - Dispone sobre las "Diretrizes para la Implementación de Repositorios Archivísticos Digitales Confiables" (Consejo Nacional de Archivos – CONARQ, 2023).

Además, se destacan: las Jurisprudencias del STJ y STF - anulan pruebas recogidas sin la debida autorización judicial, o también, a través del manejo indebido previo a la pericia oficial (Motta, 2022; Fischer, 2025; Pereira, Torres, 2025); la Instrucción Normativa IN DG/PF n. 299/25 - fija y detalla directrices técnicas dirigidas a la preservación, análisis y utilización de elementos digitales recaudados en los procesos investigativos de la PF (Souza, 2026) y; las Normas Regulamentadoras Internacionales (NRs) y Normas Brasileñas de Regulación (NBRs) - directrices de recomendación, regulación y estandarización de procesos, buenas prácticas al Sistema de Gestión de Seguridad de la Información (SGSI) (Brasil, 2026).

En esa coyuntura legal, surge el Paquete Anticrime (PA) instituido por la Ley n. 13.964/2019 que visó el perfeccionamiento de la legislación penal y procesal penal, cuya idealización se dio en la búsqueda de reducir lagunas en la seguridad pública, considerando que cuenta con 70 medidas específicas dirigidas al fortalecimiento del sistema penal, confiriendo así, la imputación de acciones más rígidas y menos burocráticas dirigidas a la mitigación de ocurrencias violentas, impunidads y reincidencias en ese escenario. Las perspectivas de su implementación implican la movilización de las sociedades; la transparencia de las acciones; la integración de los sectores privados y públicos; las elecciones; y obviamente, la persecución criminal (Brasil, 2019).

Según Santos (2022), la edificación del PA se alicerzó en el elevado índice de corrupción activa, pasiva, necesaria y predictiva. Esto se ha adherido a los problemas de superfacturación, competencia, fraude digital y falsedad de notas fiscales. Todos, experimentados en el país en sus divergentes sectores de la socioeconomía, pero con énfasis en la Administración Pública. El investigador resalta que con el PA, las pruebas periciales pasaron a ser inseridas en la CdC, efectivamente. La problemática de la corrupción es uno de los principales temores de la población brasileña, y suscita la reflexión sobre la efectivación de la prisión en sed cautelar o sentencia en juzgado. En ese escenario, la Ley n. 13.964/2019 incluyó el denominado “Juiz de Garantías” como responsable de las etapas de investigación criminal diferenciandolo del juez que actúa en la instrucción y juicio del proceso penal, intuyendo la

garantía de la imparcialidad de ese magistrado y el no contacto del mismo con cualquier prueba criminal para inferir un prejulgamento (Brasil, 2019). Es decir, "[...] la actuación del juez de garantías garantizaría, en la secuencia, otro juez imparcial, que no tuvo contacto previo con la investigación, eso daría paridad de armas entre la acusación y la defensa" (Santos, 2022, p. 112).

Se constató que la Teoría del Proceso Penal inserta la prueba cabal dentro del PA, en la explanación de Abreu; Cardoso y Passos (2022), esa condición le confiere el status de mecanismo reconstructor de eventos investigados en determinado proceso judicial. En el campo de las pruebas lícitas/ilícitas, los autores argumentan que el PA tiene embasamiento en los presupuestos del DPP concernientes a las tres Teorías, resumidas de la siguiente forma: (i) Teoría de los Frutos del Árbol Envenenada – basada en la contaminación e inadmisibilidad de pruebas derivadas de fuente ilícita; (ii) Teoría de la Fuente Independiente – permite pruebas de naturaleza lícita y sin relación causal con la prueba ilícita original, y; (iii) Teoría del Descubrimiento Inevitable – considera la derivación de la prueba si descubierta por medios lícitos.

En lo que se relaciona a la identificación de los principales desafíos experimentados por la CdCPD y CCDA y las posibles lagunas de la Ley n. 13.964/19 que afectan la seguridad de datos del instituto del DPP, las literaturas de Motta (2022), Santos (2022), Gava y Flores (2025), y Pereira y Torres (2025) resaltan que la ciberseguridad es indispensable para los resultados procesales, una vez que ofrecen mayor seguridad y transparencia jurídica y penal. Sin embargo, en cambio, denotan una gama de problemas de orden jurídico e infraestructural. Esto se justifica por Lucas et al. (2023), al señalar el crecimiento exponencial del interés de la comunidad científica en lo que se refiere a la aplicación de técnicas de ciberseguridad para mitigar los ataques a las redes de computadoras, configurando la relevancia potencial de tales métodos. Delante de eso, se resalta como principal elemento desafiador, la "quebra de la cadena de custodia", representada por la "[...] falla o interrupción de la trayectoria de las pruebas, como en la identificación, manejo y descarte de las informaciones usadas en la investigación, la cual perjudica la confiabilidad y el contradictorio por no permitir la garantía de la integralidad de la prueba" (Marques; Barbosa, 2025, p.?).

En la concepción del ordenamiento jurídico en acto procesual, se vio adicionalmente que:

> [...] el instituto de la ruptura de la cadena de custodia se refiere a la idoneidad del camino que debe ser recorrido por la prueba hasta su análisis por el magistrado, siendo cierto que cualquier interferencia durante el

> procedimiento puede resultar en su insistencia. Tiene como objetivo garantizar a todos los acusados el debido proceso legal y los recursos a él inherentes, como la amplia defensa, el contradictorio y principalmente el derecho a la prueba lícita (STJ. Agravo en Recurso Especial n. 1.847.296-PR (2021/0049381-6).

