ACCCF / APPLIED KNOWLEDGE LIBRARY

06

VOLUME

Originality, structure, continuity, and provenance

Spanish edition · 2026

Manual for Authenticating Audio, Video, and AI-Generated or Manipulated Images

Examination methods, references, synthetic content, and limits of conclusion

Analyze a multimedia file without turning a detector, metadata, or a visual printout into an automatic verdict on authenticity, authorship, or truth.

For multimedia forensic experts, lawyers, researchers, journalists, reviewers, and preservation professionals. Speaker, face, photogrammetry, or sensitive-content analysis requires additional specialization and controls.

Editorial coordination: Jocsan Laguna · Consejo Americano de Ciberseguridad y Cómputo Forense

General technical guide and open educational material. It does not constitute legal advice, an expert opinion, or instructions for accessing systems without authorization. Examples and data are fictitious; figures are editorial reconstructions.

Contents

Visible pagination corresponds to the PDF edition. Word may update this index when the document is opened; headings retain internal navigation.

Introduction: seeing is not verifying 3
Chapter 1. The question of authenticity 3
1.1 Originals, copies, edits, and representations 3
1.2 Defining the assignment and references 4
Chapter 2. Acquisition and preservation 4
2.1 Original object and version chain 4
2.2 Extracting frames, audio, and streams 5
2.3 Security and privacy 5
Chapter 3. Structure, metadata, and chronology 5
3.1 Container, codec, and streams 5
3.2 Chronology of capture, conversion, and publication 6
3.3 When a time does not match 6
Chapter 4. Technical examination 6
4.1 Still images 6
4.2 Video: structure and temporal continuity 6
4.3 Audio: signal, environment, and synchronization 7
4.4 Example of an edit that looks obvious 7
Chapter 5. Synthetic content and detectors 8
5.1 Detectors as indicators, not judges 8
5.2 C2PA and other provenance signals 8
5.3 Legal frameworks without universal categories 8
Chapter 6. Limited reporting and conclusions 9
6.1 Traceability of each test 9
6.2 When no conclusion is possible 10
Annex A. Protocol and formats 10
A.1 Multimedia receipt record 10
A.2 Test matrix 10
A.3 Derivatives register 11
Annex B. Functional legal framework and final checklist 11

Introduction: seeing is not verifying

An image can show something that never happened, and an original camera file can record a staged scene. Authenticity is not answered by saying “it looks clear.” Separate questions must be asked: Is the file what it purports to be? Was it produced using the stated method? Does it preserve continuity? Does it faithfully represent the event? Can its creation be attributed to someone?

Multimedia analysis does not mean searching for a filter that outputs “false.” It means documenting the object’s history and comparing its structure, content, metadata, references, and context. Downloading from a platform can lose information without changing the event shown; editing can be legitimate; compression can produce artifacts that look like manipulation. The conclusion arises from convergence and evaluated alternatives.

SWGDE recommends multiple methods for video authentication and cautions that an original file may contain a staged scene. Its audio guides show that every measurement carries uncertainty linked to sampling, compression, configuration, and environment.[1][2]

> **Four distinct questions**
> Is the file original in the stated sense? Has it been transformed? Did the scene occur as claimed? Who produced or published the content? These four questions cannot be answered by a single percentage.

Chapter 1. The question of authenticity

1.1 Originals, copies, edits, and representations

Originality is a statement that requires context. It can refer to the first file produced by a camera, the file supplied by a provider, or a complete copy known to date from a particular time. An export can retain content in a different structure; a screen re-recording can show the same scene with new characteristics; an enhanced image can make details easier to read without being suitable for every test. Identify the representation before analyzing it.

Generation, editing, conversion, and publication are distinct events. Generation can mean capture with a sensor or synthesis with a service. Editing changes content or sequence. Conversion changes the container, codec, size, or compression without necessarily implying deception. Publication adds an account, URL, audience, and date. Preservation records all known events without collapsing them into “manipulated.”

