ACCCF / Applied Knowledge Library

08

VOLUME

Preserving content and verifiable context

Spanish edition · 2026

Email, Online Post, and Social Media Certification Manual

EML, headers, URLs, files, posts, traceability, and presentation

Preserve what is needed to review a message or post before it disappears, without confusing a screenshot with the source or an on-screen date with proof of origin.

For lawyers, forensic examiners, compliance and communications professionals, investigators, and anyone who needs to preserve an email, online post, or conversation. Notarial, expert, or administrative certification depends on the territory and procedure.

Editorial coordination: Jocsan Laguna · American Council on Cybersecurity and Forensic Computing

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

The visible pagination corresponds to the PDF edition. Word may update this table of contents when the document is opened; headings retain internal navigation.

Introduction: preserve before it changes 3
Chapter 1. Scope and preparation 3
- **1.1 What needs to be proven** 3
- **1.2 Prepare the capture environment** 4

Chapter 2. The complete message 4
- **2.1 EML: body, headers, and attachments** 4
- **2.2 Forwarding, downloading, and conversion** 4
- **2.3 Attachments and third-party delivery** 5

Chapter 3. Channel authentication 5
- **3.1 Received headers and transport** 5
- **3.2 DKIM, SPF and DMARC** 6
- **3.3 Date, Message-ID and content** 6

Chapter 4. Files, URLs, and posts 7
- **4.1 Complete URL record** 7
- **4.2 Posts, threads, and media** 7
- **4.3 Web archives and third-party dates** 7

Chapter 5. Documented preservation and certification 8
- **5.1 Acquisition record** 8
- **5.2 Custody and access control** 9
- **5.3 Expert, notarial, or administrative certification** 9

Chapter 6. Takedown, reporting, and reputational harm 9
- **6.1 Preserve before takedown** 9
- **6.2 Harm and scope** 9
- **6.3 Integrated case study** 10

Appendix A. Preservation templates 10
- **A.1 Email record** 10
- **A.2 Post record** 10
- **A.3 Object manifest** 11
- **A.4 Takedown request log** 11

Appendix B. Legal framework and final checklist 11

Introduction: preserve before it changes

A post can be edited, an account can be closed, an attachment can be replaced, and a link can stop working. Preservation seeks to record what existed at a given time, where it was located, how it was obtained, and what representation remains. A screenshot can show a fragment, but review requires the complete object and its context: URL, account, date, time zone, files, replies, metadata, and acquisition process.

Email provides a clear example. Preserving only an image of the message loses headers, structure, and attachments. Saving only the attachment loses the statement describing its contents and, in some cases, the hash used to verify it. EML brings these components together and allows them to be related. It does not prove that every statement is true or that a specific person wrote the body.

Here, “certification” means a documented process, not a universal guarantee. A notarial act, an expert examination, a preservation record, and a witnessed screenshot can have different functions and effects. The person preserving evidence must state what they did and what they can prove; solemnity must not be used to conceal an incomplete source.

> **Golden rule**
> Preserve content and context at the same time. A sharp image of a post without a URL or date is a useful reference, not a complete reconstruction of the object.

Chapter 1. Scope and preparation

1.1 What needs to be proven

Proving that a post existed is different from proving that an account published it, that a person wrote it, that it was publicly available, that it contained a threat, or that a specific file was delivered. The allegation determines the source: visible post, export, EML, platform records, recipient, administrator, or witness. If you only need to establish existence on a date, do not expand the analysis into authorship.

Define the period, accounts, URLs, keywords, participants, content types, and third-party data. Also define whether preservation will support a report, takedown, legal proceedings, internal investigation, or archival record. Urgency does not eliminate the need for authority or third-party protection.

