ACCCF

APPLIED KNOWLEDGE · HISPANIC AMERICA

HISPANIC DIGITAL EVIDENCE MANUAL 2026 V1

Preserve, verify, and explain digital evidence in the Spanish-speaking world.



Prepared and signed by

Jocsan Laguna Romero

President of ACCCF

Institutional issue of the Council

Contents

General technical guide. It does not constitute legal advice or an expert opinion. Examples are fictitious or anonymized; figures are editorial reconstructions.
Visible pagination corresponds to the PDF edition. Word may update this index when the document is opened; headings retain internal navigation.

Introduction to the guide 6
How to use this guide 7
Chapter 1. Scope, questions, and authority 8
1.1 The question that governs the work 8
1.2 Authority before access 8
1.3 Initial source inventory 9
1.4 Complete example: a sales claim 10
1.5 Basis and conclusion: the method also protects people 11
Chapter 2. Integrity, originals, and context 13
2.1 The original is not always the device 13
2.2 Integrity, authenticity, attribution, and truthfulness 13
2.3 Hash as a control, not a dogma 14
2.4 Internal metadata and system dates: a distinction that prevents errors 15
2.5 The case of the photographs and the bench 16
2.6 Accessibility and context preservation 16
Chapter 3. Roles, responsibilities, and decisions 18
3.1 Functions before job titles 18
3.2 First response without improvisation 18
3.3 Operational communication 19
3.4 Independence, privacy and third parties 20
3.5 A syllogism of roles 20
Chapter 4. Lifecycle and forensic readiness 22
4.1 Prepare before receiving a case 22
4.2 Points of no return 23
4.3 Documented lifecycle and deliverables 24
4.4 Longitudinal retention and analysis 25
4.5 Preparedness as a social responsibility 26
Chapter 5. Decision trees by scenario 27
5.1 Device powered on or off 27
5.2 Local, remote, or provider acquisition 27
5.3 Mobile devices and isolation 28
5.4 Optical discs: identifiers and format 29
5.5 When to stop 30

5.6 The tree as reasoning, not decoration 31
Chapter 6. Modern sources and call detail records 33
6.1 Cloud, SaaS, and exports 33
6.2 Email and EML 33
6.3 Requesting and receiving call detail records 34
6.4 Example provider request body 35
6.5 Virtualization, IoT, and synthetic content 36
6.6 Verifying that law is in force: the example of a repealed reform 37
6.7 The source does not reside in only one place 38
Chapter 7. Initial receipt and preservation 40
7.1 A clear receipt record 40
7.2 Packaging and sealing 41
7.3 Labels and relationships between objects 42
7.4 Accessories and connections as part of receipt 43
7.5 Receipt of files and messages 44
Chapter 8. Acquisition and technical documentation 45
8.1 Physical, logical, volatile, and documentary acquisition 45
8.2 Actual connection: source, write blocker, and workstation 45
8.3 Media and adapters: NVMe, SATA and optical discs 46
8.4 Logical acquisition and manifest 47
8.5 Live memory and tool validation 48
8.6 Reproducible exports and queries 49
8.7 Errors and incidents 49
Chapter 9. Custody, transfer, and preservation 51
9.1 The chain that answers questions 51
9.2 Electronic transfers and keys 51
9.3 Storage and subsequent access 52
9.4 Opening and replacing seals 53
9.5 Access, shared custody, and conflicts 54
Chapter 10. Examination, timelines, and alternative hypotheses 56
10.1 Examining is not finding a culprit 56
10.2 Metadata: listen to the file without believing everything 56
10.3 Timelines: reconcile clocks before constructing the account 58
10.4 Antennas, coverage, and azimuth: geography without shortcuts 59
10.5 Corroboration that actually discriminates 61
10.6 Hypothesis matrix: allow the evidence to contradict 62
10.7 Repeat, reproduce, and know when to stop 63
Chapter 11. Reporting, reasoning, and challenge 65
11.1 The report is the way back to the source 65
11.2 Fact, result, inference, and opinion 66

11.3 The syllogism and the false consequence 66
11.4 Explain contradictions without hiding them 67
11.5 Draft conclusions that fit the evidence 67
11.6 Challenge and independent review 68
11.7 Delivery, annexes and subsequent access 69
Chapter 12. Errors, learning, and public service 71
12.1 Errors are not corrected by rewriting the past 71
12.2 Receipt and preservation errors 71
12.3 Source, capture and export errors 72
12.4 Errors of interpretation 73
12.5 Legal and applicability errors 74
12.6 Lessons learned that change the procedure 75
12.7 The final measure: prevent the next abuse 76
Annex A. Functional legal equivalents 77
Executive summary 77
1. Method and limits of the comparison 77
2. Core matrix by legal function 78
3. Mexico: legal framework and transition 85
4. Peru: distributed regime and financial update 87
5. Chile: signatures, dates, and security regulation 88
6. Argentina: limited presumptions and reliability of the medium 89
7. Colombia: data messages, preservation, and acknowledgments 90
8. Ecuador: documentary equivalence and payment system 91
9. Spain and the European Union: non-discrimination, trust services, and procedure 92
10. Functional comparison of financial records and incidents 94
11. International methodological standards 97
12. Rules for using the matrix without false equivalences 98
A.13 Practical application: select the regime before the conclusion 99
A.14 Data protection during an investigation in Mexico 100
Annex B. Scope and authority form 101
B.1 Form content 101
Annex C. Receipt and initial preservation record 103
C.1 Example physical receipt record 103
C.2 Receipt of files or messages 104
Annex D. Acquisition record 105
D.1 Complete example 105
Annex E. Chain of custody and transfers 107
E.1 Example of sequence 107
E.2 Electronic transfer 107
Annex F. Request and acquisition through a provider 108

F.1 Model request....108
F.2 Export or API record....108
Annex G. Inventory and manifest of objects....110
G.1 Example of manifest....110
Annex H. Timeline and time zones....111
H.1 Example of timeline....111
H.2 Rule for conflicting dates....111
Annex I. Hypothesis and corroboration matrix....112
I.1 Worked example....112
Annex J. Review of synthetic content....114
J.1 Applied format....114
Annex K. Report structure and conclusion....115
K.1 Recommended sequence....115
K.2 Example of a complete conclusion....116
Annex L. Operational checklists....117
L.1 Receipt and acquisition....117
L.2 Analysis, reporting and delivery....117
Annex M. Version, source, and lesson control....119
M.1 Regulatory and technical record....119
M.2 Turning a lesson into improvement....119

Introduction to the guide

Preserving digital evidence does not mean storing files until there seem to be enough. It means protecting the possibility that another person, using different judgment and tools, can reach a conclusion consistent with the facts. A device is no substitute for a witness; a screenshot is no substitute for the file; an opinion is no substitute for method. The work begins long before the first file is opened: it begins when someone decides which assertion must be established and what the consequences of acting will be.

This guide arises from an uncomfortable but necessary question: how many abuses could be avoided if the first person to receive evidence performed the simplest tasks correctly? Identify the object, photograph its condition, define the authorization, request the native file, preserve the complete message, record the date and time zone, do not confuse an antenna with a person, and do not present intuition as science. The foundations are not ornamental. They prevent an accusation from being built on an assumption and a defense from collapsing because of an avoidable omission.

The rule governing everything else can be stated as follows: source, authority, condition, method, record, verification, and limited conclusion. First identify what can provide information. Then verify who can authorize access and under what conditions. Document the condition in which the object arrives, select an appropriate method, and make a record. Only then verify and conclude within what the sources permit. If one phase fails, the next cannot be repaired with rhetoric: acknowledge the limitation and decide what can be recovered without fabricating a perfect account.

Magical realism, as used here, is not literary ornamentation. It is the recognition that everyday objects can tell something extraordinary: a bench can describe a pause, a spindle ring can identify a disc, a bag can create a false sense of isolation, and one clock can contradict another. Analogies are bridges to understanding, not substitutes for evidence. Rigor means always returning to the source and asking what it can establish and what it merely appears to suggest.

Purpose of this work
Provide foundations so that no one has to learn digital evidence the hard way. Share a method that police officers, forensic experts, lawyers, engineers, and organizational leaders can use without concealing difficult decisions or areas of uncertainty.

The examples are fictitious or anonymized. The images are editorial reconstructions: they show devices and actions but do not constitute actual case evidence. Legal sources are cited with their function, article, scope, and consultation date. When an equivalence between countries is only partial or sector-specific, this is stated explicitly, because similar wording does not produce the same legal effect.

How to use this guide

If you are the first person to receive a case, start with Chapters 1, 3, 5, and 7. They explain how to define the assignment, allocate functions, choose a path based on the object's condition, and document receipt without improvising. You do not need to become an analyst to avoid the initial errors: you need to know what to preserve and when to ask for help.

If you acquire or analyze evidence, work through Chapters 4, 6, 8, 9, and 10. The technical chapters explain how to select sources, document acquisitions, verify files, build timelines, and evaluate alternative hypotheses. If you present or review evidence, use Chapters 2, 11, and 12 and the legal and operational annexes. The goal is not to repeat a procedure but to understand why each decision leaves a useful trace.

Forms are not an end in themselves. An empty record with an attractive filename can still amount to pseudo-custody, just as a photograph without a URL may be only an incomplete image. Each form must capture a decision or verification: what was authorized, what was received, what changed, who verified it, and what limitations exist. If a field does not help answer those questions, remove it.

The reading is cumulative. Concepts return because each adds a layer: a source may be original in a limited sense, an export may be a better source than the device, an antenna describes coverage rather than a direction, and a signature may carry legal weight without showing which hand pressed the button. Do not rush toward the commands. Speed comes once your judgment is clear.

Chapter 1. Scope, questions, and authority

1.1 The question that governs the work

A poorly formulated assignment produces an inflated investigation. “Review everything” does not state what must be established, how the result will be used, or what risk of alteration is acceptable. A precise question, by contrast, makes it possible to decide which sources are necessary and which must not be touched: which transactions are disputed, during which period, in which systems, and with what legal or business consequences.

Write down the parties’ accounts separately. One party claims to have made sales that were not paid for; the other maintains that it did not receive those transactions. Do not merge them into a single account. The first hypothesis must not become an instruction to search only for information that confirms it. The second must not be dismissed because it is inconvenient. The method’s function is to allow both to be tested, not to help one win in advance.

Recovery for operational continuity does not require the same level of rigor as a forensic examination intended for judicial challenge. In the first case, a controlled copy that lets you resume work may suffice. In the second, you need authority, integrity, context, traceability, reviewability, and an explanation that does not depend on the signatory’s prestige. Confusing these objectives produces two errors: doing too much for a simple recovery or doing too little for an assertion with serious consequences.

Question	What must be documented	A decision that prevents improvisation
What does each party allege?	Separate accounts by person, fact, and date.	Do not treat an account as a proven fact.
What needs to be established?	Fact, period, system, and expected result.	Define the sources and method.
What will it be used for?	Operational continuity, internal investigation, forensic examination, or proceedings.	Define the level of documentation.
What may fall outside the scope?	Excluded data, devices, accounts, or periods.	Reduce unnecessary exposure.

1.2 Authority before access

Being able to open a file does not mean being authorized to examine it. The authorization must identify the holder, permitted actions, systems, responsible persons, exclusions, and communication channel. If access to third-party information, a shared account, or a provider is

required, document the lawful means. Technical capability does not create authority; it only permits what authority allows.

Proportionality asks whether the source and method are necessary for the objective. An administrative export may provide a better answer than a complete device review, with less alteration and exposure. Collecting everything is not thoroughness: it can create noise, expose data, and elegantly obscure the question. If a source offers greater discriminating power with less intrusion, it is the initial candidate.

Confidentiality is decided on receipt, not at the end of the report. Determine who may view, copy, transfer, and publish information, especially when third parties, minors, victims, or trade secrets are involved. Personal data processing must be lawful, limited to stated purposes and what is necessary, with security and confidentiality measures proportionate to the risk. The new law also requires significant breaches to be reported immediately so that individuals can protect themselves.[1]

Operational rule
If authority or scope is unclear, stop and clarify it. Record the question, the answer received, who provided it, and when. "I did not know whether I was allowed" is not a defensible chain of custody.

1.3 Initial source inventory

Compile a list of devices, accounts, files, servers, providers, documents, and people who can provide context. Include unavailable sources and the reasons: a lost device, unknown password, expired retention period, unresponsive provider, or unauthorized access. Absence also changes the plan and possible conclusions. An incomplete case file must not be presented as a complete universe.

Prioritize according to the ability to resolve hypotheses, volatility, and risk of loss. RAM, an active session, a rotating log, and an expiring link may each require different actions. Priority is determined not by which device seems most important, but by which information may disappear first and which question it answers. Ockham's razor starts with the source that best discriminates, not the one with the greatest technical prestige.

Inventory field	Example of a useful record	Why it matters
Identifier and custodian	Commercial remittance, processor, bank, and authorized representative.	Avoid asking the wrong custodian for data.
Type, period and format	One week of transactions, native CSV, and a field dictionary.	Allows structure and meaning to be compared.

[1]Federal Law on the Protection of Personal Data Held by Private Parties, new law published on 20-03-2025 and amended on 14-11-2025. Articles 5–9, 18–20, and 31: principles, security, confidentiality, breaches, and time limits. Official online source

Inventory field	Example of a useful record	Why it matters
Availability	Missing file, active link, or pending provider.	Declare limitations from the outset.
Risk	Rotation, remote wiping, third-party exposure, or physical loss.	Define the priority and method.
Authorization and contact	Holder, secure channel, and alternate.	Avoid questionable access and undocumented delays.

1.4 Complete example: a sales claim

A retail chain claims that it made sales for which it was not paid. The question is not to “review all its computers,” but to determine whether the transactions were recorded, transmitted, and settled. Define the date, amount, reference, and processor. Priority sources are merchant reports, remittance files, processor records, interconnection equipment, and bank reports. Each source answers a different part of the sequence.

Authorization is limited to those systems and the relevant period. If the transactions do not appear in the remittance file produced by the store itself, the finding guides the investigation but does not yet establish who caused the discrepancy. The transactions may never have occurred, the remittance may be incomplete, another channel may have been used, or the export may be defective. A responsible conclusion begins with the absence documented in the source, not with an accusation against the first available suspect.

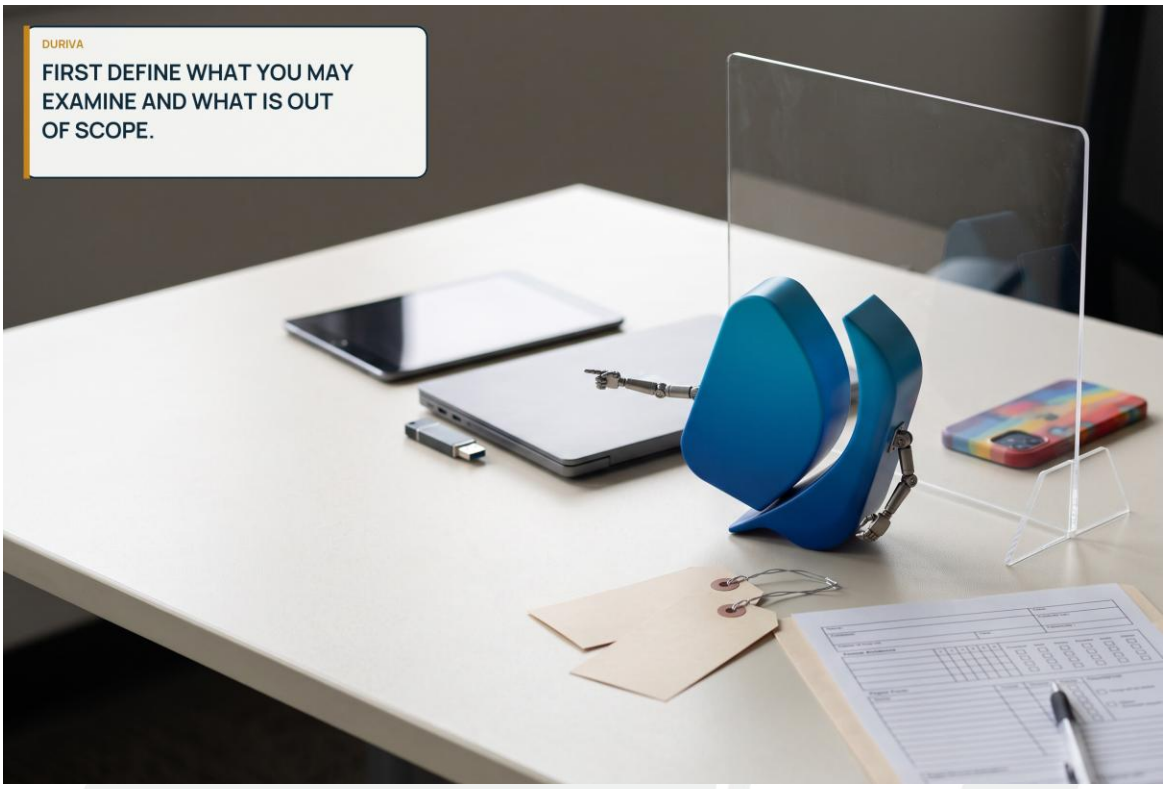


Figure 1. Define sources before acting: what can be reviewed and what is excluded. Editorial reconstruction; it does not constitute actual evidence.

