
ARTÍCULO

Propuesta de Forensia informacional en los archivos audiovisuales digitales televisivos

Proposal for Informational Forensics in digital audiovisual television archive

Jorge Caldera-Serrano

Departamento de Información y Comunicación, Facultad de Ciencias de la Documentación y la Comunicación,
Universidad de Extremadura, Badajoz

jcalser@unex.es, <https://orcid.org/0000-0002-4049-1057>

Resumen: En un contexto de creciente digitalización, manipulación de contenidos y proliferación de narrativas mediáticas controladas, este artículo propone y desarrolla el concepto de forensia informacional como un campo emergente en la intersección entre la ciencia de la información, la archivística y la investigación forense digital. A través de una revisión crítica de conceptos como autenticidad documental, trazabilidad informativa y análisis forense, se plantea un marco conceptual y metodológico orientado a salvaguardar la integridad, veracidad y transparencia de los archivos digitales, con especial atención a los archivos audiovisuales de televisión. Se analiza cómo estos archivos, debido a su valor testimonial, son especialmente vulnerables a procesos de censura, manipulación narrativa y omisión intencionada de información. El artículo propone una mirada forense que permita detectar vacíos documentales, reconstruir contextos suprimidos y preservar versiones auténticas, incorporando prácticas propias del peritaje documental, la diplomática y la documentología forense. Se ha utilizado IA para revisión y mejora de la redacción.

Palabras clave: forensia informacional; archivos audiovisuales; veracidad documental; trazabilidad informativa; archivística digital.

Abstract: *In a context of increasing digitalization, content manipulation, and the proliferation of controlled media narratives, this article proposes and develops the concept of informational forensics as an emerging field at the intersection of information science, archival studies, and digital forensic investigation. Through a critical review of concepts such as documentary authenticity, informational traceability, and forensic analysis, the paper outlines a conceptual and methodological framework aimed at safeguarding the integrity, truthfulness, and transparency of digital archives, with a particular focus on television audiovisual archives. It examines how these archives, due to their testimonial value, are especially vulnerable to processes of censorship, narrative manipulation, and intentional omission of information. The article advocates for a forensic-informed perspective that enables the detection of documentary gaps, the reconstruction of suppressed contexts, and the preservation of authentic versions, incorporating practices drawn from documentary expertise, diplomatics, and forensic documentology. AI has been used for the revision and improvement of the writing.*

Keywords: *informational forensics; audiovisual archives; documentary veracity; informational traceability; digital archiving.*

Recibido: 06-07-2025 / **Aceptado:** 27-08-2025 / **Publicado:** 18-06-2026

Cómo citar: Caldera-Serrano, J., (2026). Propuesta de Forensia informacional en los archivos audiovisuales digitales televisivos. *Revista Española de Documentación Científica*, 49(1), 1868. <https://doi.org/10.3989/redc.2026.1.1868>

Copyright: © 2026 CSIC. Este es un contenido de acceso abierto diamante distribuido bajo los términos de la licencia de uso y distribución Creative Commons Reconocimiento 4.0 Internacional (CC BY 4.0).

1. INTRODUCCIÓN

En la era digital contemporánea, la producción y circulación de información ha alcanzado una escala sin precedentes, transformando radicalmente los procesos de creación, almacenamiento, acceso y reutilización de contenidos documentales. Esta expansión ha traído consigo importantes desafíos en cuanto a la veracidad, la autenticidad y la trazabilidad de la información, especialmente en formatos digitales complejos como los archivos audiovisuales. Estos documentos, al conjugar imagen, sonido y contexto narrativo, poseen un alto valor testimonial y cultural, pero también están expuestos a múltiples formas de manipulación, omisión o recontextualización que pueden alterar su integridad y dificultar su interpretación crítica. En este escenario, la necesidad de desarrollar metodologías que permitan no solo preservar estos contenidos, sino también validar su autenticidad y rastrear su historia documental, se vuelve urgente.

La creciente preocupación por la desinformación, los discursos mediáticos sesgados, el uso de técnicas de edición avanzadas -como los *deepfakes*- y la censura encubierta en plataformas digitales, ha colocado en el centro del debate la cuestión de la confianza en los documentos digitales. Los archivos audiovisuales de televisión, en tanto repositorios institucionales de memoria, desempeñan un papel crucial en la configuración del relato histórico y cultural de las sociedades contemporáneas. No obstante, su fiabilidad como fuentes primarias puede verse comprometida si no se cuenta con mecanismos adecuados para garantizar su integridad documental. En este contexto, surge la necesidad de enfoques interdisciplinarios capaces de articular herramientas conceptuales y técnicas provenientes de la ciencia de la información, la archivística, la diplomática documental y las ciencias forenses digitales (Iacovino, 2004).

Desde la archivística, se han desarrollado múltiples estrategias orientadas a la preservación y descripción de documentos audiovisuales, priorizando su organización, conservación y acceso. Sin embargo, estas prácticas no siempre han incorporado mecanismos de análisis crítico sobre la construcción, circulación y posible manipulación de dichos contenidos (Schüller, 2019). Por su parte, la ciencia de la información ha aportado marcos teóricos para estudiar la producción y difusión del conocimiento, pero sus aplicaciones forenses siguen siendo incipientes (Post y Chassanoff, 2021). En paralelo, disciplinas como la documentología forense, la diplomática y la criminalística han desarrollado técnicas específicas para la verificación de la autenticidad y la detección de falsificaciones en documentos. No obstante, estas aproximaciones se han aplicado principalmente en contextos judiciales, administrativos o históricos, sin una atención específica a los archivos audiovisuales contemporáneos y sus particularidades como objetos de análisis (Duranti y Rogers, 2018).

A partir de esta confluencia disciplinar, proponemos el concepto de forensia informacional como un campo emergente orientado al estudio y aplicación de métodos para analizar, preservar y validar la autenticidad de la información en entornos digitales complejos. Esta noción integra saberes provenientes de la archivística forense (en gran medida en desarrollo), la diplomática moderna, la ciencia de datos, la verificación audiovisual y la gestión documental crítica, con el objetivo de desarrollar una mirada pericial sobre la información digital que trascienda la mera conservación física o digital de los archivos. En lugar de centrarse únicamente en los aspectos técnicos de la preservación, la forensia informacional se orienta hacia la reconstrucción del recorrido informativo de un documento, el análisis de su contexto de producción y modificación, y la detección de posibles estrategias de omisión, censura o manipulación.