Objective	Priority source	Limitation to declare
Existence of a post	URL, content, page, and documented preservation.	Does not establish human authorship or the completeness of the account.
Email content	EML with body, headers, and attachments.	Does not prove the text is true.
Delivery of files	Attachments, body, hash, download, and manifest.	Does not establish the coverage of the source system.
Public reach	Visibility, audience, link, and access evidence.	Does not equal the actual number of readers.
Authorship or control	Account, sessions, devices, and context.	A visible name does not identify the person.
Sequence	Dates, time zone, replies, edits, and references.	An isolated screenshot does not establish the complete sequence.

1.2 Prepare the capture environment

Use an authorized device and account, with date and time zone recorded, a known browser, and controlled storage. Avoid signing in with a personal account that adds unnecessary data to the evidence. Do not interact with the post more than necessary: replying, reporting, or sharing can change its reach and alert the author.

Prepare folders for originals, working copies, screenshots, exports, logs, and the manifest. Do not distribute potentially illegal or harmful content to the entire team. Document its presence and deliver it through a restricted channel. If someone is at risk, prioritize their safety and contact the appropriate channels rather than pursuing an additional technical demonstration.

> **Preliminary decision**
> If a post may disappear and you have authority to preserve it, record the object and its context first. Then request a takedown or review. Removing it before preservation can leave only an allegation without a source.

Chapter 2. The complete message

2.1 EML: body, headers, and attachments

RFC 5322 describes the internet message format, with header fields and a body. EML preserves a representation of an email with these components and any attachments. Document how it was obtained: client export, server download, or delivery by another person. Provenance changes interpretation and must not be hidden beneath a familiar file extension.[1]

Preserve the file before opening it with tools that could modify it. Hash the EML and each attachment separately and link them in the manifest. The body may declare an algorithm and value for a file: verify them rather than merely copying them into a separate note. If there is a discrepancy, preserve the original delivery and request clarification.

2.2 Forwarding, downloading, and conversion

Forwarding an email can add headers and change the relationship between the message and its files. Printing to PDF preserves a rendering, not the structure. Downloading from webmail can produce different formats. Record each operation and preserve the versions, without treating a forwarded message as necessarily identical to the original.

A forwarded message can still be useful evidence of what that person received on that date, but its earlier content must be analyzed using headers and complementary sources. If the goal is to establish delivery of a file, the provider's original EML is preferable to a screenshot of the forwarded message. If it is unavailable, declare the limitation and seek the message in another mailbox or server.

Representation	What it preserves	What requires supplementation
Original EML	Available body, headers, and attachments.	Provenance and content verification.
Forwarded EML	New delivery and representation of earlier content.	Forwarding history and earlier origin.
Email PDF	Layout and readable text.	Headers, attachments, and structure.

[1] RFC Editor. RFC 5322, Internet Message Format: message structure, headers, and body. It is a technical reference for preserving and understanding email, not automatic proof of a person's identity. Official online source

Representation	What it preserves	What requires supplementation
Screenshot	Fragment shown on screen.	URL, account, date, context and file.
Attachment only	Data from a file.	Message, statement, relationship, and process.

2.3 Attachments and third-party delivery

Do not edit or convert an attachment to make it easier to read before preserving it. Calculate its hash, check it against the declared value, and record whether it opens and its coverage. If a CSV opens but lacks a data dictionary, request the meaning of its fields. A hash does not prove that rows are complete or true: it establishes equality between the two objects compared.

> **Fictitious scenario**
> A provider delivers a CSV and a PDF with a hash for each in the email body. The CSV matches; the PDF does not. Preserve everything, request a new PDF delivery, and record that the CSV matches the declaration without asserting that the provider's content is complete. The second delivery receives another identifier; it does not replace the first.