Además, Exmo. Fiscal Douglas Fischer (2025) relata que en el campo de las nulidads/invalidades promovidas por la quiebra de la CdC, la jurisprudencia del STJ en diversos Recursos y Agravos procesales, comprende que para configurar la referida quiebra, deben ser analizados minuciosamente los aspectos: eficacia de la prueba (posibles adulteraciones); demostración de daños efectivos al proceso; garantía de idoneidad y confiabilidad de la prueba, explicando que: Si una prueba es ilícita (inválida), ni cabería al juzgador hacer el análisis de su confiabilidad. Una excluye la otra. La prueba ilícita no puede ser usada en el proceso. La prueba lícita, incluso con la ruptura de la cadena de custodia, debe ser analizada para saber se confiere credibilidad al juicio. Es decir, tiene que ser evaluada por el juzgador y no eventualmente excluido (Fischer, 2025, p. 1).

Igualmente, Alves y Bezerra (2023, p.1) observan que el PA representa una innovación al ordenamiento jurídico brasileño, una vez “elevar al nivel de la ley el Reglamento de la cadena de custodia”. Sin embargo, pesa ajustes necesarios en lo que se asocia al incumplimiento de las imposiciones regulatorias a la CdC, cuyos resultados imputan a la jurisprudencia, la responsabilidad sobre sus análisis en términos de nulidad absoluta o relativa. La nulidad de acuerdo con el CPP a partir de su art. 563 en adelante, rige que cuando absoluta se asocia a la no admisión de la convalidación, presumiendo una naturaleza que jamás debería existir. Cuando, por su parte, admite la convalidación sin ningún perjuicio al interés público, a la acusación o a la defensa. Sobre lo anterior, la jurisprudencia en el 720 del STJ (6a Turma), existe el entendimiento de que “las irregularidades constantes de la cadena de custodia deben ser sopesadas por el magistrado con todos los elementos producidos en la instrucción, a fin de verificar si la prueba es confiable” (Alves; Bezerra, 2023, p.8). Sin embargo, Cavalcanti e Silva (2026) hacen mención a la omisión del legislador frente a la ruptura de la CdC, lo que fomenta debates sobre la admisibilidad o no de la prueba. Esto se conecta directamente con: (i) el valor de la misma; (ii) el acto correspondiente a la tal ruptura, y; iii) las directrices legales en el contexto.

Como factores extra a los ya discurridos que envuelven los desafíos a la seguridad de datos en la CdC, el Cuadro 4 resumió los hallazgos de las demás literaturas estudiadas.

Cuadro 4 - Desafíos encontrados en las literaturas estudiadas sobre la nulidad, ruptura de la cadena de custodia y brechas en el PA

Desafíos	Autor/año
Ilegalidad de los prints de pantallas (WhatsApp / medios sociales) y extracción de datos de teléfonos móviles - titulares del estado de prueba comprobatoria controversial, frente al entendimiento jurídico en cuanto al envío y exclusión de mensajes de forma libre, por quien envía y/o recibe, sin que haya rastro o almacenamiento de las mismas.	Motta (2022)
Falta de registro documental de todas las etapas de la prueba cabal; pérdida o inacesibilidad a los medios periciados en su originalidad, impidiendo la autenticación o construcción de contraprobación técnica; dificultades impuestas por la policía/pericia en la accesibilidad a la imagen o consistencia física de la prueba requerida por la defensa; no registro de acceso y no autorización de terceros previamente a las acciones periciales; problemas en la preservación de la criptografía y/o firma digital.	Marques y Barbosa (2025)
Falta de regulación específica y de estandarización en el tratamiento de las pruebas; subjetividad histórica y caracterización de cada prueba; adulteración de las pruebas; problemas de accesos y tránsitos de los datos; definición de la prueba como registro documental de pericia jurídica; inmaterialidad, independencia y confiabilidad del vestígio digital; documentación de la CdC en la garantía de la autenticidad de la prueba; ética y gobernanza; capacitación técnica; uso de tecnología de forma irresponsable.	Gava y Flores (2023), Lima y Romanelli (2023), Pereira y Torres (2025) y Silva y Lopes (2025)
Brechas de la Ley n. 13.964/19 demandan medidas inmediatas de perfeccionamiento para estandarizar procedimientos, implementar tecnologías de rastreo y potencializar la integración interinstitucional, enfrentando condiciones personales, materiales insuficientes y divergencias económicas entre estados y municipios que afectan a los órganos de pericia oficial criminal.	Pereira y Torres (2025), Cavalcanti e Silva (2026)

Fuente: Adaptado por el autor (2026).

Tangible las pruebas digitales, en especial, las recolectas en aparatos celulares, drones, medios sociales y aplicaciones en general, los ministros del STJ (2023a) atestiguan no ser admisible ningún tipo de prueba digital sin el debido registro relativo a los procedimientos adoptados por la policía, objetivando preservar la integridad, autenticidad y confiabilidad de los componentes en esas condiciones, condición esa, vigente hasta el presente momento.