En este artículo, se propone una primera delimitación teórica y metodológica del concepto de forensia informacional, con especial énfasis en su aplicación al ámbito de los archivos audiovisuales de televisión. Se parte de la premisa de que estos archivos no son únicamente depósitos neutros de contenidos, sino dispositivos discursivos que pueden reflejar, reproducir o silenciar narrativas determinadas. En este sentido, aplicar una mirada forense a este tipo de colecciones implica cuestionar críticamente la manera en que se construyen, describen, conservan y difunden los documentos audiovisuales en los entornos institucionales. Este trabajo pretende contribuir a la apertura de una nueva línea

de investigación que responda a las crecientes demandas sociales, científicas y éticas en torno a la fiabilidad de los documentos digitales, promoviendo un enfoque que combine el rigor técnico de las ciencias forenses con la sensibilidad crítica de la ciencia de la información y la archivística.

2. OBJETIVOS, OBJETOS Y METODOLOGÍA

Este artículo tiene como propósito principal sentar las bases teóricas y metodológicas de un nuevo campo de estudio que hemos denominado forensia informacional, entendida como una propuesta interdisciplinar orientada a analizar la autenticidad, la trazabilidad y la integridad de los documentos digitales desde una perspectiva informacional y forense. En concreto, se plantean dos objetivos: (1) proponer una definición operativa del concepto de forensia informacional, fundamentada en la convergencia entre la ciencia de la información, la archivística digital y la investigación forense documental y (2) explorar su aplicabilidad al campo de los archivos audiovisuales digitales de televisión, con especial atención a los procesos de preservación, circulación, censura o manipulación de estos documentos.

El objeto de estudio seleccionado son los archivos audiovisuales digitales de televisión, definidos como colecciones institucionales o corporativas de contenidos audiovisuales generados en contextos televisivos, que se encuentran almacenados, organizados y, en muchos casos, digitalizados para su preservación o reutilización. La elección de este objeto responde a varias razones. En primer lugar, estos archivos poseen un valor documental y testimonial significativo, al constituir una fuente primaria para la construcción de narrativas históricas, políticas, culturales y sociales. En segundo lugar, la naturaleza híbrida y compleja de los documentos audiovisuales (imagen, sonido, metadata, temporalidad) plantea desafíos específicos en términos de autenticidad, lo que los convierte en un campo fértil para la experimentación conceptual y metodológica. En tercer lugar, su circulación actual, tanto en plataformas abiertas como en repositorios institucionales cerrados, los expone a riesgos de edición no controlada, ocultamiento selectivo o recontextualización interesada, lo cual exige nuevas formas de análisis que vayan más allá de los enfoques archivísticos tradicionales.

La metodología empleada en este trabajo se enmarca en una estrategia cualitativa y exploratoria propia de las Ciencias Sociales, adecuada para trabajos teóricos en líneas de investigación emergentes. Se ha llevado a cabo una revisión bibliográfica crítica e interdisciplinar, con consulta sistemática en bases de datos académicas de referencia como Web of Science, Scopus y Google Scholar. Las búsquedas se articularon mediante operadores booleanos y combinaron términos como “forensic information” AND (“digital archives” OR “audiovisual archives”), “documentary authenticity” AND (“television” OR “broadcast archives”), “archival forensics” OR “forensic archivistics”, “deepfake” AND “documentary integrity” AND (“media archives”), e “information traceability” AND “audiovisual content”. A partir de esta revisión, se realizó un análisis teórico-comparativo entre distintas corrientes y disciplinas, con el objetivo de identificar puntos de convergencia, vacíos conceptuales y posibilidades de integración. Las principales disciplinas en las que se han obtenido resultados relevantes incluyen la Archivística Digital, con énfasis en autenticidad y preservación de objetos complejos (Pacheco *et al.*, 2023); la Documentación y Diplomática Forense, orientadas a la validación estructural y contextual de documentos (MacNeil, 2004); las Ciencias de la Información, que aportan marcos críticos para el análisis de circulación y trazabilidad de contenidos (Post y Chassanoff, 2021); y los Estudios de Comunicación y Semiótica Audiovisual, enfocados en el análisis narrativo y discursivo de materiales televisivos (Skowronek, 2014; Unger, 2016). Dentro de cada una se han identificado corrientes como la archivística forense aplicada, los enfoques críticos de la gestión documental, la verificación multimodal en entornos digitales y la teoría crítica de la información, más allá de la vertiente tecnológica del control de manipulación de imágenes. La selección de materiales y enfoques respondió a su pertinencia directa con los objetivos del trabajo y su aplicabilidad a la forensia informacional en archivos televisivos, priorizando investigaciones que aborden riesgos de manipulación, pérdida de trazabilidad y sesgo narrativo. Entre las principales aportaciones destacan la sistematización de procedimientos de control de versiones, el diseño de metadatos enriquecidos y la propuesta de metodologías de verificación cruzada. Como puntos débiles se identifican la nula estandarización de protocolos forensiales aplicados a archivos audiovisuales televisivos y la limitada integración entre técnicas forenses digitales y prácticas archivísticas, lo que

abre lagunas de investigación en el desarrollo de herramientas interoperables y en la formación interdisciplinar de los profesionales del sector. Finalmente, se formula una propuesta conceptual aplicada que describe los ejes fundamentales de la forensia informacional, y se delinearán posibles metodologías de análisis documental forense adaptadas a los archivos audiovisuales televisivos, tales como el estudio de metadatos, el rastreo de versiones, la detección de vacíos documentales o la comparación de coberturas informativas. Esta metodología no busca ofrecer una solución técnica definitiva, sino abrir una vía crítica y operativa para abordar las nuevas problemáticas de veracidad documental en entornos digitales complejos.

3. FORENSIA INFORMACIONAL: DELIMITANDO CONCEPTOS

La necesidad de un enfoque conceptual integrador que permita afrontar los desafíos actuales en torno a la veracidad, la trazabilidad y la autenticidad de la información en entornos digitales ha adquirido una importancia creciente en el marco de las transformaciones tecnológicas contemporáneas. Frente a fenómenos como la manipulación digital, la proliferación de contenidos audiovisuales generados mediante inteligencia artificial o la circulación fragmentada y opaca de documentos electrónicos, resulta urgente revisar críticamente los conceptos clave que han sustentado tradicionalmente la gestión documental, así como explorar sus posibilidades de rearticulación bajo un nuevo paradigma interdisciplinar. En este apartado se abordan los principales términos implicados en esta reformulación —autenticidad documental, trazabilidad de la información, análisis forense digital, archivística digital, diplomática documental, documentología forense y veracidad informativa— con el objetivo de evidenciar la necesidad de una conceptualización transversal que los aglutine: la forensia informacional.