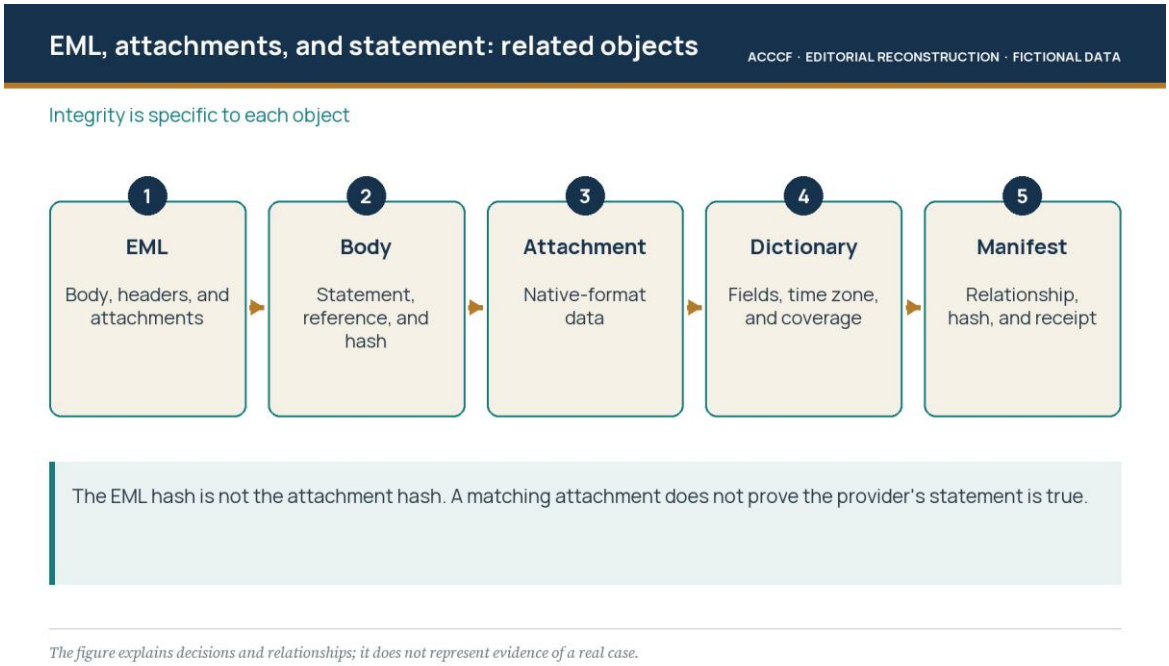


Figure 1. EML, attachments, and statement: related objects. Integrity is specific to each object. Editorial reconstruction; not actual evidence.

Chapter 3. Channel authentication

3.1 Received headers and transport

Received fields provide a declared sequence of servers, dates, and transport data. Review them in the order defined by the message structure, without assuming that all are necessarily trustworthy or that the first visible field corresponds to the human sender. Intermediate systems can add fields. The analysis compares servers, times, domains, and other authentication results.

The visible From address may not match the authenticated domain or sending server. An IP address in a header can identify infrastructure, not a person. Dates may depend on different clocks. The analysis does

not turn a complex header into magic proof; it explains which components are verifiable and which rely on trust.

3.2 DKIM, SPF and DMARC

DKIM associates a domain with a message through a cryptographic signature and allows signed components to be verified. SPF publishes which hosts are authorized for a domain within the protocol context; DMARC provides domain alignment and policy. These mechanisms help assess channel and domain, but do not prove who wrote the text or whether it is true. A failure may also require review of forwarding, configuration, or transformations.[23]

The report records the domain, selector, signed fields, result, date, and query source when available. Writing “DKIM pass” is not personal identification. Likewise, “SPF fail” does not by itself prove malicious spoofing: review the path and configuration. The technical analysis preserves the original message so another person can verify it.

3.3 Date, Message-ID and content

Message-ID can help relate messages and systems, but its uniqueness and structure depend on the generator. Preserve dates literally with their time zones and compare them with server logs and receipt events. The download date is not the send date. An attachment date is a separate layer.

Allegation	What can be verified	What does not follow
Authenticated domain	Signature, alignment and channel configuration.	A specific person wrote the message.
Send date	Consistent headers and logs.	The text was created at that exact moment.
Received message	Mailbox, EML, and server logs.	The person read or understood it.
True content	Sources independent of the reported event.	DKIM or a hash proves the event.
Compromised account	Sessions, recovery and abnormal activity.	A different address alone proves theft.