Assertion	Source needed	What it does not establish
Camera file	Device, structure, copy, and provenance.	The scene was not staged.
Edited video	History, structure, continuity, and comparison.	Fraudulent intent or falsity of everything.
Synthetic content	Generation, history, service and references.	A specific tool identified by appearance alone.

[1] SWGDE 23-V-001-1.2. Best Practices for Digital Video Authentication. Examination using multiple methods, origin, structure, and limitations; an original camera file may depict a staged scene, and an edited file alone does not prove intent to deceive. Official online source

[2] SWGDE. Best Practices for Digital Audio Authentication. Global and local analysis and comparison with specimens; uncertainty depends on sampling, compression, configuration, and environment. No universal measure establishes authenticity. Official online source

Assertion	Source needed	What it does not establish
Account publication	URL, account, date, and available records.	The account holder produced the file.
Actual event	Content, corroboration and circumstances.	File originality proves the event.

1.2 Defining the assignment and references

The assignment must state whether the goal is origin, continuity, editing, identification, synchronization, content, or provenance. Not every question can be answered technically with the same file. If only a compressed download is available, there may be insufficient information for a conclusion of originality; declare this at the outset, not at the end to excuse an answer already decided.

References include camera originals, other files from the same sequence, sample recordings from the same device and configuration, publication versions, editing projects, and service records. Producing specimens on an evidence device can alter its content: preserve it first and assess whether equivalent equipment should be used instead. References must be comparable in resolution, codec, lighting, environment, and configuration.

> **Starting condition**
> If the assignment asks to establish that a person said something and only a clip without context is available, the first task is to obtain the complete file, its provenance, and comparison sources, not to issue an authenticity opinion based on appearance.

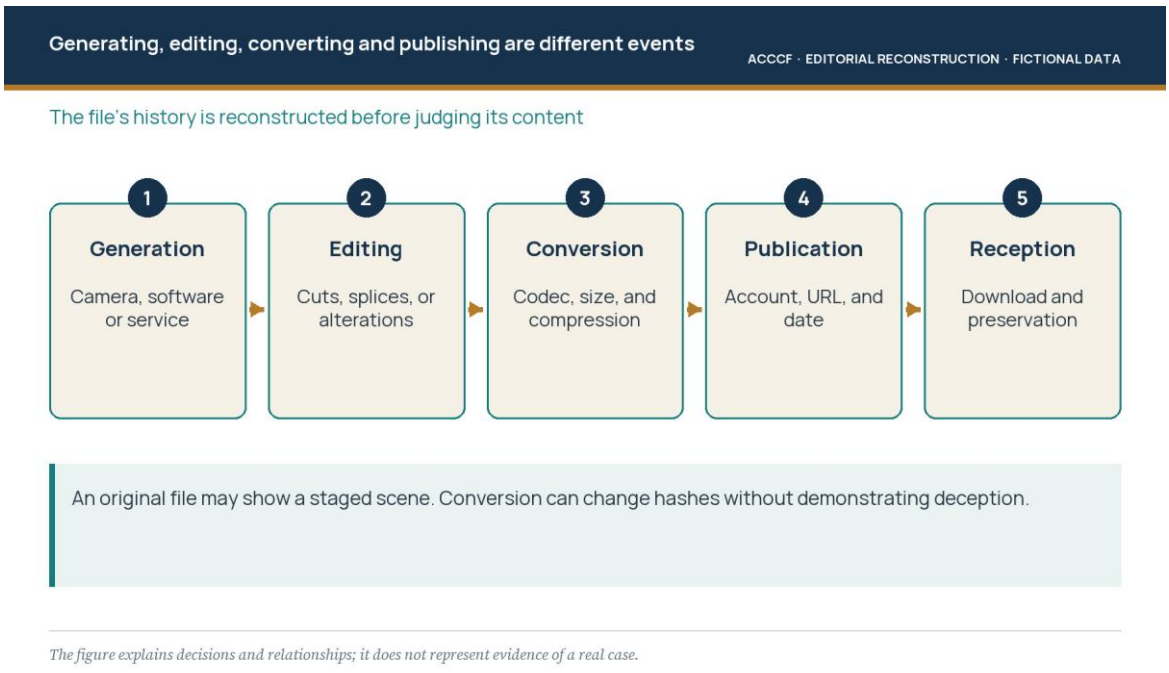


Figure 1. Generation, editing, conversion, and publication are distinct events. The file's history is reconstructed before judging its content. Editorial reconstruction; it does not constitute actual evidence.