El concepto de autenticidad documental ha sido históricamente uno de los pilares de la archivística y la diplomática (Pacheco *et al.*, 2023). En el entorno analógico, la autenticidad se entendía como la correspondencia del documento con su origen, autoría y contexto de producción, garantizada por su forma externa y los mecanismos institucionales de validación. Sin embargo, en el entorno digital, la autenticidad se vuelve más vulnerable debido a la maleabilidad de los soportes y a la ausencia de huellas físicas. La integridad de un documento digital puede ser comprometida sin dejar rastros visibles, lo que exige nuevas herramientas de verificación basadas en metadatos, firmas digitales, blockchain o tecnologías de trazabilidad. En este sentido, la trazabilidad de la información se convierte en un principio estructurante: alude a la posibilidad de rastrear el origen, las modificaciones y la trayectoria de un documento o dato a lo largo del tiempo (Pacheco *et al.*, 2023). La trazabilidad no solo es clave para garantizar la fiabilidad documental, sino que también constituye un criterio de calidad informativa fundamental en contextos periodísticos, científicos y archivísticos (Gotel *et al.*, 2012).

Por su parte, el análisis forense digital se ha desarrollado como una subdisciplina de la informática forense, centrada en la recuperación, preservación y análisis de evidencias digitales con fines probatorios (Le-Khac y Choo, 2020). Aunque su foco ha estado tradicionalmente en contextos judiciales o criminales, sus métodos —análisis de metadatos, comparación de versiones, detección de alteraciones— son perfectamente aplicables al estudio de documentos digitales desde una perspectiva informacional. Esta expansión metodológica justifica su conexión con la archivística digital, entendida como el campo que estudia la organización, preservación y acceso de documentos electrónicos. La archivística digital, aunque centrada en la gestión institucional de documentos nacidos digitales o digitalizados, debe afrontar ahora nuevos desafíos relacionados con la autenticidad, la manipulación y la veracidad de los fondos documentales, especialmente en colecciones audiovisuales susceptibles de modificación no autorizada o recontextualización maliciosa (Pacheco *et al.*, 2023).

La diplomática documental, disciplina auxiliar de la archivística, se ha ocupado tradicionalmente del análisis crítico de documentos históricos, con el fin de establecer su autenticidad a través del estudio de su estructura, lenguaje, fórmulas y contexto de producción. Si bien su ámbito de aplicación ha sido mayoritariamente el documento histórico, su metodología resulta útil como modelo para abordar la autenticidad documental en el entorno digital (MacNeil, 2004). En la actualidad, algunos de sus

principios han sido retomados por la documentología forense, que se centra en el análisis técnico de documentos contemporáneos (escritos, firmados o electrónicos), especialmente en contextos legales o periciales. Esta disciplina busca establecer la autoría, la antigüedad o la integridad de un documento, utilizando tanto técnicas grafológicas como herramientas digitales de análisis.

En este contexto, resulta pertinente introducir el término archivística forense como una categoría emergente —aunque no formalmente consolidada— que denomina aquellas prácticas que integran saberes archivísticos y métodos forenses para el análisis de documentos digitales en situaciones que requieren verificación rigurosa de autenticidad (Jaillant, 2022). Aunque el concepto no ha sido desarrollado como disciplina autónoma, algunos autores y profesionales han comenzado a utilizarlo en relación con prácticas de auditoría documental, litigios o procesos de verificación institucional. La archivística forense puede considerarse, por tanto, un antecedente directo de la forensia informacional, aunque esta última propone una ampliación de enfoque tanto en lo conceptual como en lo funcional.

La noción de veracidad informativa, por su parte, trasciende el ámbito documental y se sitúa en el núcleo del debate ético y epistémico contemporáneo. En un ecosistema mediático fragmentado, automatizado y susceptible a la desinformación, la veracidad de la información ya no depende únicamente de la autoría o de la intención del emisor, sino también de la trazabilidad de sus fuentes, la integridad de sus soportes y la transparencia de sus procesos de circulación. La veracidad se convierte, así, en un valor operativo y no meramente normativo, que debe ser garantizado mediante herramientas técnicas, criterios analíticos y responsabilidades institucionales (Li y Chang, 2023).

En vista de lo anterior, se propone el concepto de forensia informacional como un nuevo marco teórico y operativo para integrar estas dimensiones. Desde una perspectiva académica, definimos la forensia informacional como el conjunto de métodos, técnicas y criterios aplicados al análisis, preservación y validación de la autenticidad, trazabilidad e integridad de documentos digitales, particularmente en contextos donde se requiere una alta fiabilidad informativa, como archivos, medios de comunicación, bibliotecas digitales o bases de datos científicas. Su carácter es eminentemente interdisciplinar, al nutrirse de la archivística, la ciencia de la información, la investigación forense digital, la diplomática documental y la teoría crítica de la información. En este sentido, la forensia informacional no pretende sustituir estas disciplinas, sino articularlas en un espacio común de análisis y aplicación.

Los ámbitos de aplicación de esta propuesta son amplios y diversos. Puede aplicarse en archivos institucionales, donde la preservación y verificación de documentos digitales es clave para la transparencia administrativa; en repositorios científicos, donde la trazabilidad de los datos y la integridad de las publicaciones constituyen un requisito epistémico; en bibliotecas digitales, que gestionan grandes volúmenes de información susceptible de manipulación; y especialmente en archivos audiovisuales, donde el potencial de alteración mediante tecnologías como los *deepfakes* plantea nuevas amenazas a la autenticidad documental.

A partir de esta conceptualización, se puede delinear un perfil profesional emergente asociado a la forensia informacional. Este profesional, que podríamos denominar perito informacional o analista forense de información, debería poseer competencias en gestión documental digital, análisis forense de datos, auditoría de metadatos, evaluación de integridad informativa y análisis crítico del discurso. Entre sus funciones se incluirían: detectar alteraciones documentales, reconstruir trayectorias informativas, realizar informes periciales sobre la autenticidad de contenidos, identificar vacíos o sesgos en colecciones documentales, y aplicar criterios éticos en la validación de la información. Las herramientas que debería manejar incluirían software de análisis forense, tecnologías de blockchain documental, sistemas de gestión archivística, bases de datos académicas, así como metodologías cualitativas de análisis de contenido. Su actuación ética se fundamentaría en los principios de transparencia, trazabilidad, acceso equitativo a la información y defensa de la integridad documental frente a la manipulación o censura.