What the example teaches
A well-defined question avoids an invasive review of personal devices and requires comparison of independent sources. Evidence is not accumulated by volume: it is selected for its ability to resolve an assertion.

1.5 Basis and conclusion: the method also protects people

Identification, collection, acquisition, and preservation are not merely technical operations. ISO/IEC 27037 presents them as decisions that must be documented to permit subsequent review. The source and authority shape the method; possession of a password or device alone does not create legitimate access. This sequence also prevents an investigation from becoming a second injury to those affected.[2]

In Mexico, electronic information may be admitted as evidence when the reliability of the method, attribution, accessibility, and integrity are established. That requirement is not met by an isolated screenshot or by an expert's assertion that they saw something on a screen. It must

[2]ISO/IEC 27037:2012. Guidelines for the identification, collection, acquisition, and preservation of digital evidence. Edition confirmed by ISO as remaining in force.Official online source

be possible to explain how the information was generated, communicated, received, or stored and how it was kept intact from generation onward. Precision delimits what can subsequently be asserted.[3][4]

Limited conclusion
Before handling evidence, you must be able to answer which assertion is being investigated, who authorizes it, which sources discriminate best, which exclusions protect third parties, and what result you expect. If any answer is missing, the first deliverable is not an acquisition: it is a documented clarification.

[3]Federal Code of Civil Procedure, Article 210-A: reliability of the method, attribution, accessibility, and integrity of electronic information. Code repealed by decree of 07-06-2023, subject to the gradual transition regime.Official online source
[4]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

Chapter 2. Integrity, originals, and context

2.1 The original is not always the device

In digital evidence, the notion of an original rests on integrity from the final form onward and on the ability to consult it later, not merely on retaining a device. A native file, bit-for-bit image, export, screenshot, and printout are different representations. Each can be useful if its relationship to the source and the information it preserves or loses is known. The question is not merely “Do I have the object?” but “What can I establish with this representation?”

A bit-for-bit image of the medium can preserve allocated and unallocated sectors; a logical export may preserve only certain files; a screenshot can display a view without preserving structure or metadata; a printout can make content readable without providing the original file. None is universally superior. The choice depends on the question and the need for review. Do not destroy the source object to produce a representation that later proves insufficient.

The Mexican Commercial Code addresses written form, originals, integrity, and accessibility in Articles 93 and 93 Bis, while Articles 348 to 350 of the CNPCF serve a similar function for electronic information. These rules do not turn every copy into an original or every PDF into a complete source. Document which representation you hold and how it was obtained.[5][6]

2.2 Integrity, authenticity, attribution, and truthfulness

Integrity means that the object remains complete and unaltered within the stated scope. Authenticity requires support for the claim that the object is what it purports to be. Attribution links an action or document to an origin; content truthfulness asks whether the events narrated occurred. Conflating these concepts produces overbroad conclusions: a file can be intact and still have been false since its creation.

A valid signature may give rise to presumptions of authorship and integrity under the relevant legal regime, but it does not prove that the individual pressed a particular button or that every statement is true. The review must include the certificate, validity period, method, context, and possibility of key compromise, as well as independent corroboration. Even a cryptographically valid sequence may require an explanation of who controlled the key and device at that time.

Defensible assertion	Evidence required	Assertion to avoid
The hashes match.	Same algorithm, object, and time documented.	The content is true.

[5]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

[6]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

Defensible assertion	Evidence required	Assertion to avoid
The file has not changed since then.	Hash calculated on receipt and subsequently verified.	The file was never tampered with.
The export contains these fields.	Provider method, parameters, and format.	The export is complete.
No activity was observed within the scope.	Sources, filters, period and reproducible query.	The activity never existed.

2.3 Hash as a control, not a dogma

A hash function produces a value that allows objects to be compared. If two files have the same value under the same algorithm, their bit-for-bit content matches within the comparison performed. If a file changes, the value changes. This helps detect substitutions or differences, but does not explain why they occurred or establish origin, date, authorship, or truthfulness.
Record the algorithm, operator, date and time zone, exact object, location, and relationship to the evidence. SHA-256 is a common choice for integrity checking, not a magic word. Two different representations of the same information can have different values without proving falsity: a format conversion can change the file even when the visible content is similar. A newly calculated hash establishes integrity only from the moment it is calculated.

Appropriate wording for the report
"The received file had a SHA-256 hash of [value], calculated on [date and time zone]. Subsequent verification matched. This establishes that the object did not change between the two checks, not that it is authentic or complete from its origin."



Figure 2. A hash compares objects; it does not establish authorship or the truthfulness of content. Editorial reconstruction; it does not constitute actual evidence.

2.4 Internal metadata and system dates: a distinction that prevents errors

The properties displayed by an operating system may reflect when a file was copied, downloaded, or modified on that computer, not when it was originally created. Those dates are not useless: they help reconstruct the object's history on that system. The error is to present them as the original capture date without further verification. You must read what each field means, on which system, and for which assertion.

A photograph's internal metadata can include the capture date, device model, and coordinates if they were enabled. Tools such as ExifTool can read them. But they are not immutable and do not independently prove that the scene occurred as described. A file can be edited, its metadata can change, and a device clock can be wrong. The capture date is a source that must be corroborated with others: content, application logs, backups, locations, sequence, and testimony.

NOM-151 sets out requirements for preservation and digitization in Mexico. It does not replace the methodology for the case or establish the truthfulness of the content. Preservation must cover access conditions, integrity, relationship to the original, available metadata, responsible

persons, and any records or third parties involved. The visible date is only the start of a more rigorous question.[7]

2.5 The case of the photographs and the bench

In one case examined by the author, a set of photographs provided dates and coordinates compatible with a location different from the one alleged. The phone's accelerometer also showed a pause consistent with the moment when a person said they had sat on a bench. The significance lay not in the bench as an object, but in the pause: an everyday pattern that helped test an account without resorting to dramatic interpretation.

The sensors recorded neither sadness nor intent, nor did they turn the data into metaphysical certainty. They could be consistent with a sequence, but the conclusion required corroboration: photographs, messages, movements, cloud sources, testimony, and review of whether the data were generated by sensors or entered manually. Science is not expressed as "the phone told the truth," but as "these sources, given their origin and behavior, are compatible with this sequence and not the other."[8]

Methodological lesson
A source does not become true because it is abundant or sophisticated. Metadata helps when you understand what it is, when it was generated, what alteration is possible, and which other sources it matches. Confidence comes from convergence, not from an adjective.

2.6 Accessibility and context preservation

An inaccessible object cannot be reviewed. Preservation requires the ability to open, read, interpret, and relate information to its context. A proprietary file may require a particular software version, format documentation, or a supplementary export. A visual copy aids presentation but must not delete the native file or the data needed for verification. An attractive report that does not allow the source to be located is a presentation, not a complete investigation.

[7]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

[8]Jocsan Laguna. Libro abogados, chapter 1. Narrative research material supplied by the author. Names changed in the guide to protect identities.



Figure 3. Source, export, working copy, and printout: representations with different coverage. Editorial reconstruction; it does not constitute actual evidence.

Limited conclusion
Integrity does not equal authenticity, attribution does not equal physical identity, and a date does not equal an event. Document each concept separately to avoid turning a control tool into an absolute conclusion.

Chapter 3. Roles, responsibilities, and decisions

3.1 Functions before job titles

One person may perform several functions if the case permits, but each action must be associated with a specific function. Authorizing, executing, documenting, safeguarding, reviewing, and communicating are not the same. The director does not necessarily acquire evidence; the technician does not unilaterally decide what is published; the lawyer does not replace technical verification; and the custodian does not alter the source to facilitate analysis. For a law enforcement agency, this distinction allows personnel without engineering training to receive and protect the case without becoming improvised analysts. The first responder records the condition and risks, protects the object, and requests support. The specialist selects the method based on that intake, not an incomplete telephone description. The independent reviewer checks whether the assertion and evidence are related, regardless of who submitted the report.

Function	Primary responsibility	Expected record
Authority for the assignment	Defines the scope, permissions, and exclusions.	Authorization and approved changes.
First response	Identifies the condition, prevents loss, and requests support.	Initial record and photographs.
Specialist	Selects and executes the method.	Acquisition, tools, and incidents.
Custodian	Controls access, location, and transfers.	Chain of custody.
Reviewer	Reviews the method, findings, and limitations.	Observations and resolution.

3.2 First response without improvisation

The first responder does not need expertise in forensic acquisition to do this correctly. They must avoid powering on, exploring, or connecting devices without authorization; photograph the condition; record what is visible; and request support. If someone has already opened files, record that too; do not conceal it to make the receipt record look perfect. The receipt must state what happened before arrival, not the version that makes the sequence look ideal.

A visual inspection can provide guidance, but adding a table, screenshot, or conclusion does not turn it into a forensic examination. The digital forensics expert must explain the method, source, tool, parameters, verifications, and limitations. When someone without that expertise

presents a perception as scientific analysis, the problem is not vocabulary: it is methodological authority and reviewability.



Figure 4. Independent review tests the source, method, and conclusion; it does not merely correct style. Editorial reconstruction; it does not constitute actual evidence.

3.3 Operational communication

Before acting, establish who can answer technical, legal, and custody questions. The directory includes name, role, channel, availability, and alternate. Urgent decisions are recorded with a date and justification; an informal call must not be the only record of an irreversible action. Communication is part of the evidence for the decision, not a separate administrative note.

When material is delivered to a provider, preserve the conversation in a format that allows it to be reconstructed. If the provider sends files by email, retain the EML with its body, headers, and attachments. If an exclusion or new export is agreed, add it to the authorization and change log. If the response arrives through a link, document who opened it, with what permissions, on what date, and which version was downloaded.

Minimum communication record
Who made the request, to whom, what was authorized, through which channel, on what date, what changes resulted, and what subsequent verification exists. The conversation is not optional context: it explains why a decision was made.

3.4 Independence, privacy and third parties

Independent review seeks errors, not culprits. It checks whether the object is correct, whether the method answers the assignment, whether dates are consistent, and whether the conclusion goes beyond the findings. The reviewer may request that a query be repeated or a source added, but must not alter the original to make it match the preliminary version. A review that merely seeks to confirm what the analyst has already written is not independent.

Privacy requires separating the purpose of the investigation from unnecessary exposure. Third-party data must be reviewed using criteria of proportionality, security, and confidentiality. The privacy notice is not a ritual document: it explains which data are processed, for what purpose, who may access them, and how rights are exercised. If the case involves personal data, the controller must adopt necessary and sufficient measures without turning the examination into a public transfer of information.[9]

Since 2025, the federal authority for personal data protection has been the Secretaría Anticorrupción y Buen Gobierno, not the INAI. This change does not remove protection obligations or make every investigation an exception: it requires updating the recipient of a request or complaint where appropriate and avoiding citation of the former institute as though it were still the current authority.[10]

3.5 A syllogism of roles

Major premise: a forensic examination requires subject-matter expertise, method, and reviewability. Minor premise: a visual inspection without source identification, parameters, or verification offers none of these. Conclusion: the appearance of analysis is not enough to turn a perception into a forensic examination. The answer is not to dismiss the person who performed the inspection, but to allocate functions correctly and preserve what can be established.

The first response can document condition and custody without presenting itself as analysis. The specialist can acquire evidence later using a method. The reviewer can check what was and was not done. This prevents good intentions from becoming indefensible assertions and allows each person to contribute what their role can genuinely support.[11][12]

Limited conclusion

Competence is demonstrated by function and method, not job title. If a person cannot explain the source, procedure, and verification, their intervention must be presented for what it is: receipt, guidance, or inspection, not a technical expert opinion.

[9]Federal Law on the Protection of Personal Data Held by Private Parties, new law published on 20-03-2025 and amended on 14-11-2025. Articles 5–9, 18–20, and 31: principles, security, confidentiality, breaches, and time limits.Official online source

[10]Secretaría Anticorrupción y Buen Gobierno. Communiqué 011, 21-03-2025: transfer of personal data protection functions from the INAI to the Secretariat.Official online source

[11]ISO/IEC 27037:2012. Guidelines for the identification, collection, acquisition, and preservation of digital evidence. Edition confirmed by ISO as remaining in force.Official online source

[12]Jocsan Laguna. Sinaloa. Development and conclusions of a technical opinion in digital forensics. Material supplied by the author; errors are generalized without exposing personal data.

Chapter 4. Lifecycle and forensic readiness

4.1 Prepare before receiving a case

Forensic readiness means knowing which assets exist, what logs each produces, who can export them, how long they are retained, and how to request assistance. A prepared organization does not log everything forever: it identifies relevant sources, defines proportionate retention, and verifies that logs can be recovered with their context. Retention is not unlimited accumulation; it is deciding what information may be needed and for how long.

It also prepares forms, emergency credentials, provider contacts, time synchronization, and preservation procedures. The first response should not depend on searching the internet to learn how to seal a device or determine who administers an account. The right contact, emergency authorization, and a copy of the receipt record must exist before the incident, not be discovered while logs rotate or access is lost.

Minimum preparation	What must be checked	Error prevented
Inventory of assets and owners	Responsible person, source, format, and location kept up to date.	Requesting records from the wrong custodian.
Retention and format	Available period, fields, time zone, and export process.	Discovering too late that the data no longer exists or cannot be understood.
Directory and alternates	Technical, legal, custodial, and provider contacts, with alternates.	Depending on one person.
Time synchronization	Time source, offset, and periodic review.	Building a false timeline from incompatible clocks.
Exercises	Fictitious evidence, receipt, acquisition, transfer, and review.	Improvising the procedure during a crisis.

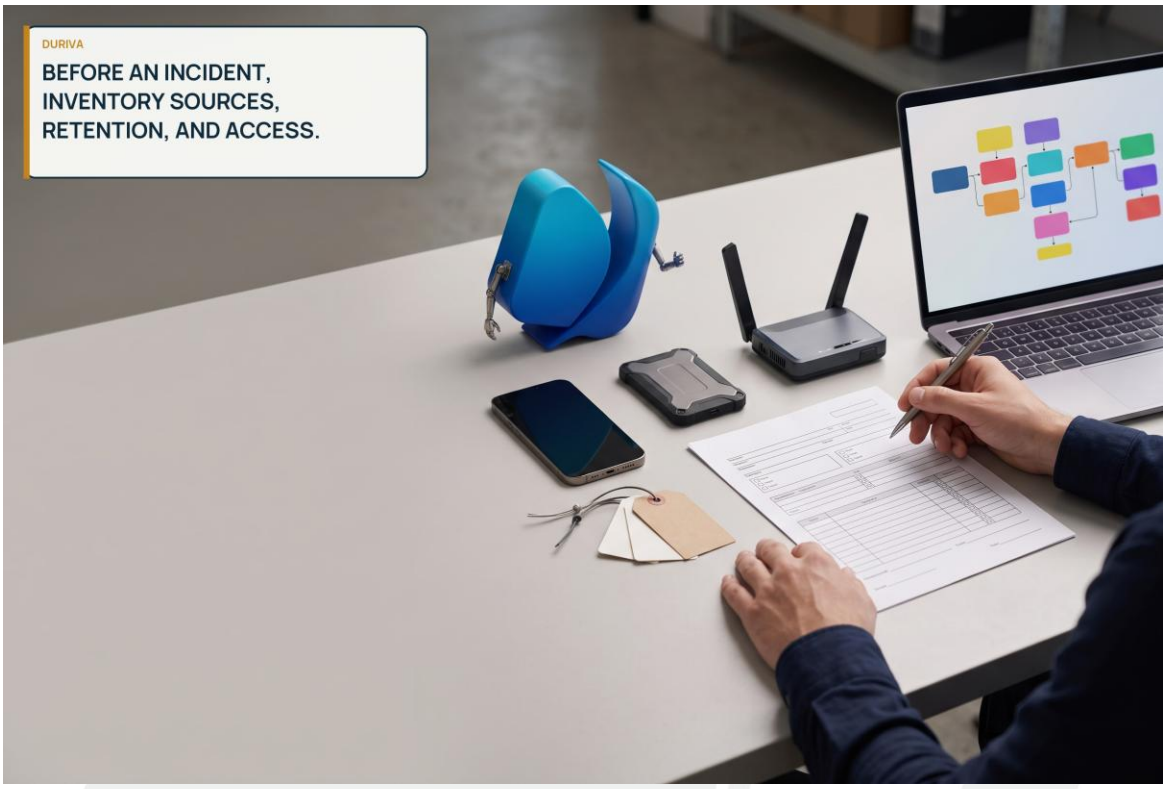


Figure 5. Pre-incident preparation: source inventory, retention, and access. Editorial reconstruction; it does not constitute actual evidence.