Ejemplo de eso, fue dado en la decisión del STJ pertinente al tráfico de drogas y aprehensión de aprehensión de celular, extracción de datos y captura de pantallas, fundamentado en la posible quiebra de la CdC dada por la volatilidad, auditabilidad, repetibilidad, reproductibilidad, y en la justificabilidad de la susceptibilidad a la alteración de las pruebas digitales, siguiendo el principio de la mesmidad. En él, por unanimidad, se dio el provimento al agravo régimenntal, frente a la quiebra de la CdC en no adoptar procedimientos a la garantía de la idoneidad de las pruebas digitales, bajo la siguiente alegación:

> [...] no siendo posible inferir la idoneidad de las pruebas extraídas por el acceso directo al celular aprendido, sin la utilización de herramienta forense que garantise la exactitud de las evidencias, no habiendo registros de que los elementos inicialmente recolectados son idénticos al que corroboraron la condena (STJ, AgRg no 828054 - RN (2023/0189615-0), 2024).

Otrossim, en Agravo Régimenntal sobre el proceso relativo a la homicidio calificado y asociación criminal, envolviendo prisión preventiva, prueba digital, CdC, demanda de pericia técnica complementaria y de la comprobación de la fidedignidad de los elementos probatorios digitales, objetivando conocer y discutir la ruptura de la CdC de las pruebas digitales y constrangimiento ilegal mediante la prisión preventiva, al analizar las peculiaridades relativas a la volatilidad y modificabilidad de las evidencias para comprobar sus integridads y confiabilidads, aspectos esos generadores de dudas que no pueden ser desfavorables al reo, se decidió por unanimidad dar parcial provimento al mismo (STJ, AgRg no HC 1014212 / ES – Agravo Régimenntal en el HC 2025/0231341-3, 2026).

Finalmente, Matida (2020) y también Ramalho et al. (2023), resaltan que aunque todavía existen los desafíos ya presentados en este estudio, la garantía de la autenticidad, integridad, confiabilidad y mesmidad de las pruebas integradas a las CdCs física, digital o digital arquivística, poseen un carácter decisivo en la conducción de los resultados procesales de orden jurídico, minimizando los riesgos de condenar sujetos inocentes y liberar erróneamente individuos criminales, pero también inducir pérdidas financieras a las arcas públicas, indenizaciones injustas y, desperdicio de tiempo lo que resulta en la construcción de la desconfianza poblacional al sistema judicial.

3. Metodología

Este estudio adoptó de acuerdo con Enrique y Medeiros (2017), una investigación básica considerando su finalidad en expandir conocimientos científicos sin una aplicación práctica respecto del fenómeno de la seguridad de datos en la CdC Digital y Digital Arquivística que compone el DPP, sus desafíos y posibles brechas de la Ley n. 13.964/19, con base en bibliografías académica-científicas. Para ello, adoptó un abordaje de naturaleza cualitativa, ya que buscó analizar el contexto subjetivo del referido fenómeno, esto es, sus aspectos culturales, históricos, humanísticos, de valores y percepciones, que no son medibles. En cuanto a la clasificación de sus objetivos, estos fueron exploratoriosnarrativos, explorando ese contexto temático, relatando y discutiendo los hallazgos literarios.

Para el procedimiento de levantamiento de datos, se utilizó la técnica de revisión de literatura, dada por la determinación de las palabras clave: Cadena de Custódia, Derecho Processual Penal, Ley n. 13.964/2019, Seguridad de Datos y Tecnologías de Ponta, cruzadas entre sí por medio del término "and" que integra el método booleano de recolección objetivando

el refinamiento de los materiales. Se aplicaron los criterios de inclusión que consideraron: artículos físicos y digitales de tipo académico, científico y técnico con recorte temporal de 2015 a 2026, salvo legislaciones y normativas legales, publicados en el idioma portugués. Para la exclusión: trabajos con acceso apenas al resumen o sin disponibilidad del texto completo; estudios redactados en idiomas que no los determinados; investigaciones que fuyan de la temática central propuesta, y; duplicidad del trabajo en las fuentes de recolección analizadas.

Como fuentes de recolección fueron usadas la base de datos del CAPES y de Google Académico y plataformas de la SciELO y de entidades jurídicas diversas. El procedimiento analítico del proyecto siguió las etapas: 1) lectura de datos básicos como título, resumen y resumen; 2) descarte con base en los criterios de exclusión; 3) compilación de los materiales efectivamente escogidos en planilla Excel a partir de las variantes: autor/año y título; tipo del artículo y local de publicación; objetivos; resultados y conclusiones, para facilitar sus accesos e identificar las citas aplicadas; 4) lectura integralizada de los artículos restantes; 5) análisis de los resultados y discusiones comparativas entre los diversos autores.

4. Resultados y discusión

Las literaturas estudiadas, en general, identifican que la promulgación de la Carta Magna de 88 (Brasil, 1988) enfocada en la organización política democrática en Brasil, configura un marco histórico de total importancia, considerando que además de institucionalizar una nueva doctrina a la organización y gestión de la seguridad pública en Brasil, también estimuló la promulgación de una serie de legislaciones y reglamentos, así como el uso de tecnologías de punta en ese ámbito, las cuales experimentan elevados y continuos riesgos a sus seguridad de datos.