La analogía más cercana a este perfil puede encontrarse en la figura del perito documental, que opera en contextos legales para establecer la veracidad o falsedad de un documento (Pacheco *et al.*, 2023) (Moussa, 2021). No obstante, la forensia informacional se diferencia de este enfoque tradicional en su orientación estructural y preventiva: no se limita a actuar *ex post*, como en un juicio, sino que propone un marco teórico y técnico para integrar la veracidad y la trazabilidad como principios de gestión documental cotidiana. En otras palabras, no se trata solo de descubrir la falsedad, sino de construir sistemas informacionales más resistentes a la falsificación y a la opacidad.

En definitiva, ante un ecosistema digital cada vez más complejo y vulnerable, se impone la necesidad de articular un marco conceptual actualizado que permita responder a las nuevas formas de manipulación, censura y circulación opaca de la información. La forensia informacional se presenta como una propuesta innovadora que busca integrar saberes dispersos en una arquitectura común, con vocación tanto analítica como operativa. Su desarrollo puede contribuir decisivamente a fortalecer la fiabilidad informativa en contextos críticos, y a generar nuevas capacidades institucionales, profesionales y tecnológicas para la defensa de la integridad documental en la era digital.

4. FORENSIA INFORMACIONAL EN LOS ARCHIVOS AUDIOVISUALES TELEVISIVOS

El campo de los archivos audiovisuales televisivos representa un terreno particularmente sensible y complejo para la aplicación del paradigma de la forensia informacional. Como conjunto de documentos que contienen testimonios visuales y sonoros de la actualidad, la historia reciente y la construcción mediática de lo real, estos archivos poseen un valor documental, cultural y epistémico de primera magnitud. Sin embargo, su naturaleza digital, su condición de productos mediáticos sometidos a procesos de edición, su circulación fragmentada y su relación estructural con los poderes comunicativos y políticos, los convierten en objetos informacionales especialmente vulnerables a manipulaciones, censuras, distorsiones narrativas y pérdidas de trazabilidad (Shu K. *et al.*, 2020). La forensia informacional, como marco interdisciplinar orientado a garantizar la autenticidad, trazabilidad y veracidad de la información digital, se presenta como una herramienta teórica y práctica de gran utilidad para abordar los desafíos que plantean estos entornos. Este apartado propone un análisis en profundidad de su aplicación a los archivos audiovisuales de televisión, identificando riesgos, procedimientos y posibles impactos.

El archivo audiovisual televisivo constituye una categoría documental con características propias que lo distinguen de otros tipos de archivos institucionales o bibliotecarios. Por un lado, se trata de documentos compuestos por imagen, sonido y su montaje, lo que supone una capa de complejidad semiótica y técnica adicional. Por otro, están generados en un contexto de comunicación masiva, donde los intereses editoriales, comerciales y políticos juegan un papel determinante en la selección, tratamiento y difusión de los contenidos (Caldera-Serrano, 2025). Además, son documentos sometidos a procesos constantes de edición, recontextualización, digitalización y circulación multiplataforma, lo que dificulta su fijación y control.

Estas particularidades convierten a los archivos televisivos en un espacio especialmente propenso a fenómenos de pérdida de autenticidad y de trazabilidad. A diferencia de los documentos textuales tradicionales, cuya alteración suele dejar huellas más fácilmente detectables, los documentos audiovisuales pueden ser modificados de forma imperceptible mediante técnicas digitales avanzadas (por ejemplo, la supresión de fragmentos, la edición del orden narrativo, el cambio de audio o subtítulos, o incluso la sustitución de rostros o voces mediante tecnologías de deepfake) (Zhang, 2022). Estas transformaciones pueden ser tanto accidentales —debido a malas prácticas de conservación, digitalización deficiente o pérdida de metadatos— como intencionales, en contextos de censura, propaganda o reescritura interesada del pasado reciente (Alanazi y Asif, 2024).

La naturaleza mediática de los documentos audiovisuales televisivos introduce una serie de riesgos específicos que deben ser abordados desde una mirada forensial. En primer lugar, la manipulación editorial puede conducir a la omisión de coberturas relevantes, la descontextualización de declaraciones, la construcción de relatos sesgados o la invisibilización de determinados actores sociales (Caled y Silva,

2022). En segundo lugar, existe el riesgo de censura o supresión documental, especialmente en entornos políticos autoritarios o polarizados, donde determinados registros audiovisuales pueden ser eliminados, alterados o sustituidos para proteger intereses ideológicos o borrar huellas de responsabilidad (May, 2023). En tercer lugar, la distorsión narrativa puede producirse a través de la reorganización del archivo, la selección parcial de imágenes o la alteración del orden cronológico, afectando la lectura histórica de los acontecimientos. Finalmente, la pérdida de trazabilidad se presenta como uno de los principales problemas estructurales: la ausencia de metadatos completos, la falta de registros sobre procesos de edición y conservación, y la carencia de sistemas de versionado, dificultan reconstruir la historia documental de un archivo y verificar su autenticidad (Seeger y Chaudhuri, 2015).

Estos riesgos no son meramente hipotéticos. Existen numerosos casos reales que ilustran cómo los archivos televisivos pueden ser objeto de manipulación o censura. En 2019, por ejemplo, medios de comunicación y activistas denunciaron que algunas coberturas sobre protestas sociales en América Latina fueron sistemáticamente omitidas o distorsionadas en la televisión pública de determinados países (Democracia Abierta, 2020). En otros contextos, como la cobertura de conflictos bélicos, se han detectado casos de imágenes reemitidas fuera de contexto para reforzar determinadas narrativas, o de archivos editados con posterioridad a su emisión original para eliminar declaraciones comprometedoras (Sierra y Sola-Morales, 2020). La aparición de tecnologías de inteligencia artificial capaces de generar contenidos audiovisuales sintéticos —como los *deepfakes*— añade una nueva capa de complejidad, al hacer posible la creación de documentos falsos que pueden infiltrarse en colecciones documentales sin ser fácilmente detectables.