4.2 Points of no return

Some actions can prevent subsequent analysis: resetting a phone, reinstalling the operating system, encrypting without retaining keys, deleting an account, allowing logs to rotate, or replacing a link without preserving the previous version. Containment must assess these consequences and must not be performed reflexively. Powering down can preserve a state or destroy memory and sessions; suspending an account can stop activity or eliminate access to the only available export.

When an irreversible action is necessary to protect people or continuity, record who authorized it, why it was essential, what evidence was preserved beforehand, and what analytical capability was lost. Good intentions do not recover deleted data. Containment is judged not only by the harm avoided, but also by the ability to explain what was done, why, and at what evidentiary cost.

Urgent decision	Evidentiary risk	Recommended prior action
Power off or restart	Loss of memory and sessions.	Assess live acquisition and document the state.

Urgent decision	Evidentiary risk	Recommended prior action
Suspend an account	Loss of access to records or content.	Export logs and request preservation from the provider.
Lock the device	Possible remote encryption or wiping.	Confirm keys and the authorized access method.
Server replacement	Overwriting or loss of logs.	Preserve images, logs, and configuration.
Delete link	Loss of the version or download channel.	Preserve the URL, permissions, version, date, and received file.

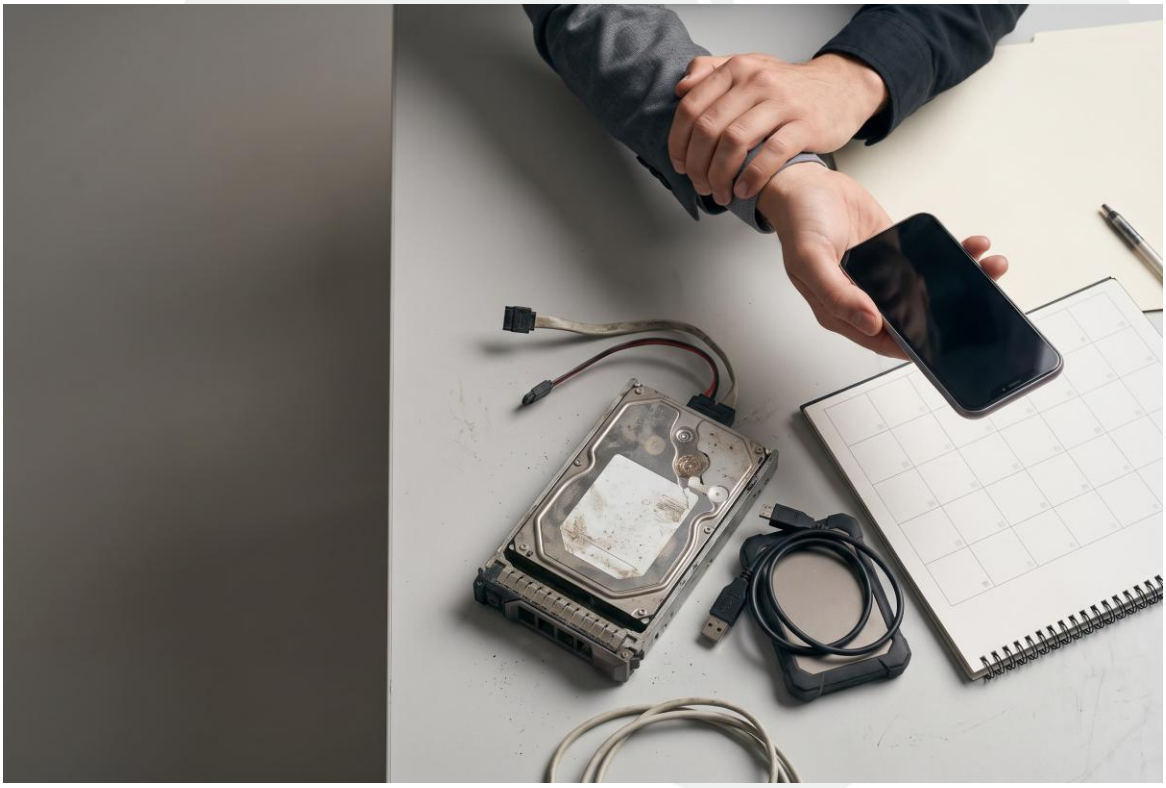


Figure 6. Points of no return: actions that can prevent subsequent analysis. Editorial reconstruction; it does not constitute actual evidence.

4.3 Documented lifecycle and deliverables

The lifecycle comprises authority, identification, initial preservation, acquisition, custody, examination, analysis, reporting, and preservation. Each phase produces a deliverable that

feeds the next. If a phase lacks documentation, the next receives an assumption rather than a verifiable basis. The chain cannot be sustained by a folder containing only a conclusion.
ISO/IEC 27037 provides guidance on identification, collection, acquisition, and preservation; NIST SP 800-86 organizes collection, examination, analysis, and reporting. These are methodological references, not laws or guarantees of validity. This guide translates them into understandable actions and forms that make the work demonstrable without turning methodology into automatic certification of the content.[13][14]

Phase	Minimum deliverable	Acceptance question
Authority	Scope, permissions, exclusions, and responsible persons.	Can we do this, with this goal and this scope?
Identification	Object, condition, custodian, identifiers, and photographs.	Do we know exactly what we have and how it got here?
Acquisition	Method, tool, parameters, output, and incidents.	Can another person repeat it and relate it to the object?
Custody	Transfers, access, seals, and verifications.	Can we reconstruct who accessed it and why?
Analysis	Hypotheses, sources, results and alternatives.	Are we also looking for what contradicts the first version?
Reporting and preservation	Conclusion, limitations, annexes, and subsequent access.	Can it be reviewed, opened, and understood in the future?

4.4 Longitudinal retention and analysis

An isolated event may seem anomalous only because the routine is unknown. When the question is whether behavior was unusual, preparatory, or repeated, compare one day's activity with earlier and later periods. A brief access may be the final stage of lengthy preparation; many small accesses may indicate distributed conduct. Longitudinal analysis prevents a snapshot of the incident from becoming a complete explanation of the past.
Log retention is neither infinite nor uniform. In Mexico, the Telecommunications and Broadcasting Law distinguishes a first twelve-month period in systems that allow consultation and delivery in real time to competent authorities, and another twelve months in electronic storage systems, with delivery within forty-eight hours of notification of the request. The point

[13]ISO/IEC 27037:2012. Guidelines for the identification, collection, acquisition, and preservation of digital evidence. Edition confirmed by ISO as remaining in force.Official online source
[14]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodological guidance, not legislation or a guarantee of admissibility.Official online source

is not to memorize the deadline: it is to request the source before retention and coverage change the possibility of analysis.[15]

Preservation decision
Do not wait for the minimum retention period to expire before requesting logs. Regulatory retention does not guarantee indefinite availability or coverage of every event. Preserve early, document the period, and compare patterns before declaring something unusual.

4.5 Preparedness as a social responsibility

Preparation prevents an emergency from becoming an arbitrary decision. An organization that knows who responds, what it retains, how to export, and what not to touch is less likely to destroy useful evidence or expose third-party data. Preparation also democratizes the work: a first responder can act methodically even without being an engineer, because procedures and contacts already exist.

Limited conclusion
Preparation does not mean logging everything; it means being able to recover relevant information with its context. If a critical source has no responsible person, known retention, documented format, or authorized access, that weakness must be resolved before an incident.

[15]Telecommunications and Broadcasting Law, published on 16-07-2025. Articles 182 and 183: requirements and data retention, real-time consultation, and delivery within 48 hours according to the segment. Official online source

Chapter 5. Decision trees by scenario

5.1 Device powered on or off

A powered-on device may contain volatile memory, sessions, keys, connections, and processes that disappear when it is shut down. It may also continue modifying data while being observed. A powered-off device may be more stable for imaging, but encryption and hibernation state change the options. The decision is based on the question and available capabilities, not inherited habit.

Do not power down as a universal rule or keep a device running out of anxiety. Record its state, visible activity, known encryption, connections, authority, and the need for memory. If live acquisition cannot be performed safely, document this and request support before changing the state. The first decision is not which tool to choose: it is understanding what each option loses.

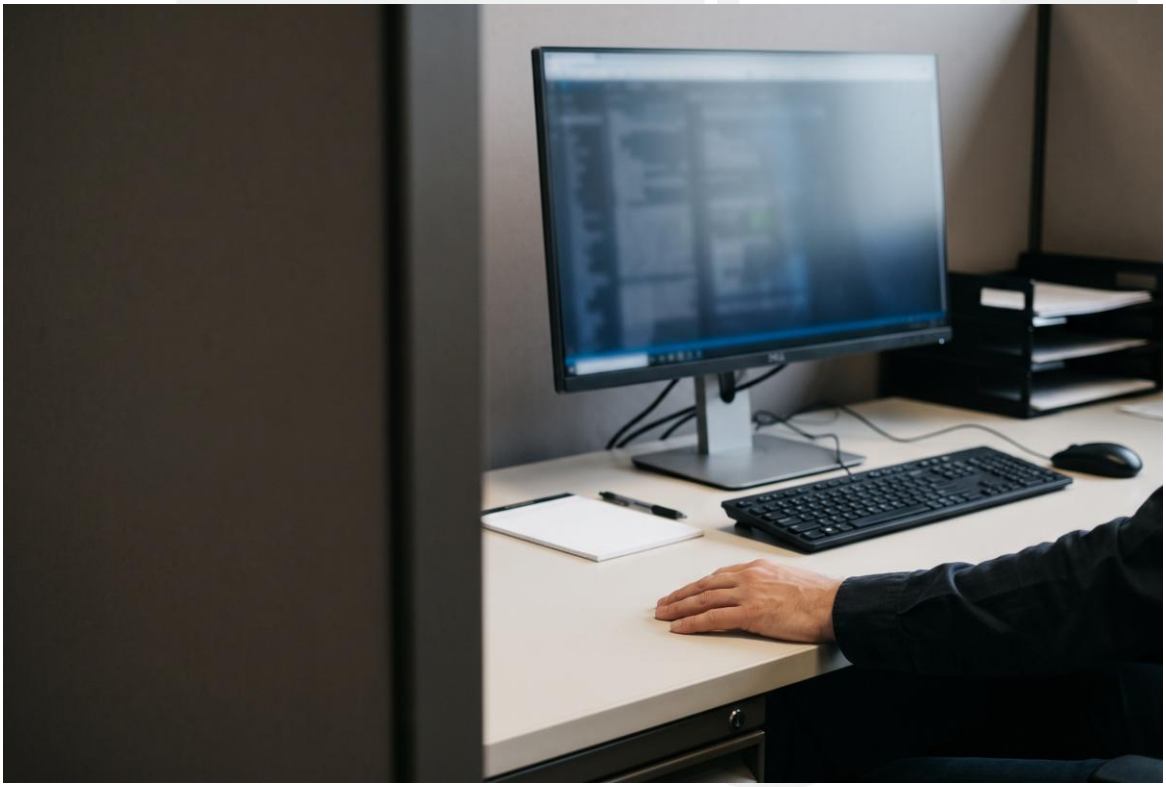


Figure 7. Powered-on device: record its state and activity before deciding. Editorial reconstruction; it does not constitute actual evidence.

5.2 Local, remote, or provider acquisition

Local acquisition lets you observe the device and its context, but is not always the best source. An administrative export may preserve events that the device does not store or that have already been deleted locally. Remote acquisition requires documentation of the operator's

identity, parameters, date, time zone, format, and transfer channel. The question is not where the visible file is, but where the source with the greatest coverage and least alteration resides. Ask the provider for the appropriate source, not “all the information.” Define the period, account, fields, format, column meanings, and generation process in the request. If an official portal is available, document who uses it, their role, and the filters applied. If the provider delivers a file without explaining how it was created, record that limitation. A native file from the provider may be better evidence than a printout of the same file made by someone else.

Condition	Preferred route	Required record
Memory or sessions required	Live acquisition if authorized and validated.	State, process, output, time, and unavoidable alteration.
Device powered off and stable	Image or logical acquisition, according to the objective.	Source, connection, method, coverage, and incidents.
Events on platforms or third-party systems	Administrative export or provider.	Role, filters, time zone, format, fields, and EML delivery.
Limited access or unvalidated tool	Stop and escalate without altering the state.	Reason, state, risk, and next responsible person.

5.3 Mobile devices and isolation

For a phone, assess its power state, lock status, encryption, network connections, synchronization, remote wiping, and battery. Isolation can prevent remote changes, but can also prevent legitimate acquisition or trigger lockouts. Removing the battery is not a universal instruction, and many devices do not allow it without damage or alteration. Connectivity may be necessary to export or preserve an account, so isolation is not always the first response.

The isolation method must be genuine and tested. An antistatic bag is not equivalent to a Faraday cage. Document the technology used, how it was verified, which connections remained active, and which risks were accepted. If conditions do not permit a safe decision, preserve the state and escalate. A “Faraday” label is not enough if the packaging does not perform that function or its effectiveness is not tested in the specific scenario.



Figure 8. Antistatic protection and radio-frequency isolation are not the same function. Editorial reconstruction; it does not constitute actual evidence.

5.4 Optical discs: identifiers and format

An optical disc requires precise identification. It is not enough to write “a CD” or “a DVD” when the label, cover document, and inspection do not match. Record the media type, make and model if available, capacity, condition, available readers, and any visible identifiers. The spindle ring may contain a code or manufacturing identifier; inspect it without touching the data surface and photograph it with context.

Not every disc has the same unique identifier, and not every visible code is a serial number with evidentiary value. The correct instruction is to inspect the spindle ring and record exactly what appears, without inventing an identifier when none exists. Also distinguish rewritable media from read-only media: a DVD-RW is not merely an aesthetic variation, because its rewritability changes the possibilities and must be documented as such.