Con base en ello, el fenómeno de los desafíos a la seguridad de datos de la CdC de pruebas criminalísticas, sean ellas físicas o digitales y archivadas, esto es que componen la CdcPP, CdCPD y CCDA, especificadas particularmente por Matida (2020), Motta (2022), Gava y Flores (2023) y Fischer (2025), representan una condición estructurada sobre un modelo de defensa técnica con vistas a garantizar sus autenticidads, integridads, confiabilidads y mesmidades. Estos principios del DPP y del CPP son imprescindibles para los análisis periciales, como defienden también los estudios de Stecker y Damian (2021), Magnus y Comploier (2021), Lima y Romanelli (2023), Souza (2022) y Ramalho et al. (2023), Marques y Barbosa (2025), Pereira y Torres (2025) y Silva y Lopes (2025).

Con relación a esos principios, se vio claramente que la CdC es amplia, compleja y sujeta a numerosos desafíos, especialmente en lo que se refiere a la seguridad de datos de las tecnologías de punta aplicables a las CdCPD y CCDA, conforme discutido por Stecker y Damian (2021), Motta (2022), Gava y Flores (2023) y Silva y Lopes (2025), entre otros. Se notó ser común a las literaturas analizadas, la confirmación de la necesidad creciente a la implementación de esa evolución tecnológica para el alcance de los principios arriba revelados, estos, dirigidos de las diez etapas conferidas a las cadenas de custodias de pruebas criminales, con énfasis a las TICs y a los dispositivos de ciberseguridad.

A pesar del estudio no haberse profundizado en las tecnologías aplicables a las CdCPD y CCDA, fue verificado que Brasil cuenta con una diversidad de leyes y normativas en la regencia de procedimientos cabibles a sus estructuras, y que involucran etapas desde la identificación hasta el descarte de las evidencias en juicio. En esto, se destaca el art. 4° de la LGPD (Brasil, 2018) que generó la EC n. 115/22 (Brasil, 2022) fundamentada en tres directos básicos garantizados a los ciudadanos por la CF de 88: la autodeterminación informativa que trata del autocontrol de datos personas a cada brasileño; el crimen de invasión de dispositivo informático que prima por el derecho anterior y; la exigencia de ley específica correspondiente en ese caso, a la EC 115/22.

Estas garantías también se rigen en el Art. 154-A del CP (Ley no 14.155/21) (Brasil, 2021), por la Ley n. 13.964/19 (Brasil, 2019), y demás legislaciones y normas nacionales e internacionales pertinentes al uso de tecnologías en el DPP. En la concepción de Abreu; Cardoso y Passos (2022), Santos (2022) y Pereira y Torres (2025), la promulgación de la Ley n. 13.964/19 es esencial a la minimización y combate a la corrupción en todas sus posibilidades, modernizando el CPP y potencializando las CdCPD y CCDA. Uno de los principales puntos regido por esa Ley se asocia a la licitude de las pruebas, esto es, de su veracidad y preservación iniciadas en el ambiente de origen, vestígio(s) del crimen, recolección, almacenamiento, transporte, catalogación y guarda. Esas etapas van al encuentro de lo que resumió en el Cuadro 2. Reunidas, son cruciales para los resultados periciales.

Se verificó adicionalmente, que las cadenas de custodia digital y digital arquivística, son sustentadas sobre teorías específicas que para Abreu; Cardoso y Passos (2022), involucran la ilegalidad o ilicitude de la prueba; la ocurrencia de nexo de causalidad con la misma dentro de los parámetros regidos por la Ley n. 11.690/08 y art. 157 § 1o y 2o del CPP, y; la flexibilidad de la ilicitud de pruebas a veces inevitable. Esa realidad marca las tecnologías de punta como instrumentos cada vez más indispensables a la CdCPD y a la CCDA.

En ese proceso teórico-analítico, se identificaron los aspectos:

actuación y responsabilidad pericial; fraude procesal, quiebras de sigilo; comprometimientos de la verdad; garantía de preservación de pruebas; recomendaciones archivísticas, todas pertinentes a la estructura de la CdCPD y CCDA, que mientras sistemas que controlan la custodia de pruebas criminales de forma digital, necesitan actuar en consonancia con la PDS y su gestión, como discutido por Gava y Flores (2023).

En lo que se refiere a las quiebras de la cadena de custodia, autores como Alves y Bezerra (2023), Fischer (2025) y Marques y Barbosa (2025) presentan y discuten recursos y agravios regímenes de divergentes jurisprudencias del STJ en nivel nacional, exponiendo las divergencias en la concepción del ordenamiento jurídico sobre la licitude y nulidad de pruebas digitales con foco en la admisión o no de sus convalidaciones.

Generalmente, la Magistratura comprende que las pruebas digitales de la CdC requieren obligatoriamente los registros debidos conducidos de forma cronológica y de responsabilidad al trámite de la evidencia criminal. Esta condición legal implica una serie de posibilidades que abren brecha a la Ley n. 13.964/19, identificadas en el Cuadro 4 de esa investigación, y que fueron resumidos en el Cuadro 5, dando énfasis a los problemas con la seguridad de datos.