En este contexto, es imprescindible subrayar el valor testimonial y probatorio de los archivos audiovisuales televisivos. Estos documentos no son meros productos mediáticos; constituyen registros históricos que permiten reconstruir acontecimientos, documentar intervenciones políticas o sociales, verificar declaraciones públicas y analizar representaciones colectivas. Son fuentes primarias para la historiografía contemporánea, la investigación periodística, los estudios culturales y la memoria colectiva (Terras y Nyhan, 2022).

Su vulnerabilidad frente a la manipulación representa, por tanto, no solo un problema técnico, sino una amenaza directa a la integridad del conocimiento histórico y al derecho ciudadano a la información. La ausencia de mecanismos sistemáticos para verificar su autenticidad, establecer su trazabilidad y preservar su integridad, convierte a estos archivos en objetos frágiles que pueden ser instrumentalizados en disputas ideológicas o manipulaciones políticas.

Frente a esta situación, la mirada forensial permite abordar los archivos televisivos no solo como fuentes documentales, sino como escenarios de análisis crítico. La forensia informacional aplicada a estos contextos implica la utilización de herramientas y metodologías para detectar alteraciones, omisiones, vacíos o estrategias de control narrativo. Esta perspectiva permite, por ejemplo, identificar la supresión sistemática de determinados colectivos (como pueblos originarios, movimientos sociales, minorías políticas), la ausencia de cobertura sobre ciertos eventos, o la edición selectiva de testimonios que favorecen una única lectura de los hechos.

Desde un punto de vista metodológico, este análisis puede incluir técnicas como la comparación de versiones de emisiones archivadas, el análisis de metadatos para detectar incongruencias temporales o técnicas, el estudio de logs de edición, la aplicación de modelos de análisis de discurso para identificar sesgos o silencios narrativos, y la consulta cruzada con otras fuentes (como archivos ciudadanos, hemerotecas digitales, redes sociales o archivos independientes). En este sentido, el análisis forensial no se limita a verificar la autenticidad técnica del documento, sino que apunta a su integridad comunicacional y su coherencia narrativa como fuente documental.

Un ejemplo hipotético pero plausible podría ser el caso de una cobertura de un acto de represión policial que, en la versión conservada en el archivo televisivo oficial, omite los planos de violencia directa o sustituye los testimonios de las víctimas por declaraciones institucionales. Un análisis forensial podría detectar que existen versiones alternativas en redes sociales o medios independientes que contradicen

esta versión archivada, o que el documento ha sido reeditado con posterioridad a su emisión original. Del mismo modo, podrían identificarse patrones de ausencia sistemática de cobertura sobre determinadas movilizaciones o temáticas, revelando un sesgo estructural en la construcción del archivo.

5. PROCEDIMIENTOS DE FORENSIA INFORMACIONAL EN ARCHIVOS TELEVISIVOS

La aplicación operativa de la forensia informacional en archivos audiovisuales de televisión requiere la implementación de una serie de procesos técnicos y metodológicos orientados a garantizar la autenticidad, la trazabilidad y la integridad de los documentos. Estos procesos deben comenzar desde la propia fase de ingesta del material en el sistema archivístico (Giménez, 2018), incluyendo la conservación de versiones originales, el registro exhaustivo de metadatos técnicos, contextuales y editoriales, y la aplicación de tecnologías de trazabilidad como blockchain o sistemas de control de versiones.

En términos operativos, el procedimiento forensial podría incluir las siguientes etapas:

1. **Preservación de originales sin editar (brutos).** El primer paso fundamental en un entorno forensial es la conservación de la primera versión íntegra del contenido audiovisual producido o emitido. Esta tarea requiere establecer un protocolo de preservación obligatoria que garantice que toda grabación, una vez finalizada su producción o captación, se almacene en su versión bruta, sin cortes, filtros, compresiones o remezclas. Este archivo original debe considerarse como el documento fuente, equiparable a un acta notarial audiovisual, y su acceso debe ser restringido para preservar su inviolabilidad. Por ejemplo, una entrevista política emitida con cortes editoriales debería tener en archivo la versión completa grabada, con silencios, repeticiones y errores, de manera que se puedan reconstruir intenciones editoriales o detectar posibles manipulaciones discursivas posteriores. Su valor reside también en la capacidad de autenticar el contenido de los propios documentos finales producidos, así como en su potencial atribución de supuesta objetividad, pese a que, como cualquier contenido audiovisual, la toma es siempre selectiva y, por tanto, portadora de un sesgo intencional más o menos subliminal por parte de la persona operadora de cámara. En este sentido, es necesario reconocer la vulnerabilidad inherente a la toma digital directa, con posibilidad de manipulación de metadatos, imagen o sonido incluso en el propio dispositivo de captura, antes de su volcado al sistema de producción digital. Esta fase también exige asegurar la estabilidad técnica del archivo, mediante formatos de preservación sin pérdida (Bui *et al.*, 2019), así como el uso de sistemas de hash criptográfico para validar la inalterabilidad del archivo a lo largo del tiempo.
2. **Registro de metadatos enriquecidos.** La segunda etapa se centra en la creación de un sistema de metadatos exhaustivo y multicapas que acompañe cada objeto audiovisual desde su ingreso al archivo. Los metadatos (Blanco y Póveda, 2015) deben incluir no solo información técnica (formato, duración, resolución, códec), sino también metadatos contextuales (fecha de producción, lugar, evento asociado), metadatos editoriales (autoría, responsables de edición, criterios de selección) (Giménez, 2018) y metadatos narrativos y de contenidos (resumen, intenciones editoriales, posibles controversias). Esta riqueza descriptiva es clave para futuras investigaciones forenses que requieran establecer el marco de producción y edición del documento. Por ejemplo, en un reportaje sobre una manifestación, los metadatos deberían indicar si hubo órdenes editoriales de omitir escenas de represión policial, si se aplicaron filtros visuales específicos o si el audio fue sincronizado con posterioridad.
3. **Control de versiones y auditoría de cambios.** Una característica distintiva del enfoque forensial es la posibilidad de reconstruir todo el historial de transformaciones de un documento. Para ello, se propone la implementación de un sistema de control de versiones que registre automáticamente toda modificación realizada sobre un archivo audiovisual, incluyendo la fecha del cambio, el responsable que lo efectuó, el motivo declarado y la naturaleza exacta de la alteración (corte, sustitución de imágenes, ajuste de audio, censura de una palabra, etc.).