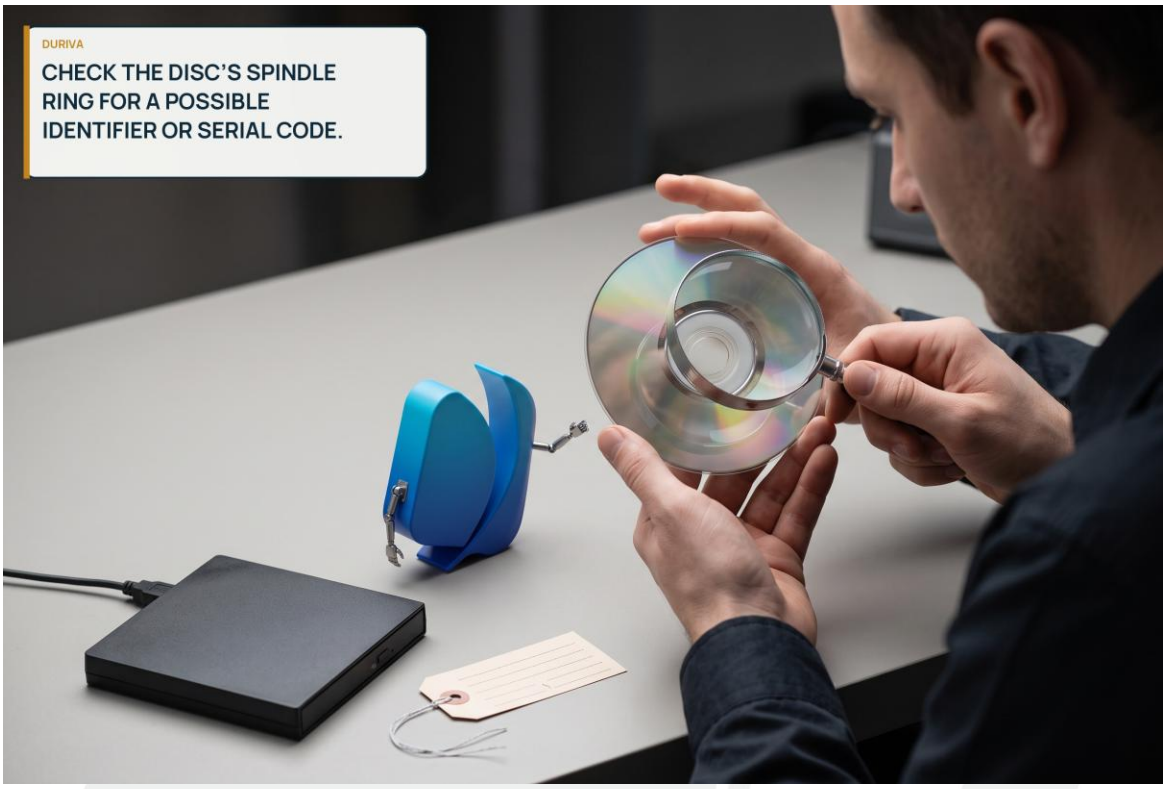


Figure 9. Inspecting the spindle ring: identifiers and codes that can identify the disc. Editorial reconstruction; it does not constitute actual evidence.

Identification before conclusions
If you cannot identify the medium, you cannot claim to have analyzed the correct object. Pseudo-custody begins with "there is a disc"; custody begins with identifiers, condition, format, photographs, and a link to the receipt record.

5.5 When to stop

Stopping is also a professional decision. Lack of authority, risk to people, inability to preserve evidence, lack of a validated tool, or danger of destroying evidence requires pausing and escalating. Continuing merely to "see whether something turns up" can cause more harm than information. A documented stop is not a failure: it preserves the possibility of analysis and avoids indefensible action.

The stop record includes the reason, the condition in which the object was left, prior actions, identified risks, and the next person responsible. If the question is resolved later, record who answered and the method used. The pause does not rewrite the past: it explains why the decision was made not to worsen the case.

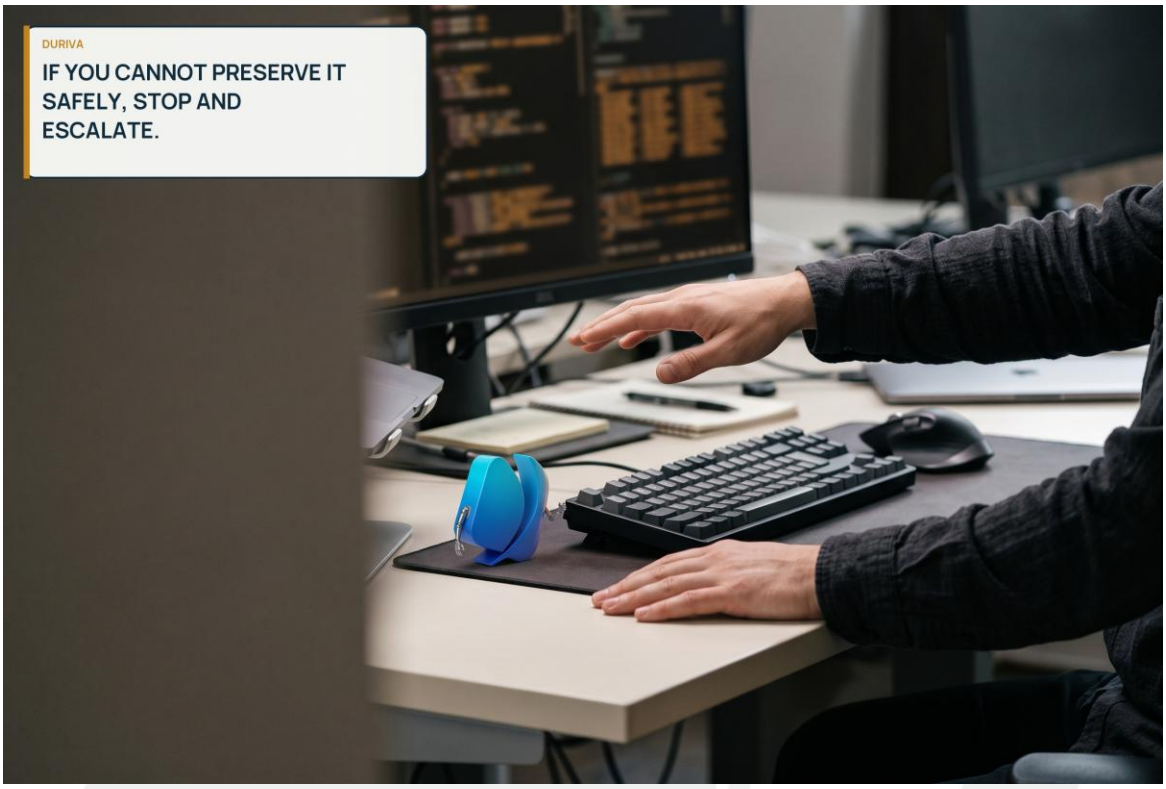


Figure 10. Stop and escalate: continuing can destroy more evidence than it produces. Editorial reconstruction; it does not constitute actual evidence.

Safety rule
Do not run unknown samples on personal devices or production networks. Use an isolated environment and controlled copies, with authorization and a defined objective. Curiosity does not justify exposing third parties.

5.6 The tree as reasoning, not decoration

A decision tree is useful when it requires answers about entry conditions, actions, and records, not when it presents a sequence of icons that no one follows. Each branch must end in a justified action, a rationale, and a record. If the condition changes, the route changes. An encrypted computer, a connected phone, or a provider with a better export must not lead to the same default operation.

Limited conclusion
The correct path depends on condition, objective, authority, and risk. If a decision is justified only by habit, the tree is poorly constructed or poorly applied. Recording the condition that led to a path is as important as recording the final action.

Chapter 6. Modern sources and call detail records

6.1 Cloud, SaaS, and exports

The user interface is only one layer. A platform may have version history, access logs, roles, tokens, IP addresses, administrative activity, shared links, notifications, and backups in other layers. The export must identify who generated it, their role, filters, time zone, format, period, and limitations. Downloading an interface is not equivalent to acquiring the account's complete history.

A PDF download may be useful for reading but insufficient for analyzing structure and metadata. Request native formats when available, together with documentation of the fields and generation process. If the platform offers an API, record the endpoint, version, parameters, pagination, limits, and response, without including secrets in the report. The output must make it possible to verify which query was made and what coverage it had.



Figure 11. Export by provider or API: filters, fields, time zone, format, and delivery. Editorial reconstruction; it does not constitute actual evidence.

6.2 Email and EML

EML preserves the message body, attachments, and headers, elements that a screenshot does not fully capture. It is especially important when the body contains a reference, an explanation of fields, or a hash value for the attachments. EML lets you review what was asserted on

delivery and relate each file to that statement. Retaining only the attachment breaks the link between the file and the integrity statement.
Preserve the original message and record how it was obtained: export from the email client, download from the server, or delivery by another person. Calculate hashes for the EML and attachments separately and document their relationship. The EML establishes the content of the received message, not that everything the sender asserts is true or that the sender's physical identity has been proven. Channel authenticity is assessed using headers, the server, and context, not a screenshot of the email screen.

Do not conflate objects
The EML hash is not the attachment hash, and the attachment hash is not the hash of the system that produced the data. Each value identifies a different object and must be recorded with its name, algorithm, date, and relationship.



Figure 12. EML preserves the body, headers, and attachments; a screenshot does not replace them. Editorial reconstruction; it does not constitute actual evidence.

6.3 Requesting and receiving call detail records

A call detail record file is an export of telecommunications records. Interpreting it requires more than a table of numbers: you need the period, time zone, event type, direction, duration, identifiers, cells, technology, empty fields, and extraction method. The request must ask for

available native formats, column documentation, and a record of the system that produced the file.
In the body of the delivery email, the provider must include the hash value for each delivered file and the algorithm used. This value lets you verify that the received attachment matches the file to which the provider refers. The EML containing that body, its headers, and its attachments must also be presented and preserved. Copying the hash into a separate note or retaining only the table is not sufficient.
On receipt, verify that the value in the body matches the attachment. If it matches, document it; if not, record the discrepancy and request clarification without editing the file. If the provider does not supply a hash, record its absence and calculate one upon receipt, making clear that it establishes integrity only from that moment. No hash alone proves the truthfulness of the calls or the identity of the person who used the phone.

Request element	What to request from the provider	What is checked on receipt
Period and time zone	Start, end, time zone, and daylight saving time.	Events within the period and consistent conversions.
Format and fields	Available CSV/XLSX/PDF formats, data dictionary, and extraction process.	Native file, columns, blank fields, and units.
Integrity	Hash of each file and algorithm in the email body.	Local calculation and documented match or discrepancy.
Delivery	EML with body, headers, and attachments.	Complete EML and related files, without separating the objects.
Context	Network type, events, roaming, cells and available identifiers.	What can and cannot be inferred from each field.

6.4 Example provider request body

The following example is fictitious and can be adapted without including sensitive data in an ordinary channel. Send the authorization and case file through the appropriate secure channel. The purpose is for the response to arrive with sufficient context for analysis and with objects whose integrity can be verified.

Example request
Subject: EXP-DEMO-2026-001 · Request for records and integrity attestation

Dear Custody Team,

Through the secure channel already authorized, I request the records for the period from 1 to 3 November 2026, with express indication of the applicable time zone and daylight saving time. Please include, where available, start date and time, duration, event type, direction, line and device identifiers, cell, technology, and an explanation of blank fields.

Please provide the files in their available native format (CSV and/or XLSX), a PDF reference copy, the field dictionary, and a description of the extraction process and date. For each file, please indicate the algorithm and corresponding hash value in the body of your response.

The delivery must preserve this email in EML format, including its body, headers, and attachments. Any limitation of format, retention, or coverage must be expressly stated.

Sincerely,
Authorized technical officer · EXP-DEMO-2026-001

6.5 Virtualization, IoT, and synthetic content

In virtualization, distinguish among the host, guest, snapshots, shared storage, and administration logs. In IoT, distinguish among the device, application, hub, cloud, firmware, and synchronization. The presence of data on a screen does not indicate where it was generated or how many copies exist. Acquisition must identify the layer, not merely the product: a camera is not all the evidence, and a router is not the entire network.



Figure 13. Virtualization: host, guests, snapshots, and shared storage. Editorial reconstruction; it does not constitute actual evidence.

For AI-generated or manipulated content, distinguish among generation, editing, conversion, and publication. Preserve the original, history, tool, and version when available, together with authorizations and human review. A detector provides indications, not a verdict. Legal analysis examines consent, identity, conduct, use, and the law in force; it does not turn “AI” into a universal criminal category.

Articles 199 Octies and 199 Nonies of the Mexican Federal Criminal Code regulate certain conduct involving nonconsensual intimate sexual content, including cases where the material does not depict the identified person. Article 50 of the European AI Regulation addresses deepfake transparency and adapts certain obligations for creative works and editorial review. These are different regimes and must not be merged into a supposed worldwide ban on AI.[16][17]

6.6 Verifying that law is in force: the example of a repealed reform

San Luis Potosí shows why it is essential to verify the law in force: the reform approved in November 2025 added specific AI offenses, but Articles 187 Ter, 272 Bis, and 272 Ter were

[16]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

[17]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

repealed on 30 July 2026. This example is merely a local precedent, not a universal rule or general authorization. The conduct must be analyzed under the law in force and any other applicable offenses.[18]

Update rule
A citation includes the instrument, article, function, version, and official source. Do not cite a law merely because its name is similar or present a bill as an enacted decree. Comparative equivalence is limited to function and scope; it does not imply identical procedural effects.

6.7 The source does not reside in only one place



Figure 14. Device, application, account, and provider: layers of modern evidence. Editorial reconstruction; it does not constitute actual evidence.

[18]San Luis Potosí. Parliamentary Gazette, 30-07-2026: repeal of Article 187 Ter and the chapter containing Articles 272 Bis and 272 Ter. Historical precedent, not a rule in force.Official online source

Limited conclusion
The user view does not exhaust the source. The appropriate export may reside with a provider, in a cloud, in version history, or in a delivery email. Identify the layer and preserve its context before analyzing the content.

Chapter 7. Initial receipt and preservation

7.1 A clear receipt record

The receipt record answers what arrived, how it arrived, who delivered it, who received it, when, where, and in what condition. It includes available identifiers, accessories, seals, photographs, and observations. It is not enough to write “a computer” or “a USB drive”: record the make, model, serial number when available, capacity, physical condition, and any prior labels. For a disc, record the media type, capacity, format, and spindle-ring code when visible.

The first responder does not need expertise in forensic acquisition to do this correctly. They must avoid powering on, exploring, or connecting devices without authorization; photograph the condition; record what is visible; and request support. If someone has already opened files, record that too; do not conceal it to make the receipt record look perfect. The goal is not to fabricate a flawless receipt, but to document the conditions that existed at the outset.

Field	Required content	Fictitious example
Object and identifier	Type, make, model, serial number, capacity, and assigned code.	2.5-inch SSD, 512 GB, serial number demo-003.
Delivery and receipt	Name, role, date, time, time zone, and location.	Custodian A delivers to analyst B, 09 Nov, 14:32 −06.
Condition	Power state, lock status, network status, damage, and accessories.	Powered off, no visible damage, SATA cable and power supply.
Seal and packaging	Type, identifier, condition, and photographs.	Seal 01 intact, rigid box, and antistatic bag.
Prior actions	Opening events, connections, copies, changes, or unknowns.	It is unknown whether the device was powered on before delivery.
Initial decision	Preserve, escalate, acquire, or request clarification, and identify the responsible person.	Preserve the state and request a specialist.



Figure 15. Photograph the object's initial condition and accessories before analysis. Editorial reconstruction; it does not constitute actual evidence.

7.2 Packaging and sealing

Packaging protects against physical damage, electrostatic discharge, moisture, unauthorized access, and substitution. Select it according to the object and its condition. The seal includes an identifier, date, responsible person, and features that make opening detectable. If it is broken for examination, document this and replace it according to procedure without erasing the history. Opening and replacement are custody events, not marginal notes.

Antistatic protection and radio-frequency isolation are not equivalent. The former protects components from discharge; the latter seeks to prevent wireless communications and must be validated. Correct packaging does not remedy a poor earlier decision, but it prevents further alteration and makes it possible to reconstruct who accessed the object. Choose material for the function the evidence requires, not for the container's professional appearance.



Figure 16. Receipt and packaging: physical protection, seal, label, and relationships between objects. Editorial reconstruction; it does not constitute actual evidence.

7.3 Labels and relationships between objects

Each object receives a stable identifier that does not include the client's name. Derivatives are linked to the original through a provenance field. Do not reuse the identifier for a different export: create a related object with its own date, method, and hash. This avoids comparing files that share only a name. The physical label and receipt record must match the digital inventory and final report.

One possible convention is ED-AAAAMMDD-CASO-FUENTE-SECUENCIA-VERSION. If the organization already has another convention, retain it if it is unique and consistent. The identifier does not replace the original object: a different export from the same source receives a related identifier and a note describing the relationship. The identifier must make the object locatable without revealing the client, holder, or sensitive information.