Cuadro 5 - Principales lagunas en la CdCPD y en la CCDA que impactan el PA

Lacuna	Caracterización	Autor/año
Fraudes arquitectónicos, secreto y compartir datos	Si no apuradas en tiempo, modifican los resultados de procesos penales. Impactaron los objetivos de la Ley n. 13.964/19.	Stecker y Damian (2021); Santos (2022); Gava y Flores (2023); Lima y Romanelli (2023); Pereira y Torres (2025)
Producción de pruebas y su control por la CdCPD y CCDA	Puede ocurrir cierta ruptura en ese proceso, comprometiendo los principios básicos que orientan la CdC digital como un todo.	Pereira y Torres (2025); Silva y Lopes (2025); Cavalcanti e Silva (2026)
Problemas de infraestructura y recursos	Padronización en los procedimientos; recursos humanos calificados; tecnologías de rastreo; comunicabilidad entre los sectores; divergencias socioeconómicas entre estados y municipios de la federación.	Gava y Flores (2023); Lima y Romanelli (2023); Pereira y Torres (2025); Silva y Lopes (2025); Cavalcanti e Silva (2026); Souza (2026)
Ilegalidad del uso de prints de pantallas	WhatsApp y medios sociales, que poseen el estatus de prueba polémica.	Motta (2022); STJ (2024); STJ (2026)

Fuente: Adaptado por el autor (2026).

Discutiendo el visto en el Cuadro 5, se verificó que los fraudes modifican la autenticidad de la prueba, sin embargo, son validados aspectos como documentación irregular y/o ausencia pericial, dependiendo del entendimiento del juez. Indo al encuentro de esa realidad, existen los factores sigilo y compartir datos, que requieren procedimientos estratégicos, previamente postulados y estandarizados, cuyos procedimientos internos y externos, deben ser efectivos solamente con personal autorizado y, calificado y entre departamentos integrados.

En el entendimiento jurídico del Exmo. Ministro Ribeiro Dantas del STJ junto al recurso de Habeas Corpus RHC n. 77.836/2023, es que el objetivo de la CdC en garantizar el proceso

legal y sus recursos afines a todo y cualquier acusado, como herramienta de defensa, contradicciones y derechos a la licitude de la prueba a la que ampliamente hace jus, se apoya en el alcance del instituto al defender los trámites de la prueba "[...] hasta su análisis por el magistrado, siendo cierto que cualquier interferencia durante el procedimiento puede resultar en su insistencia" (STJ, 2023, p.1).

Las pruebas digitales, en la concepción de Stecker y Damian (2021, p.11) se tornan esenciales una vez que "[...] sin una potencia tecnológica igualitaria, entre acusación y defensa... el proceso penal como ficción es un vaciado democrático". Por lo tanto, la admisión de la prueba es cuestionable, considerando su valorización a los autos. Esto es una incorrencia común frente a la inadecuación de recursos infraestructurales y de capital humano calificado, lo que se suma, a los problemas de disparidades geoeconómicas comunes al territorio brasileño.

Lima y Romanelli (2023) defienden la cuestión de la falsedad de la fuente o de su documentación, que precisa obligatoriamente ser tratada como incidente con imputación de carga probatoria a quien de derecho, esto pues, esa condición tiende a afectar la materialidad del vestígio. Irregularidades documentales de la CdC y/o ausencia de perito, no impactan factores de licitud o legitimidad, pero, deben ser ponderadas por el jurídico para que haya fuerza probatoria y circunstancial de la prueba. Esto se da a través de su autenticación que confiere su veracidad desde el origen, y que solamente ocurre por el análisis del conjunto de ítems dispuestos en los autos.

Esto puesto, aclaramos que la producción y el examen de la prueba, son elementos imprescindibles al enfrentamiento eficaz de la macrocriminalidad existente en la actualidad perseguida por las disposiciones del PA. En esa perspectiva, Cavalcanti e Silva (2026) enfatizan que la CdC solamente alcanza eficazmente sus propósitos legales, al seguir rigurosamente las etapas dispuestas en el art. 158-B del CPP, reforzadas por los arts. 158-A al 158-F de la Ley. n. 13.964/19. Eso significa que el proceso de identificación y recogida de la prueba, necesita de forma obligatoria, ser conducido por un agente público especializado, que verifica el potencial del elemento a ser insertado en la CdC, una vez ser él el profesional que evalúa la relación directa entre vestígio y infracción penal. La súmula 361 del STF (2026) deja claro que: (i) aplicación a expertos no oficiales – la validez se vuelve nula conforme regula el § 1o del art. 159 del Código de Procedimiento Penal (CPP) cuando la ausencia de perito oficial; (ii) inaplicabilidad a expertos oficiales (servidores federales y estatales) – bajo el entendimiento de que la firma de un único experto, caracteriza la validez del laudo; iii) Impedimiento por Participación Previa: el texto original pretende evitar conflictos de interés, impidiendo que el mismo experto que actuó en la aprehensión de la prueba (p. ej., aprehensión de drogas) sea el

único a laudar el material, garantizando imparcialidad. Por lo tanto, aunque el enunciado de la súmula mantenga la regla de nulidad para exámenes realizados por un solo experto, es relativizada para expertos oficiales, siendo el laudo firmado por uno de ellos considerado válido.

Por último, en cuanto a la ilegalidad del uso de prints de pantallas como las de WhatsApp y los medios sociales, las discusiones giran en torno al entendimiento jurídico sobre el envío y la exclusión de mensajes de forma libre, por quien envía y/o recibe, sin que haya rastro o almacenamiento de las mismas, lo que tiende a invalidar su posibilidad de evidencia criminal. El STJ (2023) no admite ningún tipo de prueba digital sin el debido registro relativo a los procedimientos adoptados por la policía, objetivando preservarse la integridad, autenticidad y confiabilidad de los componentes en esas condiciones.