Reading principle

Headers are analyzed as evidence of transport and domain, not as a confession by a person. Authorship requires additional corroboration.

[2]RFC Editor. RFC 6376, DomainKeys Identified Mail (DKIM) Signatures: domain responsibility and cryptographic verification of signed components. It does not by itself establish who wrote the text or whether the content is true. Official online source

[3]RFC Editor. RFC 8616 and the technical references SPF RFC7208, DKIM RFC6376, and DMARC RFC7489: host authorization, domain signing, alignment, and policy. They help assess the channel; they do not by themselves establish human identity or content truthfulness. Official online source

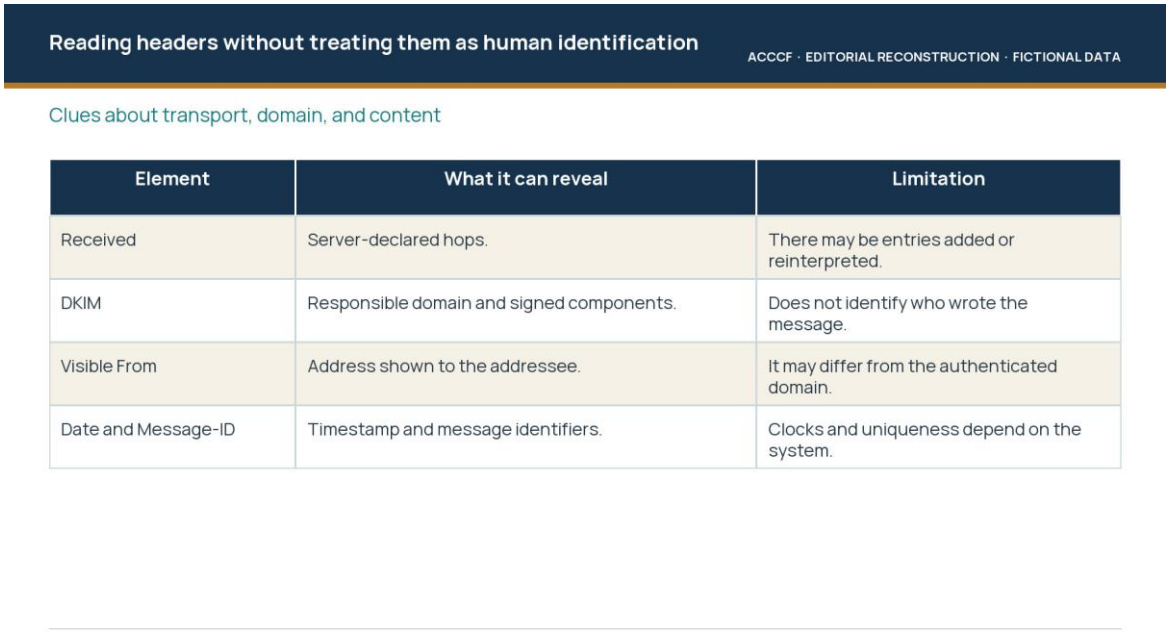


Figure 2. Reading headers without treating them as human identification. Clues about transport, domain, and content. Editorial reconstruction; not actual evidence.

Chapter 4. Files, URLs, and posts

4.1 Complete URL record

Preserve the complete URL, parameters, domain, date and time zone, visible account, access type, role, language, browser version, and page state. Record any redirect, sign-in, geographic restriction, or error. A URL can serve different content without changing its address, so preserve the object and the retrieval process.

The screenshot must include enough context to identify the page without exposing unnecessary data. Include the HTML file when useful and lawful, multimedia resources, a native export, and a description of what could not be obtained. A dynamic page may show different content to each visitor; the report must not generalize it as a universal view.

4.2 Posts, threads, and media

Preserve the text, apparent author, post identifier, visible date, URL, relevant replies, quotes, reposts, reactions, and media. Reply order may change due to algorithms or moderation. When capturing a thread, record how you scrolled and how far the coverage extends. A single reply out of context can distort the conversation.