Este tipo de trazabilidad es común en entornos de desarrollo de software y puede adaptarse al mundo archivístico mediante tecnologías de versionado o plataformas especializadas en medios (Xiang, 2021). Un ejemplo claro sería la evolución de un documental que inicialmente contenía declaraciones polémicas de una figura pública y que, tras una decisión editorial, fueron eliminadas antes de su retransmisión. La auditoría de cambios permitiría rastrear esta edición, entender su motivación y garantizar que el archivo refleje dicha evolución como parte del proceso documental (John, 2012).

4. Verificación cruzada de fuentes. Una dimensión crítica de la forensia informacional consiste en poder contrastar las versiones archivadas con otras fuentes independientes. Este ejercicio de verificación cruzada puede realizarse mediante el cotejo con archivos ciudadanos (grabaciones realizadas por espectadores), repositorios de emisiones simultáneas, redes sociales o bases de datos internacionales de medios. La verificación cruzada permite identificar incoherencias narrativas, omisiones deliberadas o manipulación en el orden de los hechos presentados (Alam et al., 2021). Por ejemplo, si una cadena omite en su archivo audiovisual la cobertura de una intervención policial durante una protesta, mientras múltiples usuarios suben a plataformas abiertas grabaciones del momento, se abre una hipótesis de silenciamiento informativo que la forensia puede documentar y problematizar. Esta fase requiere desarrollar herramientas semiautomatizadas que permitan al sistema archivístico detectar coincidencias, ausencia de sincronías o ausencias relevantes en la cobertura de eventos, facilitando alertas tempranas sobre posibles alteraciones.
5. Aplicación de análisis forense digital. La quinta etapa comprende la aplicación de técnicas propias del análisis forense digital al contenido audiovisual archivado. Estas técnicas incluyen la detección de ediciones no declaradas mediante análisis de compresión, espectrogramas de audio, identificación de cortes de video por inconsistencias de píxeles, análisis de metadatos embebidos y detección de *deepfakes* por alteraciones faciales o incoherencias fonéticas. Esta fase requiere colaboración con laboratorios de informática forense y el uso de software especializado. En contextos de alta sensibilidad política o judicial, esta fase cobra especial relevancia. Por ejemplo, en un informativo que presenta declaraciones aparentemente realizadas en directo por un líder político, el análisis forense puede revelar que se trata de una síntesis generada por IA a partir de archivos previos, alterando gravemente el valor testimonial del documento. La aplicación de estos procedimientos no solo protege los archivos, sino que también legitima su uso como evidencia en litigios, comisiones de la verdad o investigaciones académicas.
6. Evaluación narrativa y discursiva. Finalmente, la dimensión discursiva del documento audiovisual debe ser también objeto de análisis forense. En esta fase se aplican metodologías propias de los estudios de recepción, análisis del discurso y crítica mediática para detectar patrones de sesgo, omisión, silenciamiento o sobrerrepresentación de ciertas voces o enfoques. Se trata de un análisis interpretativo y crítico que permite identificar cómo se construyen las narrativas informativas y qué elementos quedan sistemáticamente excluidos. Por ejemplo, en la cobertura de un conflicto armado, puede observarse la sistemática invisibilización de víctimas civiles o la supresión de testimonios críticos con el gobierno. A nivel operativo, este análisis se concreta en procedimientos verificables aplicados sobre la obra final: (1) auditoría de EDL, diarios de montaje y metadatos, contrastando timecodes, versiones y estructuras de contenedor para detectar inserciones o manipulaciones de software de edición (Yang et al., 2021); (2) análisis plano a plano y continuidad mediante histogramas o detección de histogram similarity (El-Shafai et al., 2023); (3) examen técnico del audio con métricas técnicas y espectrogramas para localizar overdubs o ediciones no naturales; (4) verificación de integridad mediante análisis de metadata auténtica (Suhardjono et al., 2022); (5) control de integridad del archivo mediante hashes y firmas digitales, así como comparación de características de contenedor (Yang et al., 2021); y (6) evaluación crítica del montaje, ritmo, efectos visuales y semiosis audiovisual (Ferreira et al., 2021) para identificar cómo estos pueden orientar sentidos o emociones. La evaluación narrativa implica también la colaboración de profesionales en comunicación,

lingüística y estudios culturales, que puedan identificar estructuras de poder en el discurso audiovisual archivado. Este tipo de análisis es especialmente útil en contextos de revisión histórica, ya que permite reinterpretar archivos a la luz de nuevas condiciones políticas o sociales (Unger, 2016). Esta colaboración interdisciplinaria es necesaria porque la dimensión discursiva del audiovisual combina elementos técnicos, semióticos y culturales que requieren diferentes perspectivas para ser correctamente interpretados: los documentalistas aportan conocimiento sobre la estructura y autenticidad de los archivos, los comunicólogos analizan patrones de persuasión y estrategias mediáticas (Skowronek, 2014), los lingüistas descifran matices del lenguaje y la pragmática, y los especialistas en estudios culturales contextualizan simbologías y representaciones sociales (Wang, 2023). La actuación conjunta puede articularse mediante talleres colaborativos de análisis de contenido, sesiones de revisión de metadatos y del material para detectar cortes o manipulaciones, y reuniones periódicas de interpretación cruzada donde cada experto aporta su evaluación.

Este conjunto de procedimientos no solo permitiría mejorar la calidad documental de los archivos, sino también dotarlos de una legitimidad epistemológica y jurídica mayor, abriendo la posibilidad de que sean utilizados como prueba en litigios, investigaciones o ejercicios de memoria histórica.

En el contexto mediático actual, caracterizado por la desinformación, la fragmentación del discurso y la erosión de las fuentes confiables, el archivo televisivo se convierte en un territorio crítico para la defensa de la integridad informacional. La forensia informacional, entendida como enfoque transversal y operativo, permite abordar las amenazas que pesan sobre estos documentos desde una perspectiva técnica, crítica y ética. Lejos de tratarse de una mera sofisticación archivística, representa una apuesta por fortalecer los principios democráticos que deben guiar la memoria audiovisual: veracidad, trazabilidad, transparencia y pluralidad.

Al introducir procedimientos específicos, desarrollar perfiles profesionales especializados y generar una cultura institucional de la autenticidad audiovisual, la forensia informacional puede contribuir significativamente a proteger los archivos televisivos frente a la manipulación, a reconstruir narrativas silenciadas y a ofrecer garantías de fiabilidad documental en tiempos de incertidumbre. Así, los archivos no solo conservarán la imagen del pasado, sino también su verdad.