Fictitious identifier example
ED-20261109-DEMO-MBL-003-A00

ED = digital evidence
20261109 = receipt
DEMO = fictitious case
MBL = mobile source

003 = third object
A00 = initial acquisition



Figure 17. Label the object, condition, date, custodian, and identifier. Editorial reconstruction; it does not constitute actual evidence.

7.4 Accessories and connections as part of receipt

A cable, adapter, SIM card, SD card, or power supply can explain how information was accessed or which connections were possible. Record them as related objects, not invisible accessories. Photographing only the phone can omit evidence needed to acquire or interpret the data. The inventory must include every item received and its relationship to the primary device.



Figure 18. Accessories and connections: part of receipt and of acquisition capability. Editorial reconstruction; it does not constitute actual evidence.

7.5 Receipt of files and messages

Digital receipt records the origin, channel, date, apparent sender, recipient, filenames, sizes, and formats. Store files without modifying them and calculate hashes on arrival. If the provider supplies values in the body, verify them and preserve the EML. If material is received through a link, document who opened it, the permissions, download date, and version. The download is a receipt event, not an invisible action.

Never rename the original file to “organize” it before preservation. Document the relationship between the original and working copy in the manifest. If someone else previously renamed or converted the file, record that history and preserve every available version. Order is created through inventory, not by altering the received object.

Limited conclusion

Receipt is the first test of method. If the object, condition, identifiers, and prior actions are not clear, every subsequent assertion begins with avoidable uncertainty.

Chapter 8. Acquisition and technical documentation

8.1 Physical, logical, volatile, and documentary acquisition

Physical acquisition copies the entire medium and may include unallocated space; logical acquisition obtains selected files or sources. Volatile acquisition captures memory and temporary states when justified. Documentary acquisition records a visual representation when the others are unavailable, without presenting it as though it preserves every property of the original. Each method meets a different need and produces different limitations.

The choice depends on the question, not the tool's prestige. An image may be appropriate for reconstructing deleted activity; an official export may suffice to obtain platform records. Document the method with its prerequisites, authority, tool, version, parameters, output, and errors. The phrase "forensic acquisition" does not by itself describe what was done or what coverage it had.

Method	When it may be appropriate	Limitation to declare
Physical image	The entire medium is needed, including unallocated space.	It doesn't guarantee analysis of every file or platform.
Logical acquisition	Selected files or sources are required.	Selection and filtering determine coverage.
Volatile memory	Sessions, keys, processes, or temporary state are relevant.	Justification, authority, and potential loss when changing state.
Official export	The best source resides with the provider or platform.	Provider parameters, format and coverage.
Documentary acquisition	No other representation is available and the visual representation must be shown.	It does not retain all the properties of the original.

8.2 Actual connection: source, write blocker, and workstation

Write blockers and other protections are used when appropriate, but must not be invoked as an absolute guarantee. Document the actual workflow: device, connection, state, error, and verification. The source connects to the blocker and the workstation to the other end. The configuration must match what was actually done, not an idealized image from a guide.

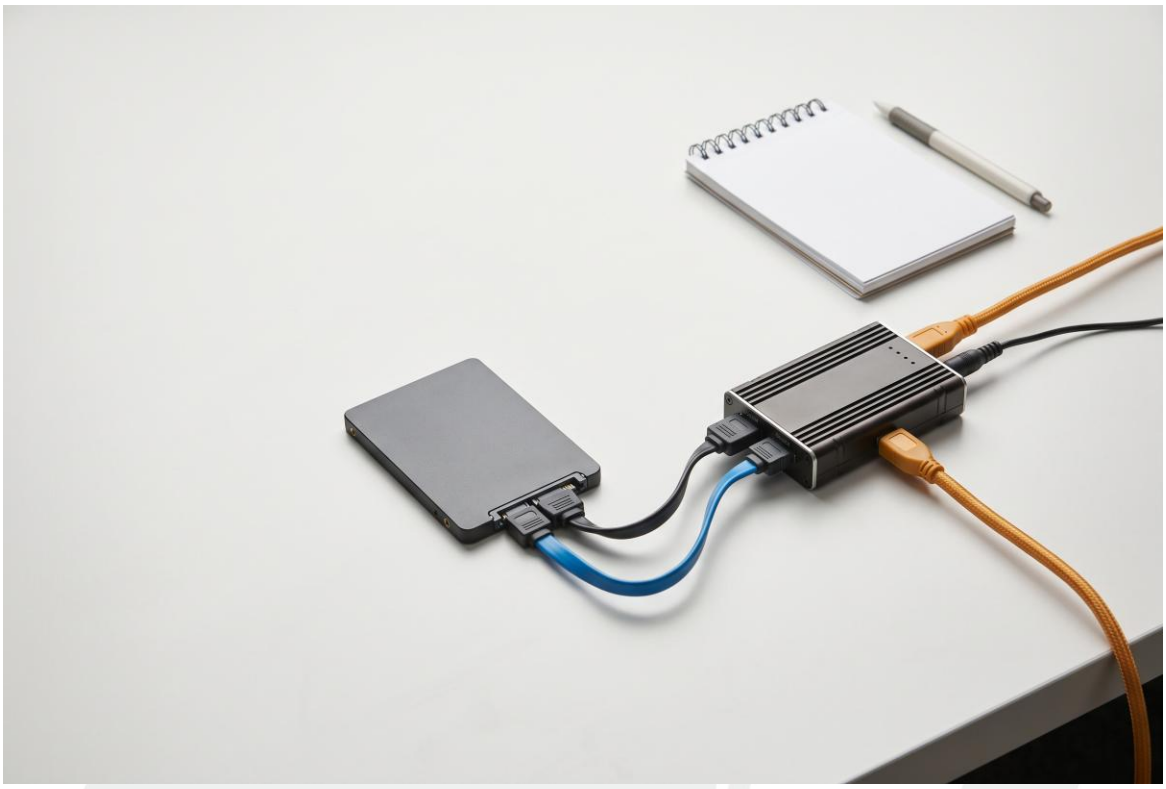


Figure 19. Source, write blocker, and workstation: the connection is also evidence. Editorial reconstruction; it does not constitute actual evidence.

Record the blocker's model and serial number when available, ports used, cables, power supply, indicator status, and any incidents. If a tool produces an error, preserve the message and assess its effect rather than concealing it. Protection is demonstrated through configuration and verification, not by asserting that a device with that name was present.

8.3 Media and adapters: NVMe, SATA and optical discs

The media form factor changes acquisition. An M.2 NVMe does not connect like a 2.5-inch SATA drive, and a 3.5-inch SATA drive requires different power. The adapter must be compatible and documented. A photograph of the adapter helps explain the path, but the record must include the model, interface, power supply, and verification that the workstation recognizes the medium correctly.



Figure 20. Media and adapters: form factor, connector, and acquisition procedure. Editorial reconstruction; it does not constitute actual evidence.

For an optical disc, document the reader, format, capacity, reading method, unreadable sectors, and relationship to the medium received. Do not claim that a DVD was acquired if the images show a folder on the computer rather than the disc. If reading fails, preserve the error and assess a second drive or method without replacing the problem with a generic assertion.

8.4 Logical acquisition and manifest

Logical acquisition obtains selected files or sources. Before performing it, define the folders, file types, dates, filters, and exclusions. The output is accompanied by a manifest linking the identifier, name, path, object type, origin, method, size, format, hash, and observations. Without a manifest, a folder full of files may have volume but is not necessarily organized evidence.

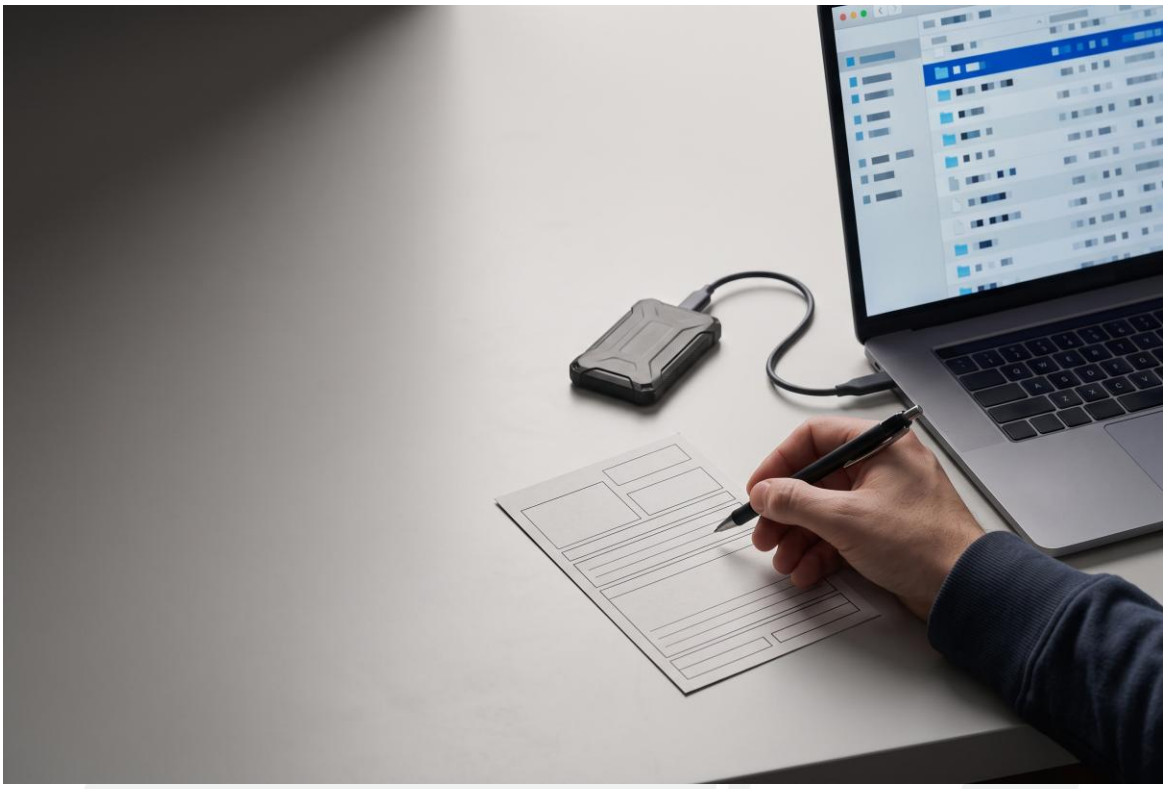


Figure 21. File manifest: origin, derivatives, format, and integrity by object. Editorial reconstruction; it does not constitute actual evidence.

Manifest rule
The manifest must not disclose secrets or unnecessary sensitive data. The path may be abbreviated in the public version if it reveals protected information, but enough of the relationship must be preserved to locate the object in the controlled case file.

8.5 Live memory and tool validation

Live acquisition is justified when memory, sessions, keys, or processes are relevant and the authority and capability to perform it exist. Document the state, tool, version, parameters, unavoidable alteration, and output. If those conditions are unavailable, escalate. Do not perform invasive acquisition merely because an export would be harder to request.

A tool must be understood and validated for its intended use. Record its name, version, environment, configuration, and test result. An update can change its format or behavior; do not reuse an old command without verifying it. Validation uses fictitious data and demonstrates that the output can be opened and linked to the expected object.



Figure 22. Validate the tool before use: fictitious data, readable output, and the expected object. Editorial reconstruction; it does not constitute actual evidence.

8.6 Reproducible exports and queries

A query must be repeatable with the same parameters. Record the system, account, role, filters, time zone, format, fields, date, operator, and result. If the platform changes its interface, preserve the version or evidence of the path used. A screenshot can show the configuration but does not replace the native output. Repeatability depends on documented conditions, not memory.

When a query returns zero records, do not conclude that the information does not exist without reviewing filters, coverage, time zone, retention, and errors. The report describes what was queried and what response was obtained. This documented negative result is more defensible than an absolute assertion. An absence can be significant, but only within the verified coverage.

8.7 Errors and incidents

Incidents must not be removed from the case file: unreadable sectors, damaged files, missing passwords, network interruptions, hash mismatches, and provider changes are recorded. Assess whether they affect coverage, authenticity, or analysis, and request a second delivery when possible. Repetition does not eliminate the first attempt; it creates another related object with another history.

If an acquisition must be repeated, retain both objects under different identifiers and explain why. Do not delete the first file to avoid an uncomfortable explanation. Traceability includes decisions that went wrong and how they were corrected. A case file that appears perfect is less defensible than one that declares the incident and how it was addressed.

Limited conclusion

Acquisition does not end with a file. It ends with an output that can be opened, linked to the object, verified, and repeated under documented conditions. If something fails, it remains within the record, not outside the narrative.

Chapter 9. Custody, transfer, and preservation

9.1 The chain that answers questions

The chain of custody makes it possible to know which object existed, where it was, who could access it, why it was moved, and how it was verified. It is not a list of signatures without identifiers. Each transfer includes the object, sender, recipient, date, time zone, purpose, seal condition, and integrity verification when applicable. It also records legitimate access without physical transfer: container opening, working copies, temporary loans, relocation, or remote download.

Documenting only the final delivery leaves gaps that prevent the history from being reconstructed. A seal may be intact on receipt even when it is unknown who opened it earlier. The chain records events: receipt, opening, copying, access, transfer, verification, and return. Every event has a responsible person and purpose, not merely a name and date.



Figure 23. Custody transfer: object, responsible persons, seal, and verification. Editorial reconstruction; it does not constitute actual evidence.

9.2 Electronic transfers and keys

A link-based transfer requires the recipient, permissions, channel, date, version, and download verification. Encryption protects content, but keys must be managed through a separate channel and secrets must not be included in the record. The recipient confirms the object and

hash before proceeding. Sharing a link without knowing who can open it is not controlled custody.

If the provider includes the hash in the email body, preserve the complete EML and attachments. The body links the statement to the delivery; the received file is verified locally. If the provider changes the file, a new delivery and new hash must be recorded without silently replacing the previous file. Any change of key or recipient must also be recorded.



Figure 24. Encryption and keys: protect content without losing control of receipt. Editorial reconstruction; it does not constitute actual evidence.

Key management rule
Encryption is not enough: record who holds the key, through which separate channel it was delivered, and how receipt was verified. Do not write keys in the record or email body.

9.3 Storage and subsequent access

Maintain the preserved original and working copy according to policy. Encrypt and verify backups, and test their recovery. A backup that no one can open is not useful preservation. Migration to another format must be documented and must not delete the original. Preservation includes future readability, format documentation, and available keys.

Regulatory retention, corporate policy, and evidentiary preservation do not serve the same purpose or have the same time limits. Do not use a universal period. Define retention by law, case, and need, with restricted access and a record of consultations. Preservation includes future readability, format documentation, and available keys. Do not confuse the first working copy with the original packaging; every opening, seal replacement, or transfer must be recorded.



Figure 25. Backup and migration: preserve the original, working copy, and subsequent access. Editorial reconstruction; it does not constitute actual evidence.

9.4 Opening and replacing seals

Opening a container for examination does not erase the seal or its history. Record who opened it, why, under what authority, the seal's condition, and what object it contained. When finished, reseal it with a new seal identifier and preserve the previous one when required by procedure. The chain is strengthened by verifiable actions, not by a generic assertion that the package was closed.



Figure 26. Opening and replacing a seal: a transfer that must also be documented. Editorial reconstruction; it does not constitute actual evidence.

9.5 Access, shared custody, and conflicts

Subsequent access requires a record of consultations, purpose, and authorization. If a person reviews, exports, or shares, the action must be associated with their role. Shared custody does not eliminate responsibility: define who decides, who executes, and who verifies. Conflicts of interest are declared and managed separately when independence requires it.



Figure 27. Access log: who may open, consult, and transfer with authorization. Editorial reconstruction; it does not constitute actual evidence.

Limited conclusion
Custody does not end when the object is stored. It ends when every access, transfer, and verification can be reconstructed, including how the ability to open it in the future is preserved.

Chapter 10. Examination, timelines, and alternative hypotheses

10.1 Examining is not finding a culprit

Examination begins once the source has been identified, acquired, and linked to the assignment. Its purpose is not to find the file that makes the first impression look correct, but to turn a mass of data into verifiable observations. The analyst opens the working copy, documents the tools, and asks small questions: which file exists, what date it shows, what a field means, what changed, which system produced the record, and which other source could contradict it. Every answer must lead back to a specific object in the manifest.