Download the image or video file when authorized and hash it separately. Link the post to the file in the manifest. If content authenticity is being investigated, apply the specific multimedia analysis volume; preservation only establishes that this version was available from that source at that time.

4.3 Web archives and third-party dates

A third-party archive may preserve a useful snapshot, but its date belongs to its capture, not necessarily to the first publication. Record who archived it, which version was captured, which resources are missing, and how it was accessed. A date in the content may have been edited by the author or use another time zone. Corroboration seeks posts, notifications, links, and records with nearby dates.

Element	Required record	Limitation
URL and redirects	Full address and access sequence.	Changing or personalized content.
Post and thread	Identifier, text, replies, and captured coverage.	Not the entire conversation if coverage was limited.
Multimedia	File, quality, hash, and provenance.	Does not establish scene authenticity or authorship.
External archive	Custodian, snapshot, date, and missing resources.	Does not establish first publication or complete content.
Access	Account, role, visibility and restrictions.	Not all users saw the same thing.

Presentation principle

Do not use a web archive to claim “it always looked this way” or a screenshot to claim “this is everything.” Describe the version, date, and coverage you can actually establish.

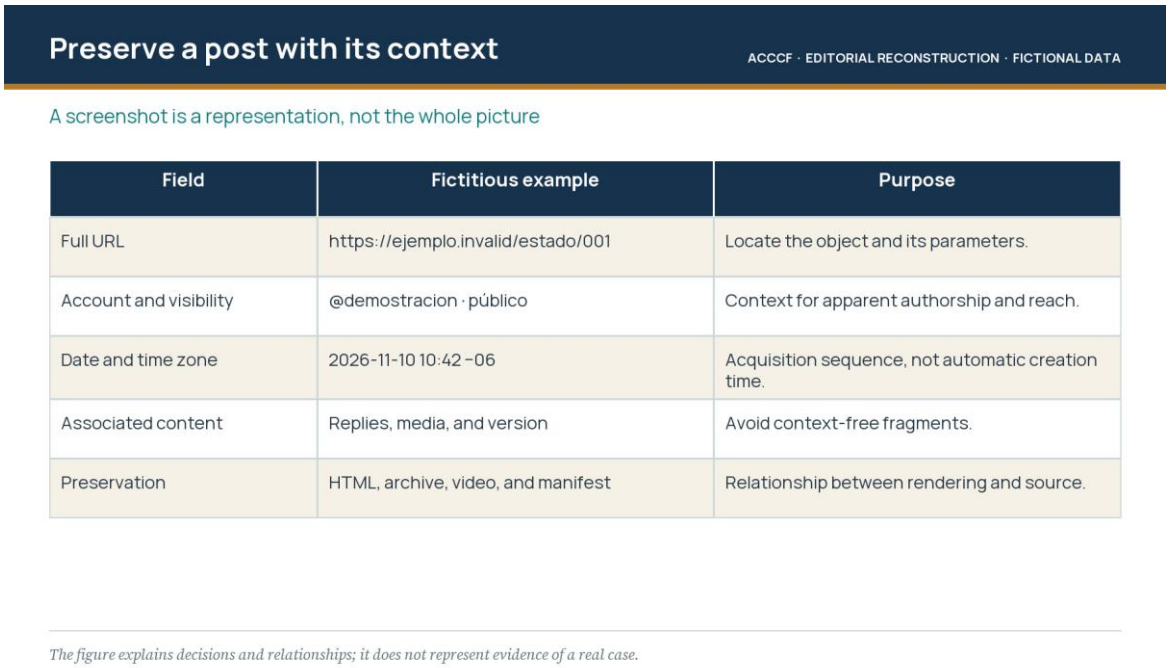


Figure 3. A post is preserved with its context. A screenshot is a representation, not the whole picture. Editorial reconstruction; not actual evidence.