Contextualizando con lo anterior, ambos Agravos citados en el transcurso de la fundamentación teórica, atestiguan que el ordenamiento jurídico en Brasil, no admiten condenas sustentadas por vestigios de origen no confirmada y periciada, una vez ser obligatoria la garantía de la fidedignidad de lo que se presenta en juicio. De ese modo, todos los desafíos y garantías legales identificados en este estudio, refuerzan la protección jurídica y la necesidad de la seguridad de datos como forma de eliminar la exigencia de violación indebida al mecanismo de seguridad, ampliando la amplitud legal que circunda la CdCPD y la CCDA.

5. Consideraciones finales

Para responder el problema directriz de esta revisión bibliográfica, indagando sobre la estructura y desafíos de la CdCPD y CCDA tangibles a la seguridad de datos para la preservación de las pruebas periciales a partir de las legislaciones afines y, en especial a las disposiciones de la Ley n. 13.964/19, los análisis teóricos permiten afirmar que las hipótesis señaladas como sus respuestas, eran ciertas, eso pues, quedó esclarecido la amplitud y complejidad que envuelve ese fenómeno, tanto en términos legales como de recursos para que las finalidades de ambas las vertes de la CdC como del PA, sean efectivamente alcanzadas.

Por lo tanto, los objetivos generales y secundarios que objetivaron abordar las características, relevancia y aspectos desafiantes a la seguridad de datos de las pruebas criminales integradas a la cadena de custodia del DPP, fueron alcanzados, considerando el conocimiento recaudado sobre principios, teorías, etapas, preservación y custodia de sus archivos y lagunas probables dejados por la Ley n. 13.964/19.

Si hizo posible, la extensión de conocimientos conceptuales y aplicaciones del temo custodia, donde se conocieron de forma más amplia, las directrices legales que rigen el uso de las tecnologías de punta aplicables a ese Instituto del DPP. Los desafíos hipoteticamente discurridos en la introducción y que envuelven los factores sigilos, búsqueda y aprehensión de pruebas, preservación/alteración del objeto y del ambiente periciado, derechos y deberes legales, estructuras de procesos fallas, fraudes, ilegalidad de pruebas oriundas de pantallas sin el debido registro policial o embasamiento leal suficiente y, todo lo que envuelve la quiebra de la CdC digitalizada, fueron analizados y comprobados como posibles elementos de impacto a los resultados periciales y jurídicos, sumando la cuestión de los fraudes, quiebras en la custodia e ilegalidad de pruebas.

El estudio bibliográfico no encontró lagunas en asociación a los desafíos de seguridad de datos en la CdC digitalizada, sin embargo evidenció baja producción de investigaciones académica-científicas que presenten las tecnologías de forma detallada dentro del sesgo jurídico. Delante de eso, se concluye que hay una inmensidad de saberes jurídicos que involucran el tema propuesto, reafirmando con eso, su relevancia, así como la necesidad de dar continuidad a nuevos estudios, considerando que el Paquete Anticrime es todavía una novedad, a pesar de sus 7 años de establecimiento. El PA se enfrenta cotidianamente con numerosos obstáculos, entre los cuales lo que estructuran la CdC digital y digital arquivística, donde la quiebra, fraude y secreto de sus archivos es imprescindible para la seguridad de datos y los resultados de los procesos penales.

Referencias

ABREU, Lauro Pereira; CARDOSO, Jaqueline Ribeiro; PASSOS, Fábio Presoti. El análisis de la necesidad de predecir la figura del juez contaminado en el ordenamiento jurídico. In: Liberas Derecho, Belo Horizonte, Vol. 3, n. 1, p. 1-33, jan./jul. 2022.https://periodicos.famig.edu.br/index.php/direito/article/view/209/136.Acceso a 12 de abr. 2026.

ALVES, Ani H. da Silva; BEZERRA, Thiago J. de S. Lima. La producción de pruebas en el proceso penal brasileño: un análisis acerca de la nulidad por la inobservancia de las normas de la cadena de custodia. In: RECIMA21 - Ciencias Exatas y de la Tierra, Sociales, de la Salud, Humanas y Ingeniería/Tecnología. Vol. 4, n. 9, 2023.https://recima21.com.br/recima21/en/article/view/4033/2901.Acceso en 07 de set. 2026.

BRASIL. Ley n. 3.689 de 3 de octubre de 1941: Código de Procedimiento Penal. Río de Janeiro: Presidencia de la República. D.O.U. de 13.10.1941 y rectificado el 24.10.1941.https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm.Acceso a 20 de abr. 2026.

BRASIL. Ley n. 12.965 de 23 de abril de 2014: Establece principios, garantías, derechos y deberes para el uso de Internet en Brasil. Brasilia, DF: Presidencia de la República.

D.O.U. de 24.4.2014.https://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm.Acceso a 20 de abr. 2026.

BRASIL. Ley n. 13.709 de 14 de agosto de 2018: Dispone sobre la protección de datos personales y modifica la Ley no 12.965, de 23 de abril de 2014 (Marco Civil de Internet). Ley General de Protección de Datos Personales (LGPD). Brasilia, DF: Presidencia de la República. D.O.U. de 15.8.2018, y republicado parcialmente en 15.8.2018 - Edición extra.https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.Acceso a 21 de abr. 2026.