Chapter 2. Acquisition and preservation

2.1 Original object and version chain

Request the native file, nearby sequence, device, or official export according to the question. Preserve the received object before renaming it, opening it with editors, or converting it. The manifest records the

original name, size, format, receipt date, channel, custodian, identifier, and relationship to other versions. Hashes are calculated by object and time; they do not demonstrate the scene.

If the file comes from a platform, record the URL, account, publication, visible date, download date and time zone, tool, selected quality, and parameters. Preserve the page and context too when lawful and relevant. A screenshot of the page does not replace the multimedia file, just as the file does not prove who administered the account.

2.2 Extracting frames, audio, and streams

When separating audio and video or extracting images, work on a controlled copy. Copy the stream without re-encoding when the method permits; if conversion is necessary, use a lossless format suitable for analysis and record the tool, version, parameters, and output. The extracted image is a derivative, not a new original.

SWGDE recommends copying streams or transcoding to lossless formats when necessary, with equivalence verification where appropriate. This practice avoids presenting a new compression as though it were a feature of the received file. Derivative names include provenance and are not overwritten.[3]

Object	Permitted use	Accompanying record
Original received	Preservation and reference comparison.	Channel, date, custodian, hash and format.
Working copy	Repeatable examination and queries.	Derivation and tools.
Frame	Local visual analysis or comparison.	Time, stream, extraction, and parameters.
Isolated audio	Signal analysis and synchronization.	Documented stream copy or conversion.
Enhanced image	Reading or presentation, not replacement of the original.	Adjustment, sequence and purpose.

2.3 Security and privacy

Files may contain minors, victims, faces, voices, locations, documents, or intimate information. Restrict access, analysis versions, and presentation versions. Do not upload the file to detectors or online services without evaluating authorization, confidentiality, retention, and jurisdiction. A free score can lead to further disclosure.

> **Laboratory rule**
> Do not run an unknown file on a production system or forward it to a group for opinions. Use a controlled environment and fictitious data to validate tools; preserve the object and minimize its dissemination.

Chapter 3. Structure, metadata, and chronology

3.1 Container, codec, and streams

Examine the container, codec, duration, frame rate, resolution, channels, timestamps, tables, and stream structure. An atypical structure may indicate editing, but also export, repair, download, or conversion.

[3] SWGDE 23-V-001-1.2. Best Practices for Digital Video Authentication. Examination using multiple methods, origin, structure, and limitations; an original camera file may depict a staged scene, and an edited file alone does not prove intent to deceive. Official online source

Compare it with specimens from the same family and configuration before interpreting. The analysis tool does not replace an explanation of the finding.

Absence of metadata does not prove manipulation: some platforms remove fields. Its presence does not prove originality either: it can be copied or written. Evaluate its meaning in light of the file's history. A coherent internal date can be compatible with a sequence yet still not establish the event if the clock or scene was prepared.

3.2 Chronology of capture, conversion, and publication

The timeline records the literal date, producer, time zone, and precision. A camera date may have no time zone; the download date belongs to another event; the publication date may depend on the server; the editing date may correspond to the project or export. Do not order everything as though it represents the same event. Preserve uncertainty and contradictory data in the sequence.

Names such as IMG_0041, IMG_0042, and IMG_0043 can guide a sequence, but imports, restarts, and renaming can defeat that inference. Review thumbnails, content, metadata, backups, application logs, and neighboring files. A gap in names does not prove deletion; it may reflect another format or a folder not included.