Chapter 5. Documented preservation and certification

5.1 Acquisition record

The record identifies the case, operator, authority, location, date and time zone, device, browser or tool, account and role, objects acquired, actions, formats, issues, and hashes. For screen capture, record navigation and filters. For export, record parameters and output. For a provider, preserve the response and channel. The record describes what was done, not an ideal procedure that did not occur.

A preservation record can complement proof of integrity and accessibility. In Mexico, NOM-151 has specific requirements for preserving and digitizing data messages within its scope; it does not certify

content as true or replace acquisition of the complete message. A timestamp or hash does not prove human authorship or lawful acquisition.[45]

5.2 Custody and access control

Separate the source from the working copy and restrict access. Electronic transfers include the recipient, permissions, date, version, key delivery channel, and download verification. The report must not contain passwords, tokens, or cookies. When preserving an authenticated page, document the role without exposing the session.

Use the working copy for analysis, redaction, and presentation. Review the public version to avoid exposing personal data, intimate images, addresses, and unrelated third parties. Do not destroy the complete preserved version when creating a redacted one; restrict its access and subsequent use.

5.3 Expert, notarial, or administrative certification

The choice depends on jurisdiction, object, and purpose. A notarial act can document a viewing; an expert examination can analyze origin, structure, authenticity, relationships, and context; an administrative record can attest to an action within its scope. None turns a fragment into complete evidence. Request the appropriate form before starting so you do not repeat actions on a page that may change.

> **Quality criterion**
> The best certification is not the one with the most stamps, but the one that allows another person to understand what was seen, where, when, by what method and what was left out.

Chapter 6. Takedown, reporting, and reputational harm

6.1 Preserve before takedown

Before requesting a takedown, preserve the URL, identifier, post, account, media, replies, and access date. Also record any versions that have already changed and reference links. If there is an immediate threat, prioritize safety and emergency channels; preservation must not become a dangerous delay.

The platform report must be specific: object, URL, reason, evidence, date, and request. Include no more personal data than necessary and do not send the harmful file to channels not intended for it. Preserve the report number, content, date, and responses. Removing a link does not prove that every copy has disappeared or that the harm has ceased.

6.2 Harm and scope

The analysis separates content, reposting, visible reach, reactions, and reported consequences. Platform counters may mean different things and do not establish individual readers or total impact. Preserve metrics with their date and meaning when known. Do not calculate economic loss by multiplying impressions without a basis.

Assessing reputational harm may require testimony, employment documents, contracts, communications, and other non-digital sources. Technical preservation establishes content and

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

[5]Ministry of Economy. PLATIICA. NOM-151-SCFI-2016 record, preservation and digitization of data messages. Review of current status and supplementary reference to the DOF text. Official online source

sequence, not the full extent of harm. The report must not invent owners of anonymous accounts or assign intent based on a post's tone.

6.3 Integrated case study

A fictitious post contains an accusation and several replies. Preserve the available thread, files, and metrics with their dates. The account then edits the text and deletes a reply. Preserve the first version with its limitations and the new version as a related object. The analysis compares changes without erasing history. Record the takedown request, but do not assert that the content stopped circulating on other accounts.

> **Lesson**
> Evidence of reputational harm is built from versions and context. A final screenshot may show less than the first, but the first does not prove the entire course of events either.

Appendix A. Preservation templates

A.1 Email record

Fictitious record

```
Case / object: EXP-DEMO-2026-008 / EML-001-R00
Source: [mailbox, server, client, or third party]
Acquisition method: [export, download, or delivery]
Apparent sender and recipients: [record]
Message date and time zone: [literal value]
Acquisition date and time zone: [literal value]
Body and statements: [reference, algorithm, and hash]
Headers: [complete file]
Attachments: [names, sizes, formats, and hashes]
Authentication: [DKIM / SPF / DMARC if reviewed]
Verification: [coincidences and differences]
Issues: [format, absence, error, or limitation]
Custody: [original, working copy and access]
```

A.2 Post record

Field	Minimum content	Control
URL and identifier	Complete address, parameters, and redirects.	Locatable object.
Account and visibility	Apparent author, role, access and visible audience.	No automatic attribution.
Dates	Visible date, acquisition date, time zone, and precision.	Do not confuse publication and download.
Content	Text, replies, reactions, media, and version.	Thread coverage.
Process	Tool, version, filters and actions.	Repeatability.
Files	HTML, image, video, export and hash.	Original / derivative relationship.
Issues	Error, access, missing content, and limitation.	Do not hide coverage limitations.