6. CONCLUSIONES

La presente investigación ha permitido delinear los contornos conceptuales y operativos de la forensia informacional como un campo emergente situado en la intersección entre la archivística digital, las ciencias de la información, los estudios mediáticos y las técnicas forenses. En un contexto de creciente desinformación, manipulación audiovisual y circulación incontrolada de contenidos digitales, se reafirma la necesidad de una mirada crítica, metodológicamente robusta y tecnológicamente actualizada que permita garantizar la autenticidad, trazabilidad y veracidad de los documentos, especialmente en los archivos audiovisuales de televisión.

El artículo ha demostrado que los archivos televisivos, lejos de ser depósitos neutros, constituyen dispositivos narrativos atravesados por intereses políticos, editoriales y tecnológicos. Su vulnerabilidad a la censura, la reescritura narrativa y la pérdida de integridad documental demanda herramientas que trasciendan los enfoques clásicos de preservación y catalogación. La forensia informacional aporta, en este sentido, un enfoque sistémico capaz de detectar alteraciones, vacíos intencionados o narrativas silenciadas, y de establecer protocolos que refuercen su valor testimonial y probatorio en contextos democráticos.

Entre los principales aportes de este trabajo destaca la identificación de riesgos específicos —como la edición indebida, la omisión de coberturas relevantes o la infiltración de *deepfakes*— así como la propuesta de procedimientos técnicos orientados a preservar la integridad informacional de los archivos audiovisuales: conservación de versiones originales, enriquecimiento de metadatos, trazabilidad de cambios y análisis comparativos de fuentes, entre otros.

Sin embargo, el desarrollo pleno de la forensia informacional enfrenta importantes desafíos. En primer lugar, se requiere una formación interdisciplinar de profesionales capaces de integrar saberes archivísticos, técnicos y críticos. En segundo lugar, resulta urgente el desarrollo de metodologías y herramientas forenses adaptadas a entornos audiovisuales digitales. Asimismo, deben definirse marcos éticos sólidos que regulen la intervención forensial sin comprometer la libertad editorial ni generar nuevos riesgos de control o vigilancia.

Por lo tanto, este trabajo invita a consolidar la forensia informacional como un campo de investigación y práctica orientado a fortalecer la transparencia, la memoria plural y el acceso crítico a los archivos audiovisuales. Fomentar investigaciones aplicadas, colaborativas y éticamente comprometidas en este ámbito resulta indispensable para garantizar que estos documentos, fundamentales para la construcción del conocimiento y la rendición de cuentas social, conserven su integridad y continúen siendo una fuente fiable en la era digital.

Información complementaria ↑

Fuentes de financiación

Esta investigación ha sido financiada por la Junta de Extremadura y los Fondos FEDER “Una manera de hacer Europa” [Grupo de Investigación QUINARI SEJ013 GR18130].

Material suplementario

No aplica.

Disponibilidad de datos

No aplica.

Agradecimientos

No aplica.

Declaración de contribución de autoría

Jorge Caldera-Serrano: Conceptualización, Análisis formal, Investigación, Metodología, Supervisión, Validación, Visualización, Redacción - borrador original, Redacción - revisión y edición.

Declaración de conflicto de intereses

El autor de este artículo declaran no tener conflictos de intereses financieros, profesionales o personales que pudieran haber influido de manera inapropiada en este trabajo.

Declaración de uso de Inteligencia Artificial

Se ha utilizado ChatGPT (2025). Versión: GPT-4-Turbo, para la revisión del texto y traducción del resumen aportado.

Prompt 1:

Solicito una revisión exhaustiva de estilo del siguiente texto, correspondiente a un artículo científico.

Por favor, realiza las siguientes tareas:

Corrige errores ortográficos, de puntuación, concordancia de género y número.

Proponme mejora la redacción para lograr un estilo preciso. No realices cambios, solo haz propuestas.

Sugiere cambios en párrafos que presenten problemas de: estructura gramatical confusa, longitud excesiva o fragmentación innecesaria, falta de coherencia o fluidez argumentativa.

Marca estos párrafos problemáticos e indica brevemente por qué deben ser modificados y alternativa de redacción.

Mantén el contenido técnico intacto y evita simplificaciones (en tu propuestas) que comprometan el rigor académico.

Prompt 2:

Traduce al inglés el siguiente resumen documental para un paper científico del ámbito de las Ciencias de la Documentación.

BIBLIOGRAFÍA

- Alam, F., Cresci, S., Chakraborty, T., Silvestri, F., Dimitrov, D., Da San Martino, G., Shaar, S., Firooz, H., y Nakov, P. (2021). A Survey on Multimodal Disinformation Detection. *arXiv preprint arXiv:2103.12541*. Disponible en: <https://arxiv.org/abs/2103.12541>
- Alanazi, S., y Asif, S. (2024). Exploring deepfake technology: Creation, consequences and countermeasures. *Human-Centric Intelligent Systems Integration*, 6, 49–60. <https://doi.org/10.1007/s42454-024-00054-8>
- Blanco Izquierdo M. J. y Poveda López I. C. (2015). Metadatos documentales en Canal Extremadura Televisión. *Cuadernos de Documentación Multimedia*, 26, 113-132. DOI: https://doi.org/10.5209/rev_CDMU.2015.v26.50633
- Bui, T., Cooper, D., Collomosse, J., Bell, M., Green, A., Sheridan, J., Higgins, J., Das, A., Keller, J., Thereaux, O., y Brown, A. (2019). ARCHANGEL: Tamperproofing video archives using temporal content hashes on the blockchain. *arXiv*, 1904.12059. Disponible en: <https://arxiv.org/abs/1904.12059>
- Caldera-Serrano, J. (2025). Comparativa de aplicaciones de inteligencia artificial para la selección documental en los archivos televisivos. *Investigación Bibliotecológica: Archivonomía, Bibliotecología e Información*, 39(103), 67–84. <https://doi.org/10.22201/iibi.24488321xe.2025.103.58963>
- Caled, D., y Silva, M. J. (2022). Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation. *Journal of Computational Social Science*, 5, 123–159. DOI: <https://doi.org/10.1007/s42001-021-00118-8>
- Democracia Abierta. (2020). *2019: Protest and disruptive changes in Latin America: In 2019, we saw protest and disruptions take place in several countries across Latin América*. Disponible en: <https://www.opendemocracy.net/en/democraciaabierta/2019-movilizaciones-ciudadanas-y-cambios-disruptivos-en-am%C3%A9rica-latina-en/>
- Duranti, L., y Rogers, C. (eds.). (2018). *Trusting records and data in the cloud: The creation, management, and preservation of trustworthy digital content*. Facet. DOI: <https://doi.org/10.29085/9781783304042>
- El-Shafai, W., Fouda, M. A., El-Rabaie, E. M., y Abd El-Salam, N. (2023). A comprehensive taxonomy on multimedia video forgery detection techniques: challenges and novel trends. *Multimedia Tools and Applications* 83, 4241-4307. DOI: <https://doi.org/10.1007/s11042-023-15609-1>
- Ferreira, S., Antunes, M., y Correia, M. (2021). Exposing manipulated photos and videos in digital forensics analysis. *Journal of Imaging*, 7(7), 102. DOI: <https://doi.org/10.3390/jimaging7070102>
- Giménez Rayo, M. (2018). La selección del material audiovisual en televisión en el entorno digital: perspectivas y realidad. *Documentación de las Ciencias de la Información*, 41, 47-59. DOI: <https://doi.org/10.5209/DCIN.61456>
- Gotel, O., Cleland-Huang, J., Hayes, J. H., Zisman, A., Egyed, A., Grünbacher, P., Dekhtyar, A., Antoniol, G., Maletic, J., y Mäder, P. (2012). Traceability fundamentals. En *Software and systems traceability*, 3–22. Springer. DOI: https://doi.org/10.1007/978-1-4471-2239-5_1
- Iacovino, L. (2004). Multi-method interdisciplinary research in archival science: The case of recordkeeping, ethics and law. *Archival Science*, 4, 267–286. DOI: <https://doi.org/10.1007/s10502-005-2595-7>
- Jaillant, L. (2022). How can we make born-digital and digitised archives more accessible? Identifying obstacles and solutions. *Archival Science*, 22, 417–436. DOI: <https://doi.org/10.1007/s10502-022-09390-7>
- John, J. L. (2012). *Digital forensics and preservation* (Technology Watch report). Digital Preservation Coalition. DOI:

<http://dx.doi.org/10.7207/twr12-03>

- Le-Khac, N.-A., y Choo, K.-K. R. (Eds.). (2020). *Cyber and digital forensic investigations: A law enforcement practitioner's perspective*. Springer. DOI: <https://doi.org/10.1007/978-3-030-47131-6>
- Li, J., y Chang, X. (2023). Combating misinformation by sharing the truth: A study on the spread of fact-checks on social media. *Information Systems Frontiers*, 25, 1479–1493. DOI: <https://doi.org/10.1007/s10796-022-10296-z>
- MacNeil, H. (2004). Contemporary archival diplomatics as a method of inquiry: Lessons learned from two research projects. *Archival Science*, 4, 199–232. DOI: <https://doi.org/10.1007/s10502-005-2592-x>
- May, L. (2023). Media and resistance in authoritarian contexts. En *Media and feminist protest in Iran*. Palgrave Macmillan. DOI: https://doi.org/10.1007/978-3-031-44861-4_2
- Moussa, A. F. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, 11, 20. DOI: <https://doi.org/10.1186/s41935-021-00234-6>
- Pacheco, A., Guardado da Silva, C., y Vieira de Freitas, M. C. (2023). A metadata model for authenticity in digital archival descriptions. *Archival Science*, 23, 629–673. DOI: <https://doi.org/10.1007/s10502-023-09422-w>
- Post, C., y Chassanoff, A. (2021). Beyond the workflow: Archivists' aspirations for digital curation practices. *Archival Science*, 21, 413–432. DOI: <https://doi.org/10.1007/s10502-021-09365-0>
- Schüller, D. (2019). Audiovisual documents and the digital age. En *The UNESCO Memory of the World Programme*, 203–217. Springer. DOI: https://doi.org/10.1007/978-3-030-18441-4_14
- Seeger, A., y Chaudhuri, S. (2015). The contributions of reconfigured audiovisual archives to sustaining traditions. *The World of Music*, 4(1), 21–34. Disponible en: <https://www.jstor.org/stable/43561464>
- Shu, K., Wang, S., Lee, D., y Liu, H. (2020). *Disinformation, misinformation, and fake news in social media: Emerging research challenges and opportunities*. Springer. DOI: <https://doi.org/10.1007/978-3-030-42699-6>
- Sierra Caballero, F., y Sola-Morales, S. (2020). Golpes mediáticos y desinformación en la era digital: La guerra irregular en América Latina. *Comunicación y Sociedad*, 2020, e7604. DOI: <https://doi.org/10.32870/cys.v2020.7604>
- Skowronek, B. (2014). Media linguistics: An interdisciplinary approach to the study of language and media. *MediaLingua*, 3(1), 1-20. Disponible en: <https://medialing.ru/media-linguistics-an-interdisciplinary-approach-to-the-study-of-language-and-media/>
- Suhardjono, S., Handayani, P., Sugiarto H., Aisyah N., y Syah Putra, A. (2022). Forensic analysis video metadata authenticity detection using Exiftool. *Journal of Innovation Research and Knowledge*, 1(12), 1727–1734. Disponible en: <https://www.bajangjournal.com/index.php/JIRK/article/view/2227/1605>
- Terras, M., y Nyhan, J.(eds.) (2022). Defining Digital Humanities: A Reader. *Digital Research in the Arts and Humanities*.
- Unger, J. W. (2016). The interdisciplinarity of critical discourse studies research. *Palgrave Communications*, 2, 15037. DOI: <https://doi.org/10.1057/palcomms.2015.37>
- Wang, H. (2023). Instrumentalisation of critical discourse studies: A linguistic analysis of public relations concepts in the CDS journal article abstracts (2000–2020). *Humanities and Social Sciences Communications*, 10(1), 304. DOI: <https://doi.org/10.1057/s41599-023-01818-4>.
- Xiang, Z., Horváth, J., Baireddy, S., Bestagini, P., Tubaro, S., y Delp, E. J. (2021). *Forensic analysis of video files using metadata*. arXiv preprint *arXiv*, 2105.06361. Disponible en: <https://arxiv.org/abs/2105.06361>
- Yang, P., Baracchi, D., Iuliani, M., Shullani, D., Ni, R., Zhao, Y., y Piva, A. (2021). Efficient video integrity analysis through container characterization. *arXiv*. Disponible en: <https://arxiv.org/abs/2101.10795>
- Zhang, T. (2022). Deepfake generation and detection: A survey. *Multimedia Tools and Applications*, 81, 6259–6276. DOI: <https://doi.org/10.1007/s11042-021-11733-y>