The difference between examination and analysis is similar to the difference between reading the parts of a watch and explaining why it stopped. In examination, gears, wear, and position are observed; in analysis, explanations are compared: lack of power, mechanical damage, manipulation, or an incorrect reading. Jumping directly to the preferred explanation makes every part seem to confirm it. Discipline means describing before interpreting and preserving whatever does not fit.[19]

Working rule
Every analytical assertion must be traceable backward: from conclusion to finding, from there to the query, to the analyzed object, to acquisition, and finally to the source. If any link cannot be shown, the conclusion must be reformulated or another source is needed.

10.2 Metadata: listen to the file without believing everything

Metadata is information about an object, not a spontaneous confession of an event. A creation date in a file system may correspond to the copy on that medium; a photograph's internal date may depend on the camera clock; an author tag may be an account name configured by anyone. Every field has a producer, a mechanism, and a possibility of alteration. Reading it properly requires knowing who wrote it, when, under what conditions, and whether analysis modified it.

A filename can also provide guidance without proving anything by itself. A sequence such as IMG_0041, IMG_0042, and IMG_0043 suggests an order of generation within a camera or application, but does not preclude copying, renaming, numbering resets, or imported files. Prudent analysis asks whether internal identifiers, thumbnails, dates, application logs, and backups preserve that sequence. The name is an investigative lead, not a chronological seal.

Suppose an image shows 18:42 and an accusation claims it was captured at 20:42. The first temptation is to declare the evidence falsified. The second, equally dangerous, is to accept

[19]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodological guidance, not legislation or a guarantee of admissibility.Official online source

18:42 as the absolute time. The correct method preserves the native file, extracts fields without altering it, checks the time zone, reviews the device clock, compares the preceding and following sequence, and seeks another independent source: a sending message, cloud copy, purchase receipt, video from another camera, or activity log. Only then can you explain whether there is a time-zone difference, a misconfigured clock, a conversion, or a larger inconsistency.



Figure 28. Metadata requires a producer, meaning, context, and corroboration; it is not infallible testimony. Editorial reconstruction; it does not constitute actual evidence.

Observed data	Technical question	Conclusion that cannot yet be reached
System date	What event does it represent in this file system?	It is the original date of the event.
EXIF date	How were the clock and time zone configured?	The scene necessarily happened at that hour.
Author or account	Who could set up or use that account?	The individual has been identified.
Consecutive filename	Is the sequence preserved in other sources?	There were no copies, no imports, no renaming.

Observed data	Technical question	Conclusion that cannot yet be reached
Coordinates	What are the precision and origin of the position?	The person was at an exact location.

10.3 Timelines: reconcile clocks before constructing the account

A useful timeline is not a column of ordered dates. It is a reconciliation of clocks that may use different time zones, synchronize with different servers, or contain human error. First record the source's literal value; then its declared or inferred time zone, the conversion applied, and the available precision. Never replace the original value with the conversion. If a provider uses UTC and a phone records local time, the report must show both and explain how they were compared.

Precision matters as much as the date. A record containing only a day cannot be placed at 14:32 for visual convenience. A file with seconds does not necessarily have second-level accuracy. If the clock has a known offset, document how it was measured and which sources it affects. If this cannot be resolved, use a time window or declare the uncertainty. This honesty prevents a visually perfect sequence from turning two incompatible events into a causal relationship.

The sequence must also preserve negative events and periods without data. A gap in the logs may result from inactivity, rotation, loss of connectivity, configuration, or deletion; the timeline must not select an explanation without evidence. Mark each event as observed, calculated, declared by a person, or inferred. Mixing these four categories as though they were identical is a subtle way of manufacturing certainty.



Figure 29. The timeline preserves each source's original time, time zone, conversion, and uncertainty. Editorial reconstruction; it does not constitute actual evidence.

Example of timeline normalization
Object: ED-20261109-DEMO-SRV-001-A00
Literal value: 2026-11-03 20:14:07
Time zone declared by the provider: UTC
Working conversion: 2026-11-03 14:14:07 -06:00
Available precision: seconds; server synchronization not established
Relationship: event preceding the email received at 14:20:11 -06:00
Limitation: temporal proximity does not establish who performed the action or that one event caused the other.

10.4 Antennas, coverage, and azimuth: geography without shortcuts

Call detail records may indicate that a line communicated through a cell. That does not turn the antenna into a person or prove that the user was beneath it. The cell describes a radio connection within conditions of network, coverage, congestion, technology, and configuration. The analysis requires the cell location, orientation or azimuth when available, technology type, date, power or available measurements, and a genuine understanding of the area. A point on a map represents equipment, not a photograph of the user.

Azimuth indicates the sector toward which an antenna is directed; it is not a laser line ending at a house. Coverage depends on propagation, obstacles, frequency, terrain, interference, power, and network decisions. A call can be served by a cell that is not the nearest. Nor does the absence of another cell in an export prove that alternative coverage did not exist: it may mean that it was not used, the data was not supplied, or the system did not retain it.

In an anonymized case file reviewed by the author, a location was treated as though it described a person's journey, although the source only permitted discussion of coverage. Other elements complicated the account: a video provided a sequence inconsistent with the asserted interpretation, and witnesses described events inconsistently. The value of the analysis lay not in replacing one absolute account with another, but in showing that the conclusion did not necessarily follow from the source. The antenna remained an antenna; the user's identity required other evidence.[20]



Figure 30. An antenna provides potential coverage, not an exact location or the user's identity. Editorial reconstruction; it does not constitute actual evidence.

[20]Jocsan Laguna. Sinaloa. Development and conclusions of a technical opinion in digital forensics. Material supplied by the author; errors are generalized without exposing personal data.

Defensible form of conclusion
“The record provided associates the event with the identified cell. In the absence of additional measurements and parameters, that data does not permit a precise location to be determined or use of the terminal to be attributed to an individual.”

10.5 Corroboration that actually discriminates

Two files saying the same thing are not always two independent sources. A screenshot and a printout of that screenshot merely repeat the same representation. By contrast, a server log, a message received by a third party, and a sequence of sensor data can have different origins and different errors. Corroboration gains strength when sources do not share the same dependency and each could have contradicted the account.

Convergence is not measured by page count. It is assessed by independence, proximity to the event, potential for error, and ability to distinguish hypotheses. A hundred screenshots of unknown origin may carry less weight than a complete EML with headers, a verifiable attachment, and server logs. Ockham’s razor does not require choosing the most convenient explanation: it invites us not to multiply causes when a simple sequence explains the data without ignoring its contradictions.

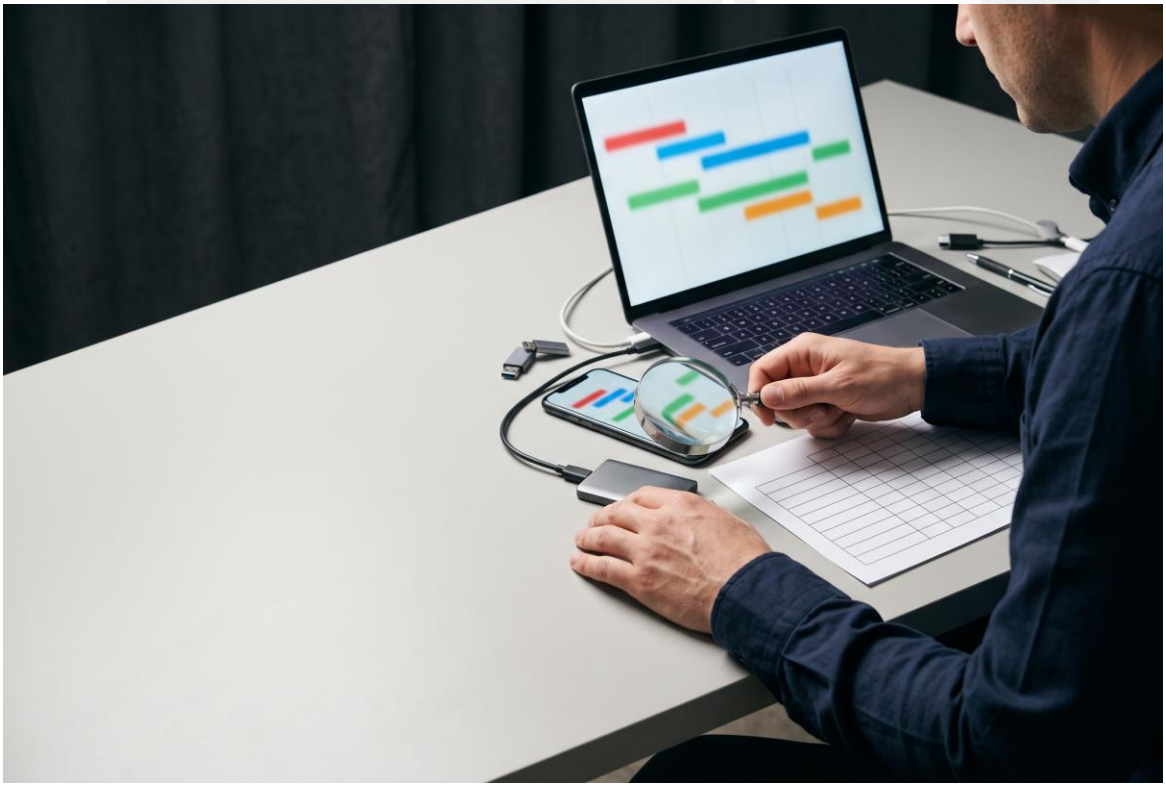


Figure 31. Corroboration compares sources with different origins and errors; it does not repeat the same screenshot. Editorial reconstruction; it does not constitute actual evidence.

10.6 Hypothesis matrix: allow the evidence to contradict

Before analyzing, write at least two plausible explanations and one condition that distinguishes them. If a company claims that an employee created a file on their departure date, the hypotheses might be: creation on that date by the assigned account; later copying of an earlier file; modification of metadata; or use of the account by someone else. Not all must be equally probable, but each must face a concrete test.

The result can be positive, negative, or inconclusive. A documented negative is not a failure: it can eliminate an explanation and prevent an unjust accusation. An inconclusive result must not be disguised as confirmation. When the source cannot distinguish between explanations, the correct response is to request another source, change the scope, or declare the limitation. The analyst earns no points for maintaining an incorrect hypothesis; trust is earned by abandoning it when the data requires.

Hypothesis	Test	Fictitious result	Limited interpretation
The document was created on 3 November.	Internal metadata, version history, and cloud logs.	The history shows a previous version dated 28 October.	The visible date does not establish initial creation.
The account was used by its owner.	Sessions, second factor, devices, and concurrent activity.	There is a session from an unregistered device.	Account attribution does not yet identify the person.
The image belongs to the same event.	Sequence, thumbnails, backups, and other nearby files.	The backup contains a consistent sequence.	Compatible with the event; context is required to interpret its meaning.
There were no other accesses.	Complete query, retention, filters, and errors.	The export covers only seven days.	None were observed within the period queried; total nonexistence cannot be asserted.



Figure 32. Seeking what contradicts the initial hypothesis prevents analysis from becoming mere confirmation. Editorial reconstruction; it does not constitute actual evidence.

10.7 Repeat, reproduce, and know when to stop

A repeatable query can be run again under documented conditions and produce a compatible result for the same object. Reproducibility also requires that another qualified person can understand and evaluate the procedure with sufficient independence. Retaining only a screenshot of the result satisfies neither requirement if the file, tool version, filters, or query are unknown. The goal is for review to be able to disagree using data, not to have to rely on the analyst's memory.[21]

Analysis stops when the assignment's questions have been answered within scope, when an additional source no longer discriminates, or when continuing would entail disproportionate intrusion. It also stops to request authority for a new source. Thoroughness does not mean opening every possible folder; it means not leaving unexamined a reasonable hypothesis that the available evidence can resolve.

[21]ISO/IEC 27037:2012. Guidelines for the identification, collection, acquisition, and preservation of digital evidence. Edition confirmed by ISO as remaining in force.Official online source

Chapter deliverable
An analysis matrix containing the assertion, source, query, literal finding, supported hypothesis, weakened hypothesis, limitation, and additional action. The conclusion arises from that matrix; it is not written first so that the matrix can be filled in afterward.

Chapter 11. Reporting, reasoning, and challenge

11.1 The report is the way back to the source

An expert report should not impress by its thickness or its use of English terminology. It must enable someone with different judgment to locate the object, understand what was done, and assess whether the conclusion follows from the findings. The structure is a path: assignment, scope, authority, sources, method, results, analysis, conclusion, limitations, and annexes. If an assertion cannot be traced back along that path, the report becomes an exercise in authority-based literature.

The primary reader is not always an engineer. A judge, lawyer, executive, or accused person needs to understand the reasoning without first learning a secret language. Clear writing does not diminish the science: it exposes it. Every specialized term is therefore explained on first use, and every screenshot is accompanied by the original object or an explanation of why it is unavailable. The simplicity of the explanation should match the rigor of the work, not its absence.



Figure 33. The report allows the source, method, findings, and conclusion to be verified; it does not depend on the signatory's prestige. Editorial reconstruction; it does not constitute actual evidence.

11.2 Fact, result, inference, and opinion

The text must distinguish four planes. A documentary fact is what is recorded on receipt: the file arrived with a particular name and size. A technical result is what verification produces: the calculated hash matches another value. An inference is a reasoned interpretation of several results: the attachment received matches the one declared by the provider. An opinion is the professional conclusion within the assignment: the delivery has a verifiable integrity mechanism from that moment. Mixing these planes allows an opinion to look like observed data.

Legal and technical questions must also be separated. The expert can describe how a record was obtained, which fields it contains, and what inconsistencies it presents. The expert need not declare that a person is guilty, that conduct constitutes an offense, or that a party should prevail. This restraint does not diminish the report's usefulness; it prevents a conclusion belonging to a different area of competence from contaminating the strength of the actual findings.

Plane	Correct example	Excess to avoid
Receipt	"adjunto.csv was received within the EML identified as EV-04."	The bank delivered the full truth.
Result	"The calculated SHA-256 matches the value written in the body."	"The content has never been altered since its origin."
Analysis	"The match links the attachment to the provider's statement."	"The call was made by the account holder."
Conclusion	"Integrity is verified between delivery and receipt."	"The evidence is irrefutable and conclusive."

11.3 The syllogism and the false consequence

A syllogism organizes premises and a conclusion. In forensic work, it helps detect leaps that enthusiasm often conceals. Major premise: a cell records a relationship between the network and a terminal within coverage conditions. Minor premise: the record analyzed associates a communication with cell A. Valid conclusion: there is a documented association between that communication and cell A. What does not follow is that a specific person was at a specific location. Supporting that requires additional premises about location, terminal, and user.

A false consequence appears when a true statement is used as a passport to another that does not follow. The file contains an IP address; therefore, the suspect wrote the message. The signature verifies; therefore, everything said occurred. The video shows a clock; therefore, the entire recording is authentic. The disk is sealed; therefore, the copy analyzed comes from it. Each conclusion requires an additional premise and separate verification. Reasoning is strengthened not by omitting those steps, but by making them visible.

For physical media, contradictory identification can be enough to block an inference. If the receipt record describes one type of disc but the images or capacities correspond to another, do not dismiss it as a minor error. First clarify which object was received, which was acquired, and which appears at each step. Suspend the conclusion until the source's identity is resolved. There is no excellent analysis of the wrong object.[22]

Testing the "therefore"
After every "therefore," write the premise that makes the conclusion necessary. If that premise is merely habit, intuition, or prestige, replace the absolute consequence with a limited observation or perform the missing verification.

11.4 Explain contradictions without hiding them

A contradiction does not always mean falsity. It can reveal a time-zone difference, a clock offset, exports with different filters, two objects with the same name, field interpretations, or a genuinely incompatible source. The report must present the difference using its literal values and analyze possible explanations. Concealing it because it weakens an account is to abandon the scientific function; exploiting it without investigating it is the opposite error.

Suppose a video has an impossible date, call detail records contain a number that does not match the expected format, and two witnesses describe incompatible positions. Do not choose which inconvenience to ignore. Check whether the video retains a counter or an uninitialized system date, whether the number was transcribed or exported incorrectly, and whether the witnesses observed the same event from different locations. If the explanation does not hold, record it as an unresolved inconsistency. State precisely how it affects the conclusion.