3.3 When a time does not match

A fictitious video shows a clock at 18:42, while an accusation claims it was recorded at 20:42. The method does not immediately declare forgery or accept 18:42 as the absolute time. Review the clock within the scene, device counter, time zone, metadata, sequence, early publication, receipts, other cameras, and testimony. The difference may be a conversion, a misconfigured clock, or a larger inconsistency.

> **Appropriate wording**
> "The file contains a visible clock reading 18:42 and an internal field with no declared time zone. The available sources do not permit that value to be reconciled with the alleged 20:42. Synchronization and corroboration are required before the time of the event can be established."

Chapter 4. Technical examination

4.1 Still images

Review dimensions, format, structure, thumbnails, sequence, compression, noise, edges, lighting, perspective, and continuity with other files. An unusual line may be a compression artifact; an apparently incompatible shadow may result from multiple lights or perspective; a generated image may not exhibit the typical errors the public expects. Visual analysis guides testing but does not replace it.

Compare the original image with clearly identified derivatives. Increasing contrast or enlarging can help reveal details, but can also create or emphasize artifacts. Retain all adjustments in the report and do not present the processed version as the original. Identifying a person by face requires a specialized method and cannot be inferred from "looks like."

4.2 Video: structure and temporal continuity

Review frames, timestamps, duplicates, scene relationships, audio synchronization, compression, camera changes, and physical continuity. A jump may correspond to a legitimate recording pause or device transition; the absence of a jump does not prove there was no editing. Global and local analyses are combined with references.

SWGDE describes correlation analysis, sensor noise, color, double compression, and other methods, with conditions and limitations. Sensor noise can be difficult to use with inadequate lighting or resolution; double compression alone does not explain the reason. The conclusion must state which method was applied, what result it produced, and which alternatives remain possible.[4]

4.3 Audio: signal, environment, and synchronization

Listen to and measure the entire file when the assignment permits: continuity, environment, cuts, echo, noise, frequency, saturation, channels, synchronization, and relationship to video. A change of environment may correspond to actual movement; a cut may result from a network interruption; an identical voice may be cloned or a recording reused. Human listening is an observation, not a sufficient measure.

SWGDE guides distinguish global and local analysis and recommend specimens with appropriate configurations. DC offset, compression, spectrum, and ENF are not standalone verdicts; each technique has conditions of use and uncertainty. Speaker identification is a distinct discipline that must not be improvised with an automatic comparator.[5]

4.4 Example of an edit that looks obvious

A fictitious video appears to lose continuity before a mirror breaks. The first version has an image cut; the original camera file shows an automatic interruption caused by the recording limit, and the next file preserves the continuation. Reviewing only the first file could suggest intentional deletion; the complete sequence shows that a segment is missing for another reason. In another case, the missing segment does prevent reconstruction of the event and must be declared.

> **Lesson**
> An anomaly requires a verified explanation. It may be editing, pausing, segmentation, codec, or export. Its effect on the case depends on the complete sequence, not on how dramatic the cut appears.

[4] SWGDE 23-V-001-1.2. Best Practices for Digital Video Authentication. Examination using multiple methods, origin, structure, and limitations; an original camera file may depict a staged scene, and an edited file alone does not prove intent to deceive. Official online source

[5] SWGDE. Best Practices for Digital Audio Authentication. Global and local analysis and comparison with specimens; uncertainty depends on sampling, compression, configuration, and environment. No universal measure establishes authenticity. Official online source



Figure 2. The analysis compares multiple indicators and their limitations. There is no universal measure of authenticity. Editorial reconstruction; it does not constitute actual evidence.

Chapter 5. Synthetic content and detectors

5.1 Detectors as indicators, not judges

A detector can produce a synthetic content score, but its performance depends on training, version, format, compression, cropping, re-recording, and content type. A positive result can be false; a negative result can overlook manipulation. Record the tool, release, configuration, exact object, date, and limitations. Do not publish the percentage alone.