BRASIL. Ley n. 13.964 de 24 de diciembre de 2019: Mejora la legislación penal y procesal penal. Brasilia, DF: Presidencia de la República. D.O.U. de 30.04.2021.http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.Acceso en 03 de abr. 2026.

BRASIL. Guía de Normas ISO y NBR para Seguridad de la Información. (online), 2026.https://ufdpar.edu.br/ufdpar/guia-de-normas-iso-e-nbr-para-seguranca-dainformacao.Acceso en 22 de abr. 2026.

CAVALCANTI, Douglas Rodrigues; SILVA, Thiago Henrique Costa. Rompie la cadena de custodia y la consecuencia para el debido proceso legal: una revisión de la literatura. In: Atâtót - Revista Interdisciplinar de Derechos Humanos de la UEG. Vol. 7, n. 1,2026.https://revista.ueg.br/index.php/atatot/article/view/16405.Acceso en 22 abr. 2026.

CONSEJO NACIONAL DE ARQUIVOS. Resolución n. 51 de 21 de agosto de 2023: Dispone sobre las "Diretrizes para la Implementación de Repositorios Arquivísticos Digitales Confiables" – Versión 2. Brasilia, DF: Ministerio de Gestión e Innovación en Servicios Públicos – CONARQ. 2023.https://www.gov.br/conarq/pt-br/legislacaoarquivistica/resolucoes-do-conarq/resolucao-conarq-no-51-de-25-de-agosto-de-2023.Acceso a 12 de ago. 2026.

CONSEJO NACIONAL DE JUSTICIA – CNJ. Audiencias de custodia completan 10 años con datos inéditos. (online) 24 de fev. 2025.https://www.cnj.jus.br/audiencias-de-custodia-completam-10-anos-com-dados-ineditos/.Acceso a 12 de abr. 2026.

FISCHER, Douglas. La cadena de custodia implica la medición de la mesmidad o fiabilidad de la prueba, no su invalidada/nulidad. (online), 11 set. 2025.https://temasjuridicospdf.com/acadeia-de-custodia-envolve-a-afericao-da-mesmidade-ou-fiabilidade-da-prova-nao-a-suainvalidade-nulidade/.Acceso en 05 de set. 2026.

GAVA, Tânia Barbosa Salles; FLORES, Daniel. Problematizando la Post-Custódia con la contemporaneidad de la cadena de Custódia Digital Archivística compartida y distribuida en la Preservación Digital Sistémica. In: InCID - Rev. Cient. Inf. y Doc. Ribeirão Preto, Vol.13, n. 2, p. 222-243, set. 2022/fev. 2023.https://www.academia.edu/95019816/Problematizando_a_P%C3%B3s_Cust%C3%B3dia com a contemporaneidad da Cadeia de Cust%C3%B3dia Digital Arquiv%C3% ADstica comptillada e distribu%C3%ADda na Preserva%C3%A7%C3%A3o Dig ital Sist%C3%AAmica. Acceso a 21 de abr. 2026.

HENRIQUES, Antonio; MEDEIROS, Juan Bosco. Metodología Científica de la Investigación Jurídica. 9a Ed. Ebook Kindle. São Paulo: Atlas, 2017, 2.9 MB, 413 p.

LIMA, Pablo Guillermo Carolis; ROMANELLI, Leonardo Leonel. La cadena de custodia a partir de la reforma del CPP: actividad probatoria de segundo grado. In: Revista del Ministerio Público Militar. Vol. 48, n.34, p. 1-38, 2023.https://revsita.mpm.mp.br/rmpm/article/view/81/75.Acceso a 21 de abr. 2026.

LUCAS, Thiago José; FIGUEIREDO, Inês S. de; TOJEIRO, Carlos; ALMEIDA, Alex

M.G. de. Comprehensive Survey on Ensemble Learning-Based Intrusion Detection Approaches in Computer Networks. In: IEEE Acess. Vol. 11, p. 122638-676, Jan. 2023.https://www.researchgate.net/publication/375103711_A_Comprehensive_Survey_on_Ensemble Learning-based Intrusion Detection Approaches in Computer Networks.

MAGNO, Levy E; COMPLOIER, Mylene. Cadena de custodia de la prueba penal. In: Cuadernos jurídicos. São Paulo, Año 22, no 57, p. 195-219, jan./mar.2021.https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/cj_n57_10_cadeIba %20de%20cust%C3%B3dia.pdf?d=637437206976264894. Acceso en 05 de set. 2026.

MARQUES, Thaysa Mendes; BARBOSA, Karlos Alves. Cadena de custodia de la prueba digital en el proceso penal. 2021, 18 P. Artículo de Conclusión de Curso (Bacharelado en Derecho). Facultad de Derecho. Universidad Federal de Uberlandia. 2021.https://repositorio.ufu.br/bitstream/123456789/47148/2/Cadeiadecust%C3%B3dia.pdf.Acceso en 04 de set. 2026.

MATIDA, Janaina. La cadena de custodia es condición necesaria para reducir los riesgos de condenas de inocentes. In: Boletín OBCCRIM. Año 28, n.331, jun. 2020.https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/541/61.Acceso en 05 de set. 2026.