The case of the photographs and the bench illustrates the constructive side: everyday sources can offer an explanation compatible with a person's account that seemed improbable. The antenna case illustrates the preventive side: a technical source can be invoked to support something it does not establish. In both, the method is the same: preserve, understand, compare, and limit. Evidence is not used to adorn an accusation or a defense, but to approach a sequence that can withstand review.[23][24]

11.5 Draft conclusions that fit the evidence

A strong conclusion is not necessarily absolute. "No events were observed in the export covering these dates, with these filters and this coverage" is stronger than "they never occurred," because it can be verified and withstands a hostile question. Similarly, "the data reviewed are compatible with sequence A and present these inconsistencies with B" explains the weight of the analysis better than "A was fully proven."

[22] Jocsan Laguna. Sinaloa. Development and conclusions of a technical opinion in digital forensics. Material supplied by the author; errors are generalized without exposing personal data.
[23] Jocsan Laguna. Libro abogados, chapter 1. Narrative research material supplied by the author. Names changed in the guide to protect identities.
[24] Jocsan Laguna. Sinaloa. Development and conclusions of a technical opinion in digital forensics. Material supplied by the author; errors are generalized without exposing personal data.

The degree of assertion must correspond to the method's discriminating power. When only a visual representation exists, describe what is visible and request the native file. When several independent sources exist, explain their convergence and their limitations. When a decisive source is missing, do not compensate with adjectives. The reader must know what was asserted, on what basis, what was excluded, and what new information could change the answer.

Situation	Defensible wording	Information that could change it
Matching hash	The object remained the same between the two documented verifications.	Misidentification of the object or the algorithm recorded.
Attributed account	The events were associated with the account; this alone does not identify the physical user.	Second-factor records, device, credential controls, and corroboration.
Date metadata	The internal date is compatible with the period under investigation, subject to the clock and time zone.	Independent backup, native sequencing and synchronization.
Query with no results	No records were observed within the coverage and filters declared.	Expanded export, corrected filters, or recovery of retention data.

11.6 Challenge and independent review

Before delivery, another person must try to break the reasoning without altering the objects. Check whether the identifier matches the receipt record, whether the copy derives from the source, whether the query produces the same result, and whether the conclusion exceeds the data. This is not limited to correcting commas. A review that merely beautifies the report leaves intact the error that could change the case.

During a hearing, the professional response is not to defend every word as personal property. If a date is wrong, correct it; if a source was unavailable, declare it; if the method does not support an assertion, withdraw it. The expert's authority lies in the quality of the method and willingness to be reviewed, not in refusing to acknowledge a limitation. Challenge is a test of the system, not an insult.



Figure 34. Independent review seeks flaws in the source, method, and inference before delivery. Editorial reconstruction; it does not constitute actual evidence.

Challenge questions
Can I locate the exact object? Can I repeat the query? Is the source independent of the account being evaluated? Is there another compatible explanation? What was not reviewed? Which assertion disappears if I remove a premise?

11.7 Delivery, annexes and subsequent access

The delivery package contains the report, manifest, referenced annexes, and controlled copies where appropriate. Annexes are named identically in the text and files. If a public version is delivered, separate personal data and secrets without destroying the complete preserved version. The report must not publish passwords, private keys, or information that could facilitate further harm.

Verify that the file opens, images are legible, internal links work, and cited annexes exist. Electronic delivery uses an authorized channel, encryption where appropriate, and verification of receipt. The report hash allows version control but does not make its content true. The delivered object must remain reviewable years later, with its format and context available.

Chapter deliverable
A report that answers every question in the assignment, identifies its sources, separates observation from inference, preserves contradictions, declares limitations, and includes annexes sufficient for independent review.

Chapter 12. Errors, learning, and public service

12.1 Errors are not corrected by rewriting the past

Every real procedure contains imperfect decisions: someone connected a device before photographing it, forgot the time zone, received a printout instead of the file, or used an ambiguous name. The professional response is not to erase the event and create an ideal record. Preserve what happened, document its scope, and determine whether the information can be recovered from another source. Improvement begins with the truth of the case file, not its appearance.

A later correction can reduce harm but cannot fabricate retrospective custody. If you calculate a hash today for a file received a month ago, the value provides control from today onward; it does not establish that the object remained intact during the previous month. If a second export is requested, preserve it as a new object with its own receipt and compare it with the first. Recognizing the difference protects both the investigation and the people involved.



Figure 35. The original is preserved; the analysis is carried out on a controlled copy. The exceptions are justified and recorded. Editorial reconstruction; it does not constitute actual evidence.

12.2 Receipt and preservation errors

Powering down by habit can destroy memory and sessions; leaving a device powered on without control can continue modifying data. Working on the original can make it impossible to

show which changes were caused by analysis. Putting a phone in an antistatic bag and calling it Faraday confuses two functions. Packaging without an identifier makes it impossible to know whether the returned object is the same. These failures are not solved by buying more tools: they are prevented through condition, authority, role, and documentation.
It is also an error to treat accessories as irrelevant. A cable or adapter explains the connection; additional storage may contain the source; a power supply can preserve a state while a decision is made. Receipt must examine the whole set without touching items out of curiosity. Photographing, identifying, linking, and requesting support are simple actions that prevent impossible explanations years later.

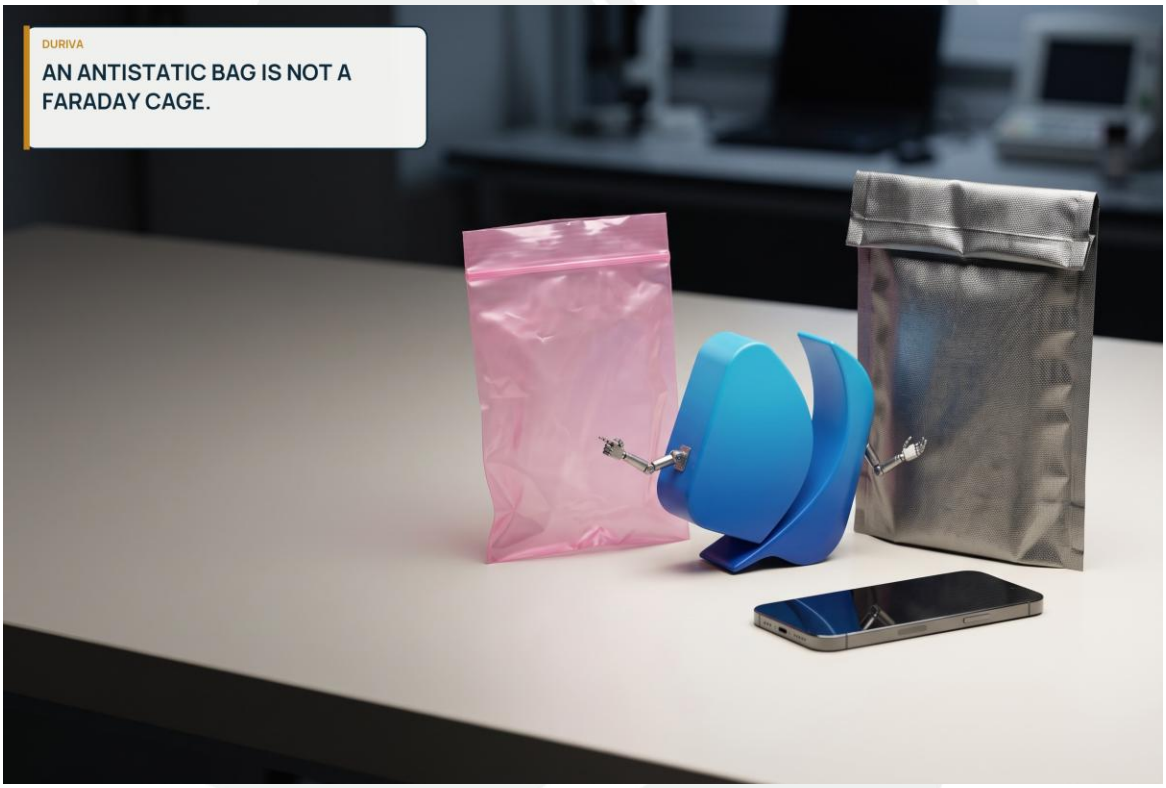


Figure 36. Electrostatic protection and radio-frequency isolation perform different functions. Editorial reconstruction; it does not constitute actual evidence.

12.3 Source, capture and export errors

A screenshot without a URL, date, account, or context is like a photograph of a page torn from a book: it lets you read a fragment but not know the book. Preserve the native source when available, accompany the screenshot with its path and time, and document who obtained it. If only the visual representation exists, say so; do not claim to have reviewed the complete history. The image can be useful without pretending to be the universe.
Exporting without filters, time zone, role, or a field dictionary can produce a file that is correct yet incomprehensible. The same problem occurs when only a PDF of call detail records is received and the email containing the integrity statement is discarded. A robust procedure

requests native format, parameters, process, fields, limitations, a hash in the body, and the delivery EML. This is not bureaucracy: it is the information needed to know what you hold.



Figure 37. Without a URL, date, account, and context, a screenshot remains incomplete even if the image is sharp. Editorial reconstruction; it does not constitute actual evidence.

12.4 Errors of interpretation

Attributing an IP address to a person without reviewing assignment, session, device, sharing, and context turns network data into physical identity. Treating an antenna as an address turns coverage into presence. Treating a date as immutable or as completely useless are two versions of the same problem: failing to ask what produced the field. Serious analysis does not oscillate between credulity and contempt; it evaluates each source according to its mechanism and corroboration.

Synthetic content detectors require the same caution. A percentage alone does not identify authorship, tool, or conduct. Compression, cropping, re-recording, and detector training can alter the result. Preserve the file, version, publication, history, and context; compare methods and explain false positives and negatives. An indication can guide a source request, but cannot replace the source.



Figure 38. An AI detector provides indications with limitations; it does not replace the file, history, context, and corroboration. Editorial reconstruction; it does not constitute actual evidence.

12.5 Legal and applicability errors

An equivalence based on similar wording can be more dangerous than citing no rule at all. Simple, advanced, digital, and qualified signatures do not produce identical effects in every country. A banking rule does not apply to every company. An archival rule does not resolve every private dispute. A bill is not a decree. A useful citation includes the instrument, article, function, scope, version, and official source; if any part is unverified, declare it.

The CNPCF transition illustrates the need to review declarations and reforms before selecting a regime. The repeal in San Luis Potosí of specific AI provisions shows that even a widely discussed reform can cease to be in force. This guide does not attempt to freeze the law: it teaches how to update it without losing the method. The legal version is checked at the time of the case and recorded in the change log.[25][26]

[25]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

[26]San Luis Potosí. Parliamentary Gazette, 30-07-2026: repeal of Article 187 Ter and the chapter containing Articles 272 Bis and 272 Ter. Historical precedent, not a rule in force.Official online source



Figure 39. Verifying legal currency, scope, and reforms prevents a historical citation from being used as a current basis. Editorial reconstruction; it does not constitute actual evidence.

12.6 Lessons learned that change the procedure

A lesson learned must produce an observable change. If an export arrives without a time zone, modify the request to require it. If two objects are confused, review the identifier and photograph. If a tool changes format, update the validation and example. Adding a sentence to an incident folder without changing the procedure merely accumulates documented regret.
Reviews are scheduled according to risk and environmental changes, not an empty calendar. Check official sources, tool versions, provider formats, and storage conditions. When the guide is updated, replace the applicable content and preserve the history rather than stacking contradictory notes. Historical records are not modified; the current procedure is improved.

Fictitious incident	Consequence	Verifiable change
Attachment without EML	The hash statement and delivery context are lost.	The receipt checklist requires EML, attachments, and comparison.
Date without a time zone	The timeline can displace events.	Template with literal value, time zone, conversion, and uncertainty.

Fictitious incident	Consequence	Verifiable change
Seal changed without a record	The opening cannot be reconstructed.	Mandatory opening and resealing event.
Conclusion exceeding the finding	The inference does not withstand challenge.	Review of premises and table of permitted assertions.
Outdated rule	An effect that no longer applies is asserted.	Verification that the rule is in force, with source and consultation date.

12.7 The final measure: prevent the next abuse

The purpose of this guide is not to train people to produce more technical paperwork. It is to help ensure that a correct receipt prevents an accusation built on the wrong object; that an honest timeline prevents a conviction based on incompatible clocks; that an organization preserves the records that can establish what happened; and that a person understands why a screenshot is not enough and what they can request. Technology becomes a service when it reduces arbitrariness.

Giving with open hands does not mean publishing secrets or providing a recipe for harm. It means sharing the foundations that allow people to work with dignity: identify, protect, question, verify, acknowledge limitations, and correct. Knowledge is not held in a closed fist. It is shared with a method so that others can do better and so that no authority—human or technical—has to demand faith where it should offer verification.

Guide conclusion

Preserving evidence is preserving the possibility of truth. The method does not promise to win: it promises that the assertion can be reviewed, that the error can be recognized, and that the conclusion will not be greater than the facts.

Annex A. Functional legal equivalents

Jurisdictions studied: Mexico, Peru, Chile, Argentina, Colombia, Ecuador, and Spain/European Union. Documentary review: 9 November 2026. The governing criterion is functional equivalence, not normative identity.

Executive summary

This matrix answers an operational question: which rule performs, in each jurisdiction, the function that this guide needs to document. It does not start by looking for an article with the same number or similar wording. Functional equivalence makes it possible to compare legal recognition of electronic documents, writing, attribution, integrity, the notion of an original, accessibility, preservation, admissibility, evaluation and burden of proof, as well as sector-specific obligations for records and incidents. Two provisions may pursue the same purpose with different presumptions, recipients, time limits, and consequences; thematic similarity must therefore never be translated into an assertion that they produce identical procedural effects.

The result shows a shared but nonuniform structure. Mexico, Colombia, and Ecuador contain especially clear rules on data messages, written form, originals, integrity, and preservation. Chile and Argentina distinguish precisely among the effects of different classes of signature. Peru distributes the regime among Law 27269, its Regulation, the Code of Civil Procedure, archival rules, and SBS regulation. Spain combines eIDAS, procedural legislation, and payment services rules. In every case, electronic form alone is insufficient to establish authorship, integrity, or content truthfulness. The guide must require source, method, context, continuity, and verifiability; a hash helps compare objects but does not by itself establish who created a file or whether the events narrated occurred.

1. Method and limits of the comparison

Official texts, legislative compilations, official gazettes, and regulator documents were used. Each entry records the instrument and articles actually located. “Direct” means that the function is expressly covered by a comparable structure; “partial” indicates that it covers only one aspect or depends on another rule; “sector-specific” limits the rule to archives, signatures, payments, or supervised entities; “not established” means that the research did not locate a sufficiently verified general rule. The last category does not assert that the country lacks regulation, but that no equivalence should be invented from the available evidence.

The comparison has three practical limits. First, a compilation may incorporate reforms on different dates, and each case requires review of the version applicable to the act and procedure. Second, civil, commercial, criminal, administrative, archival, and financial rules are not interchangeable merely because their terminology is similar. Third, admissibility, authenticity, evaluation, and burden of proof are different questions: a rule may allow a document to be submitted without giving it full probative value or reversing the burden of proof. Accordingly, this matrix guides technical documentation and the location of legal sources, but does not replace legal analysis of the case file or a judicial conclusion.

Level	Operational meaning	Rule for citing it in the guide
Direct	The function is expressly recognized and has a comparable structure.	Explain requirements, exceptions and effects; do not copy only the statement.
Partial	The rule covers part of the function or requires procedural supplementation.	Cite the complementary instrument and delimit what remains outside.
Sector-specific	The rule is limited to archives, certification, payments, or supervised entities.	Do not extend it to all digital evidence or to all subjects.
Not established	A sufficiently verified equivalence was not found.	Write “not established in this review,” never “nonexistent.”

2. Core matrix by legal function

The table focuses on recognition and form. Citations appear within the cells to keep each proposition linked to its source. The categories do not score the quality of a legal system: they describe its usefulness for the guide and the degree of correspondence verified. In particular, the notion of an “original” does not always require retention of a physical device; several legal systems address it through integrity from the final form and subsequent accessibility. The guide must avoid both superstition about the medium and the idea that a screenshot preserves every property of the file from which it came.