A.3 Object manifest

Delivery inventory

```
ID / original name / object type
Source and relationship: [original, export, derivative]
Receipt date and time zone
Method and tool / version
Size and format
Object algorithm and hash
Parent object and related objects
Opening and verification
Sensitive data and restrictions
Preserved location and working copy
Transfers and recipient
Limitations and outstanding items
```

A.4 Takedown request log

Fictitious template

```
Platform and channel: [official]
URL / post / account: [specific object]
Reason and attached evidence: [identifiers]
Request: [takedown, review, preservation]
Date and time zone: [sent]
Report number: [reference]
Response: [date, content, and action]
Other known copies: [URL and status]
Communication with affected persons: [channel and version]
Outstanding: [coverage and next review]
```

Appendix B. Legal framework and final checklist

Mexico recognizes data messages in CCom 89–94 and 1205; the CFPC/CNPCF develops reliability, attribution, and integrity according to the transition; NOM-151 regulates preservation within its scope. Peru separates signature, procedure, and archives; Chile distinguishes signature types and dating; Argentina assesses reliability; Colombia and Ecuador require preservation of format, origin, destination, and dates; Spain combines eIDAS, the LEC, and trust services. No rule makes a message true merely because it is electronic.[6][7][8][9][10][11][12][13][14][15][16]

Preservation is also constrained by privacy and third-party rights. Restrict roles, access, and dissemination; separate working and public versions; avoid publishing intimate content, minors' data,

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

[7] 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

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

[9] Peru. IOFE Regulations, DS 052-2008-PCM, Articles 3 and 4: requirement for and admissibility of digitally signed electronic documents. Official online source

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

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

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

[13] 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

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

[15] Regulation (EU) 910/2014 (eIDAS), Articles 25–26 and 46: non-discrimination against electronic signatures and documents based on their format, advanced signatures, and the legal effects of qualified signatures. Official online source

[16] Spain. Code of Civil Procedure, Articles 326 and 384: private documents, challenges, instruments for storing, accessing, or reproducing data, examination, custody, and sound judicial evaluation. Official online source

secrets, or credentials. Deliver evidence through the authorized channel with a manifest, not as a public collection of files.[17][18][19]

Final checks	Acceptance question
Item	Are the EML, URL, files, and context available?
Process	Was the person who obtained it recorded, along with their role, filters, and date?
Integrity	Does each hash correspond to an object and a point in time?
Channel	Were DKIM / SPF / DMARC interpreted within their limits?
Coverage	Were the thread, replies, and omissions declared?
Attribution	Were accounts and people kept distinct?
Privacy	Does the delivery prevent unnecessary exposure?

Closeout

Preservation means leaving a verifiable trail of what existed at a given time, not collecting screenshots until they seem sufficient.

[17]Mexico. Federal Law on the Protection of Personal Data in the Possession of Private Parties, text published on 20-03-2025 and amended on 14-11-2025. Articles 5–9, 18–20, and 31: principles, security, confidentiality, data breaches, and the handling of rights requests. The current federal authority is the Secretariat of Anti-Corruption and Good Governance. Official online source

[18]Colombia. Statutory Law 1581 of 2012, Articles 4, 8, 12, 17–18, and 26: principles, rights, information, duties of controllers and processors, and transfers to third countries. Official online source

[19]European Union. Regulation (EU) 2016/679, Articles 5, 25, 28, and 32–34: principles, data protection by design, processors, security, and notification/communication of personal data breaches. In Spain, applicable national and sector-specific legislation must also be reviewed. Official online source