MOTTA, Eduardo Titão. Cadena de custodia de la prueba digital y la ilegalidad del uso de prints como elementos de prueba en el proceso penal. In: Biblioteca del Instituto Brasileño de Derecho Penal Económico – IBDPE. 31 de mai. 2022.https://ibdpe.com.br/cadeia-de-custodia-da-prova-digital-e-a-ilegalidade-do-uso-deprints-de-tela-como-elementos-de-prova-no-processo-penal/.Acceso a 12 de abr. 2026.

PERERA, Leticia Rodrigues; TORRES, Leonardo Guimarães. Ley 13.964/2019 y la cadena de custodia: avances y desafíos en la preservación de la prueba penal. In: Revista Iberoamericana De Humanidades, Ciencias E Educación. Vol.11, n.10, p. 4487– 4497, 2025.https://periodicorease.pro.br/rease/article/view/21714.Acceso en 16 de abr. 2026.

RAMALHO, Thales Novais et al. Importancia de la cadena de custodia en la justicia brasileña: la garantía de la integridad de la prueba y el papel decisivo en la conducción de procesos judiciales. In: Revista Iberoamericana de Humanidades, Ciencias y Educación. São Paulo, v.9.n.02. fev. 2023.https://periodicorease.pro.br/rease/article/view/8412.Acceso en 04 de set. 2026.

SANTOS, Damião de Sousa. Ley n. 13.964/2019 – Brasil Paquete Anticrime. In: Educación, Salud y Sociedad: investigaciones, desafíos y perspectivas futuras. 1 ed. Capítulo 4. Río de Janeiro: Epitaya, p. 85 – 118, 2022.https://portal.epitaya.com.br/index.php/ebooks/article/view/514/395.Acceso en: 19 de abr. 2026.

SILVA, Cristiane V. da; LOPES, José A. Bezerra. El uso de pruebas digitales en el proceso penal. In: Revista Iberoamericana de Humanidades, Ciencias y Educación. São Paulo, v. 11, n. 5, mayo. 2025.https://periodicorease.pro.br/rease/article/view/19071.Acceso en 04 de set. 2026.

SOUZA, Ricardo Calmona. La Enmienda Constitucional no 115 y el derecho de protección de datos en la persecución penal: la (des)preocupación por la necesidad de una “LGPD penal”. In: DOUTRINA - Revista de Derecho de la Defensoría Pública del Estado de Río de Janeiro. No 32, 2022.https://defensoria.rj.def.br/uploads/imagens/97f7a07e38234ad09e7c42a5292a0432.pdf. Acceso en 05 de set. 2026.

STECKER, Matias Hillesheim; DAMIAN, Felipe Bochi. Cadena de custodia del vestígio digital: la tecnología como potencia defensiva. 2021, 13 p. Artículo (Mestrado en Ciencias Criminales y Especialización en Ciencias Penais). Pontificia Universidad Católica de Rio Grande do Sul – PUV/RS. Porto Alegre, RS, 2021.https://editora.pucrs.br/anais/congresso-internacional-de-cienciascriminais/assets/edicoes/2021/arquivos/40.pdf.Acceso a 12 de abr. 2026.

SUPERIOR TRIBUNAL DE JUSTICIA- STJ. Agravo en Recurso Especial n. 1.847.296-PR (2021/0049381-6). Brasilia, DF: Relator: Ministro Reynaldo Soares da Fonseca. 2021.https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2073099&num registro=202100493816&data=20210628&peticao numero=20 2100584037&formato=PDF. Acceso en 04 de set. 2026.

SUPERIOR TRIBUNAL DE JUSTICIA – STJ. La cadena de custodia en el proceso penal: del Paquete Anticrimen a la jurisprudencia del STJ. (online), 23 de abr. 2023.https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/23042023-Acadeia-de-custodia-no-processo-penal-do-Pacote-Anticrime-a-jurisprudencia-doSTJ.aspx.Acceso a 12 de abr. 2026.

SUPERIOR TRIBUNAL DE JUSTICIA – STJ. AgRg no HC No 828054 - RN (2023/0189615-0). Natal, RN: Relator: Ministro Joel Ilan Paciornik. Abr. 2024.https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento tipo=integra&documento sequencial=242041837&registro numero=202301896150&peticao numero=202300906480&publicacao data=20240429&formato=PDF. Acceso en 06 de set. 2026.

SUPERIOR TRIBUNAL DE JUSTICIA – STJ. AgRg no HC 1014212 / ES Agravo Régimenntal en Habeas Corpus 2025/0231341-3. Victoria, ES: Ministro Carlos Pires Brandão. Fev. 2026.https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%28%28AGRHC+INPATH%28CLAS%29+OR+%22AgRg+no+HC%22+INPATH%28CLAP%29%29+AND+1014212+INPATH%28NUM%29%29+OR+%28NEAR%28%28%28AGRHC+OR+%22AgRg+no+HC%22%2C1014212%2CTRUE%29+INPATH%29%29%29. Acceso en 06 de set. 2026.

SUPREMO TRIBUNAL FEDERAL – STF. Aplicación de la Súmula no 361. Brasilia, DF. 2026.https://portal.stf.jus.br/jurisprudencia/sumariosumulas.asp?base=30&sumula=2737.Acceso a 21 de abr. 2026.