Before using an external service, verify whether the file may be shared. Local analysis can reduce exposure but also requires validation. The detector guides what to review next: source file, history, specimen, project, publication, or generation service. It does not replace any of those sources.

5.2 C2PA and other provenance signals

C2PA defines manifests, claims, signatures, and cryptographic links to content for recording provenance. A valid credential can demonstrate that certain claims were signed and linked to the asset through a compatible process. It does not prove that the scene occurred or that every producer assertion is true. Absence of a credential does not prove falsity.[6]

The review records the manifest, signer, ingredients, validation status, changes, specification version, and tool. If the asset was exported without retaining the credential, preserve that limitation and seek an earlier version. Watermarks and metadata complement, but do not replace, context or the original file.

5.3 Legal frameworks without universal categories

Legal analysis separates consent, identity, use, conduct, date, and regime. In Mexico, Articles 199 Octies and 199 Nonies of the Federal Criminal Code address certain conduct involving nonconsensual intimate content, even where the material does not depict the identified person. In the European Union, Article 50

[6] Coalition for Content Provenance and Authenticity. C2PA Technical Specification 2.3 (05-01-2026). Provenance, manifests, assertions, and cryptographic linking to content. Absence of credentials does not prove falsity, and their presence does not prove the truth of the scene. Official online source

of the AI Regulation governs transparency for certain deepfakes and provides for adaptation for creative and fictional works. Neither amounts to a worldwide ban on all AI.[78]

A satirical, educational, or openly synthetic work must not be analyzed as deceptive without reviewing its context. Conversely, an "AI-generated" label does not resolve consent, harm, ownership, or use. The technical conclusion is limited to provenance and transformations; legal analysis is developed using the applicable law and facts.

Fictitious case

A publication shows a person speaking with a declared cloned voice. The file has a generation manifest and a visible description of the production. The voice's authenticity as a natural voice is justifiably rejected, but the publication does not conceal its synthesis. Questions of authorization, use, and effect on the audience remain separate.

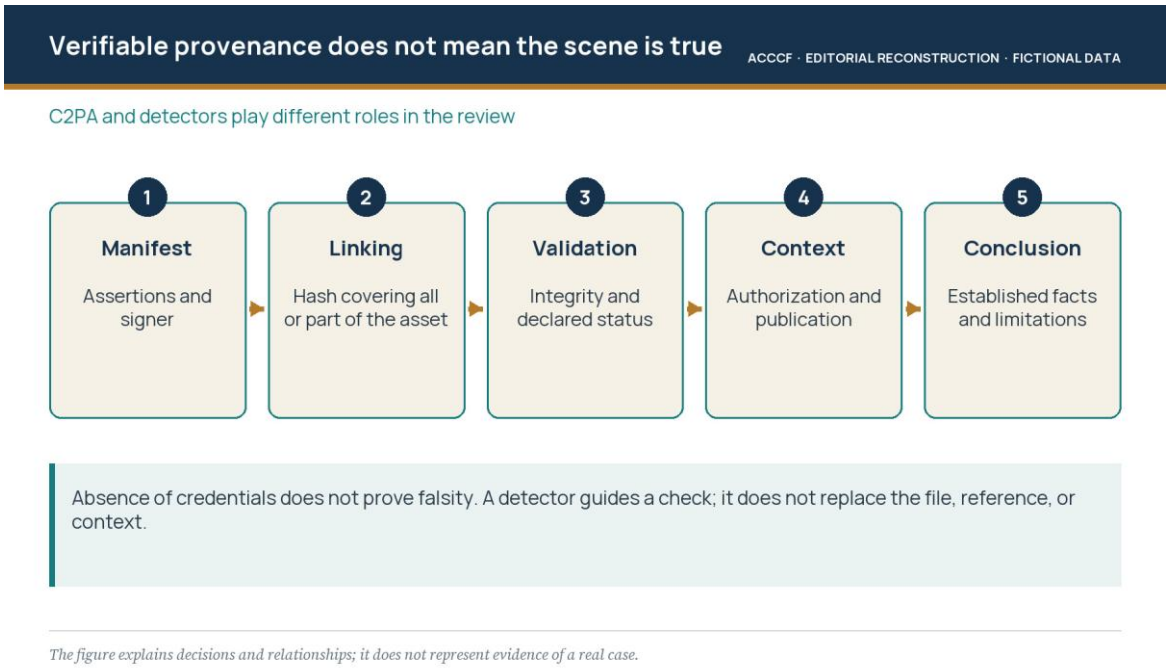


Figure 3. Verifiable provenance does not mean the scene is true. C2PA and detectors play different roles in the review. Editorial reconstruction; it does not constitute actual evidence.

Chapter 6. Limited reporting and conclusions

6.1 Traceability of each test

The report identifies the assignment, objects, representations, tools, versions, parameters, specimens, queries, and results. Each finding refers to the file, time, or region analyzed and to the derived figure where appropriate. Images are accompanied by their source and the adjustment used. If a test could not be performed, explain why and how it affects the conclusion.

Observation, measurement, inference, and conclusion are distinguished. "The frame shows discontinuity" is observation; "correlation decreases in this region" is a result; "consistent with editing"

[7]Mexico. Federal Criminal Code, Articles 199 Octies and 199 Nonies, compilation including the amendment of 13-03-2026: certain conduct involving nonconsensual intimate sexual content, even where the material does not depict the identified person. Official online source

[8]Regulation (EU) 2024/1689 on artificial intelligence, Article 50, consolidated text as of 27-07-2026: transparency for certain deepfakes and adaptations for creative, satirical, artistic, or fictional works. Official online source

is inference; “the file was fabricated by a person” requires another source. The writing preserves these planes so that the reader can review the inferential step.

Result	Permitted formulation	Information that can change it
Matching hash	The object did not change between two checks.	Identification or algorithm error.
Atypical structure	Compatible with editing or conversion; requires reference.	Original export of the device.
Positive detector result	Indicative result with version and limitations.	Original, history, or independent analysis.
Valid C2PA	Signed claims linked to the asset.	Certificate, chain of custody, or content that was false from the outset.
No conclusion	Insufficient data for originality or the scene.	Native file and comparable specimens.

6.2 When no conclusion is possible

An inconclusive conclusion is not a defeat: it prevents suspicion from becoming a damaging public assertion. If only a compressed copy without history or references is available, the report can describe what was observed and identify which source is needed. Do not fill the gap with scientific-sounding language or a collection of filters.

The independent reviewer attempts to reproduce queries and seeks alternative explanations. The reviewer also checks that images are not presented as actual evidence when they are reconstructions and that figures do not conceal information. If a new source changes the conclusion, update the analysis without erasing the version history.

> **Closure**
> The aim is not to obtain a verdict at any cost, but to retain sufficient source and method so that the conclusion can withstand a review that does not share the first impression.

Annex A. Protocol and formats

A.1 Multimedia receipt record

Fictitious manifest

```
Object / ID: DEMO-VID-001-R00
Original filename and format: [retain name]
Declared source: [camera, export, platform, person]
Channel and date of receipt: [EML, link, device]
URL, account and publication: [if applicable]
Size, duration, resolution, and streams: [observed]
Hash and algorithm: [object and moment]
Related versions: [original, download, copy, reference]
Declared history: [generation, editing, conversion, publication]
Authority and privacy: [scope, restrictions]
Incidents: [damaged file, lack of codec, absences]
Destination: [preserved, working copy and access]
```

A.2 Test matrix

Question	Method and reference	Result	Limitation / next source
Compatible structure?	[Container, specimen]	[Observation]	[Possible conversion]

Question	Method and reference	Result	Limitation / next source
Temporal continuity?	[Frames, sequence]	[Observation]	[Pause or editing]
Consistent audio?	[Signal, spectrum, reference]	[Observation]	[Environment, sampling]
Provenance?	[C2PA, history, records]	[State]	[Absence does not prove falsity]
Actual scene?	[Independent corroboration]	[Compatible/uncertain]	[File alone is insufficient]
Authorship?	[Account, project, device]	[Association]	[No automatic personal identification]

A.3 Derivatives register

Derivative	Source	Method and parameters	Permitted use
Working copy	DEMO-VID-001-R00	Verified copy and related hash.	Examination without altering the original.
Frame 00:12:04	W01 copy	Lossless extraction; tool and version.	Local comparison.
Isolated audio	W01 copy	Documented stream copy or conversion.	Signal analysis.
Enhanced image	Frame D01	Declared contrast and crop.	Presentation, not replacement.
Report and annexes	All the objects	Manifest, queries, and version.	Independent review.

Annex B. Functional legal framework and final checklist

Electronic documents may be admitted without closing the debate on authenticity. In Mexico, CCom, CFPC/CNPCF according to the transition, and NOM-151 for preservation within its scope are reviewed; Peru separates signature, procedure, and archives; Chile distinguishes signature and date; Argentina weighs reliability; Colombia and Ecuador require preservation context; Spain combines eIDAS, LEC, and

trust services. These functions are complemented, where applicable, by specific rules on AI, intimate content, and data protection.[9][10][11][12][13][14][15][16][17][18][19]

Before delivery	Check
Question	Originality, transformation, scene, authorship or publication?
Source	Are the native file, history, sequence, specimen, and context available?
Method	Are tools, versions, parameters, and derivatives documented?
Alternatives	Have conversion, pauses, staged scenes, and legitimate editing been evaluated?
AI	Are detector limitations acknowledged and C2PA interpreted within its scope?
Privacy	Is the file shared only with authorization and minimization?
Conclusion	Does every assertion lead back to a source and declare limitations?

Closure

Authenticity is not measured by resemblance or fear of technology. It is examined using files, history, comparison, and a conclusion that accepts its own limitations.

[9] Mexico's Commercial Code, Articles 89–94 and 1205: neutrality, attribution, written form, originals, integrity, accessibility, and admission of data messages. Official compilation. Official online source

[10] National Code of Civil and Family Procedure, Articles 348–350. Compilation including the amendment of 15-01-2026. Application is gradual and depends on declarations. Official online source

[11] NOM-151-SCFI-2016, preservation and digitization of data messages, published on 30-03-2017. Requirements for records, integrity, accessibility, and digital hash. Official online source

[12] Peru. Code of Civil Procedure, Articles 188–197 and 245.5: purpose, legality, evidence, burden, evaluation, and dates determined by technical means. Official online source

[13] Chile. Law 19.799 on electronic documents and electronic signatures, Articles 1–5: equivalence, written form, simple/advanced signatures, date, and evidentiary value. Official online source

[14] Argentina. Civil and Commercial Code, Articles 318–319: correspondence by any means and assessment of the reliability of media and technical procedures. Official online source

[15] Colombia. Law 527 of 1999, Articles 5–13, 16–25, and 28: data messages, written form, originals, integrity, admissibility, retention, dispatch, receipt, and digital signatures. Official online source

[16] Ecuador. Law on Electronic Commerce, Electronic Signatures, and Data Messages, Law 67, Articles 2, 6–8, and 10–16: equivalence, written form, originals, retention, origin, dispatch, receipt, and electronic signatures. Official online source

[17] Spain. Civil Procedure Law, Articles 326 and 384: private documents, challenges, instruments for archiving, accessing or reproducing data, examination, custody, and sound judicial assessment. Official online source

[18] Mexico. Federal Criminal Code, Articles 199 Octies and 199 Nonies, compilation including the amendment of 13-03-2026: certain conduct involving nonconsensual intimate sexual content, even where the material does not depict the identified person. Official online source

[19] Regulation (EU) 2024/1689 on artificial intelligence, Article 50, consolidated text as of 27-07-2026: transparency for certain deepfakes and adaptations for creative, satirical, artistic, or fictional works. Official online source