When a cell combines rules, the function is distributed and must not be attributed entirely to the first instrument mentioned. Peru is especially instructive: Law 27269 regulates digital signatures and certificates; by itself, it does not contain a general regime for originals and preservation of data messages. Admission of digitally signed documents appears in its Regulation, while microform preservation has a specific archival regime. Separating these sources avoids constructing an elegant but false equivalence.

Recognition of the electronic document

Jurisdiction	Rule, scope, and limitation
Mexico	CCom 89 and 89 Bis: neutrality and non-rejection of data messages.
Peru	Law 27269, Articles 1–2, on electronic signatures; specific scope, not a complete documentary regime.

Jurisdiction	Rule, scope, and limitation
Chile	Law 19.799, Articles 1–3: media equivalence and validity, with exclusions.
Argentina	Law 25.506, Articles 1, 3, and 6, on digital signatures and documents.
Colombia	Law 527, Article 5: effects are not denied because a message is in data form.
Ecuador	Law 67, Article 2: the same legal value as written documents, subject to law and regulation.
Spain / EU	eIDAS Article 46: effects and admissibility are not denied solely because of electronic format.

Table sources:[27][28][29][30][31][32][33]

Written form and subsequent accessibility

Jurisdiction	Rule, scope, and limitation
Mexico	CCom 93 and 93 Bis; CNPCF 349 requires accessibility.
Peru	Regulation 052-2008-PCM, Article 3, on signature requirements; archival accessibility is regulated separately.
Chile	Law 19.799, Article 2.d requires suitable storage for subsequent use; Article 3 addresses written form.
Argentina	Law 25.506, Article 6: a digital document satisfies the written form requirement; Decree 182/2019 addresses preservation.

[27]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
[28]Peru. Law 27269 on Digital Signatures and Certificates and Regulation DS 052-2008-PCM. Specific regime for signatures and admission of digitally signed documents.Official online source
[29]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
[30]Argentina. Digital Signature Law 25.506, Articles 1 and 5–9: digital documents, burden of proof when invoking a disputed electronic signature, and limited presumptions.Official online source
[31]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
[32]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
[33]Regulation (EU) No 910/2014 (eIDAS), Articles 25–26 and 46: non-discrimination of electronic signatures and documents based on format, advanced electronic signatures, and effects of qualified electronic signatures.Official online source

Jurisdiction	Rule, scope, and limitation
Colombia	Law 527, Article 6: message accessible for subsequent consultation.
Ecuador	Law 67, Article 6: information accessible for subsequent consultation.
Spain / EU	eIDAS does not formulate a general rule identical to Article 93 Bis; LSSI and sector-specific rules complement it. Partial; do not force an equivalence.

Table sources:[343536373839]

Attribution and signature

Jurisdiction	Rule, scope, and limitation
Mexico	CCom 90–92; CNPCF 349; presumption based on a reliable and attributable method.
Peru	Law 27269, Article 3, and Regulation 3–4; digital signature under the IOFE and admission of signed documents.
Chile	Law 19.799, Articles 2.f–g and 4–5: simple and advanced signatures do not have identical effects.
Argentina	Law 25.506, Articles 5, 7–9: burden of proof when invoking a disputed electronic signature; presumptions for a valid digital signature.
Colombia	Law 527, Articles 7, 16–17, and 28: reliable method, attribution, and attributes of a digital signature.

[34]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
[35]Peru. IOFE Regulation, DS 052-2008-PCM, Articles 3 and 4: requirement for and admission of digitally signed electronic documents.Official online source
[36]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
[37]Argentina. Decree 182/2019: digital preservation and authenticated copies within the specified periods and conditions.Official online source
[38]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
[39]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

Jurisdiction	Rule, scope, and limitation
Ecuador	Law 67, Articles 10, 13–16: origin, identity, and effects of electronic signatures.
Spain / EU	eIDAS Articles 25–26: non-discrimination of simple signatures; equivalence to a handwritten signature for qualified signatures; requirements for advanced signatures.

Table sources:[40][41][42][43][44][45][46]

Originals and integrity from the final form

Jurisdiction	Rule, scope, and limitation
Mexico	CCom 93 Bis and CNPCF 350: integrity from the final form onward and accessibility; special public-chain rule in Article 350.
Peru	Not established as a general rule in Law 27269. Microforms and archival integrity have a specific regime in DL 681 and DS 001-2000-JUS.
Chile	Law 19.799, Article 2.g addresses detection of modifications in advanced signatures; Article 5 assigns value according to the type of document. Partial.
Argentina	Law 25.506, Article 8: presumption of integrity when digital verification is true. Direct for digital signatures, not universal for every file.
Colombia	Law 527, Articles 8–9: reliable assurance of integrity from the final form and presentation.

[40]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
[41]Peru. IOFE Regulation, DS 052-2008-PCM, Articles 3 and 4: requirement for and admission of digitally signed electronic documents.Official online source
[42]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
[43]Argentina. Digital Signature Law 25.506, Articles 1 and 5–9: digital documents, burden of proof when invoking a disputed electronic signature, and limited presumptions.Official online source
[44]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
[45]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
[46]Regulation (EU) No 910/2014 (eIDAS), Articles 25–26 and 46: non-discrimination of electronic signatures and documents based on format, advanced electronic signatures, and effects of qualified electronic signatures.Official online source

Jurisdiction	Rule, scope, and limitation
Ecuador	Law 67, Article 7: verification of integrity from the final form; Regulation, Article 6.
Spain / EU	eIDAS Article 26.d links data to detect modifications; LEC 326 regulates challenges to authenticity and integrity. Partial and procedural.

Table sources:[47][48][49][50][51][52][53]

Preservation and context of origin, destination, and date

Jurisdiction	Rule, scope, and limitation
Mexico	NOM-151 for preservation and digitization; CCom 93 Bis for accessibility.
Peru	DS 001-2000-JUS for microforms; IOFE Regulation for signatures and certificates. Sector-specific.
Chile	Law 19.799, Articles 2.d and 5: subsequent use and accredited dating for private instruments with advanced signatures.
Argentina	Decree 182/2019, Article 5: digital preservation for specified periods and authenticated copies.
Colombia	Law 527, Articles 12–13: format, exact reproduction, origin, destination, date, and time; third parties.
Ecuador	Law 67, Article 8: accessibility, format, origin, destination, dates, times, and integrity; third parties.

[47]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
[48]Peru. DL 681 and DS 001-2000-JUS: advanced technologies, microforms, authenticity, integrity, and archival preservation. Sector-specific scope.Official online source
[49]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
[50]Argentina. Digital Signature Law 25.506, Articles 1 and 5–9: digital documents, burden of proof when invoking a disputed electronic signature, and limited presumptions.Official online source
[51]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
[52]Ecuador. Regulation under the Law on Electronic Commerce, Electronic Signatures, and Data Messages: incorporation of annexes, dematerialization, integrity, and verification. Official source published by the Judiciary.Official online source
[53]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

Jurisdiction	Rule, scope, and limitation
Spain / EU	Sector-specific and preservation rules; no single general clause equivalent to Law 527.12 was established in this review.

Table sources:[545556575859]

Admissibility and probative assessment

Jurisdiction	Rule, scope, and limitation
Mexico	CCom 1205 admits data messages; CFPC 210-A and CNPCF 348–350 establish reliability, attribution, accessibility, and integrity.
Peru	CPC 188–197: purpose, legality, typical and atypical evidence, and burden of proof; Regulation 4 for digitally signed documents.
Chile	Law 19.799, Article 5: full probative value in specified cases; other documents under general rules.
Argentina	CCyC 318–319: correspondence by any means and assessment of the reliability of media and procedures.
Colombia	Law 527, Articles 10–11: admissibility, sound judicial assessment, generation, storage, communication, integrity, and initiator.
Ecuador	Law 67, Article 14: electronic signatures admitted as evidence; Articles 2 and 7 make effectiveness and originality subject to requirements.
Spain / EU	eIDAS 46 and LEC 326/384: admission, challenge, trust services, and sound judicial assessment.

[54]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
[55]Peru. DL 681 and DS 001-2000-JUS: advanced technologies, microforms, authenticity, integrity, and archival preservation. Sector-specific scope.Official online source
[56]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
[57]Argentina. Decree 182/2019: digital preservation and authenticated copies within the specified periods and conditions.Official online source
[58]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
[59]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

Table sources:[60][61][62][63][64][65][66]

Burden of proof and presumptions

Jurisdiction	Rule, scope, and limitation
Mexico	There is no universal presumption of authorship merely because a file exists; the method and its attribution must be established.
Peru	CPC 196: the burden lies with the party asserting facts in support of its claim or rebutting by alleging new facts, unless otherwise provided.
Chile	Value according to the type of instrument and signature; private dates require attention to accredited dating.
Argentina	Law 25.506, Articles 5 and 7–8: burden of proof when invoking a disputed electronic signature; presumptions apply only within their regime.
Colombia	Law 527, Articles 17, 21, and 28: limited presumptions of origin, receipt, and intent to sign.
Ecuador	Law 67, Article 10: presumption of origin unless proven otherwise and subject to exceptions; no automatic human authorship.
Spain / EU	LEC 326.4: presumption of the disputed characteristic and correct provision when a qualified service is involved, on its own terms.

[60]Federal Code of Civil Procedure, Article 210-A: reliability of the method, attribution, accessibility, and integrity of electronic information. Code repealed by decree of 07-06-2023, subject to the gradual transition regime.Official online source
[61]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
[62]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
[63]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
[64]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
[65]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
[66]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

Table sources:[6768697071]

3. Mexico: legal framework and transition

Mexico offers a complete sequence for the guide, but requires distinction among the commercial regime currently in force, the historical CFPC, and the gradual entry into force of the CNPCF. CFPC Article 210-A recognizes information generated or communicated by electronic, optical, or other technology as evidence and requires assessment of the method's reliability, attribution, and accessibility; its concept of an original rests on integrity from the final form. The Commercial Code contains the substantive architecture of electronic commerce: Articles 89 and 89 Bis, neutrality and non-discrimination; 90–92, attribution, sending, receipt, and acknowledgments; 93 and 93 Bis, written form, originals, integrity, and accessibility; 94, place of dispatch and receipt. Article 1205 was verified directly in the official compilation and expressly admits, among other media, photographs, video, sound, and data messages.[72]
The CNPCF, whose official compilation consulted states a latest amendment of 15 January 2026, contains a similar structure in Articles 348–350 and adds technologies such as blockchain. Article 350 also contains a special evidentiary rule for public-chain records, conditioned on their not demonstrating vulnerability or lack of reliability; it must not be turned into a general assertion that any distributed record is authentic. The transition is gradual and depends on declarations. The compilation consulted retains the general deadline of 1 April 2027; a bill published in the Parliamentary Gazette on 29 April 2026 proposed replacing it with 31 January 2030, but a bill is not a published decree. Before applying that transition to a real case, verify whether a later reform exists in the DOF and which declaration applies to the judicial body.[7374]

Instrument	Verified function	Precision to be retained in the guide
CFPC 210-A	Electronic information as proof; reliability, attribution, accessibility and integrity.	It is the historical basis of the transition, not an article that merely "changes numbers."

[67]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
[68]Argentina. Digital Signature Law 25.506, Articles 1 and 5–9: digital documents, burden of proof when invoking a disputed electronic signature, and limited presumptions.Official online source
[69]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
[70]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
[71]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
[72]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
[73]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
[74]Chamber of Deputies. Parliamentary Gazette, 29-04-2026. Bill proposing to change the CNPCF's entry-into-force deadline to 31-01-2030. This is a bill, not a published decree.Official online source

Instrument	Verified function	Precision to be retained in the guide
CNPCF 348–350	Recognition, reliability, originals, accessibility, and the public-chain rule.	Gradual entry into force; review the declaration and reforms at the time of the matter.
CCom 89–94	Neutrality, effects, attribution, sending/receipt, written form, originals, and place.	Do not confuse acknowledgment of receipt with truthfulness of content or with valid consent in every context.
CCom 1205	Express admissibility of data messages and other media.	Admissibility does not equal full probative value or eliminate challenge and expert examination.
NOM-151-SCFI-2016	Preservation, digitization, accredited PSC, hash, RFC 3161, records, and accessibility.	It is a technical requirement for preservation and digitization within its scope, not a magic certificate of authorship or truthfulness.
CNBV 316 Bis and related provisions	Receipts, notifications, encryption, access, incidents, irregularities, logs, and reviews.	Each article has different recipients, purposes, and deadlines; do not cite “316 Bis” as though it were a single obligation.

Table sources:[7576777879]

NOM-151 merits technical treatment separate from procedural rules. Its usefulness lies in preserving and documenting data messages and in the conditions of digitization, not in declaring that everything stored is true. The standardization page of the Ministry of Economy identifies it as in force, while the DOF text sets out requirements for records, integrity, and accessibility. The guide must record the tool, version, algorithm, date and time zone, operator identity, and relationship among original, copy, and record. It must not promise that a timestamp

[75]Federal Code of Civil Procedure, Article 210-A: reliability of the method, attribution, accessibility, and integrity of electronic information. Code repealed by decree of 07-06-2023, subject to the gradual transition regime.Official online source

[76]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

[77]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

[78]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

[79]General provisions applicable to credit institutions, Articles 316 Bis, 316 Bis 1, and 316 Bis 10 to 17: receipts, encryption, access, incidents, irregularities, logs, and reviews.Official online source

or record alone resolves human authorship, lawfulness of acquisition, or the completeness of a conversation.[8081]

CNBV regulation is broken down as follows: 316 Bis, receipts; 316 Bis 1, notifications; 316 Bis 10, encryption and protection; 316 Bis 11, access control; 316 Bis 12, investigation and notification of incidents, with information to the Commission within five calendar days; 316 Bis 14, irregularities and unrecognized operations with five-year retention; 316 Bis 15, logs with secure retention for 180 days and responses to user requests within ten business days; 316 Bis 17, security reviews at least annually. These periods are not exported to other countries or every type of business. For a forensic examination, request the logs linked to the operation and relevant period, not “all servers” as an indiscriminate formula.[82]

4. Peru: distributed regime and financial update

Peru requires abandoning the idea of a single law on data messages. Law 27269, amended by Law 27310, regulates digital signatures and certificates and contains 16 articles in the official text reviewed. Article 1 recognizes electronic signatures; Article 2 defines their scope; Article 3 defines digital signatures using asymmetric cryptography. The Regulation approved by DS 052-2008-PCM develops the IOFE and, in Articles 3 and 4, regulates the equivalence of digital signatures generated in that infrastructure and the admission of digitally signed electronic documents as evidence. The law itself recognizes a variety of electronic signatures and does not allow any inserted symbol or image to be treated as an accredited digital signature.[8384]

In procedural matters, the Code of Civil Procedure contains general rules in Articles 188–197: purpose, timing, relevance, legality, typical and atypical evidence, ex officio evidence, burden, and evaluation. Article 192 lists party statements, witnesses, documents, expert evidence, and judicial inspection; Article 193 admits technical or scientific aids as atypical evidence; Article 196 allocates the burden unless otherwise provided. Article 245.5 permits the judge to treat as certain a date determined by technical means that produce conviction. For archives, DL 681 and DS 001-2000-JUS cover technologies and microforms, authenticity, integrity, and preservation; their scope must not be confused with a universal rule of originality for every private file.[8586]

[80]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

[81]Ministry of Economy. PLATIICA. Record for NOM-151-SCFI-2016, preservation and digitization of data messages. Consultation of legal status and complementary reference to the DOF text.Official online source

[82]General provisions applicable to credit institutions, Articles 316 Bis, 316 Bis 1, and 316 Bis 10 to 17: receipts, encryption, access, incidents, irregularities, logs, and reviews.Official online source

[83]Peru. Law 27269 on Digital Signatures and Certificates and Regulation DS 052-2008-PCM. Specific regime for signatures and admission of digitally signed documents.Official online source

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

[85]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

[86]Peru. DL 681 and DS 001-2000-JUS: advanced technologies, microforms, authenticity, integrity, and archival preservation. Sector-specific scope.Official online source

Peruvian topic	Useful rule	Operational warning
SBS 504-2021, Article 12.6.g	Preserve evidence for forensic investigations following incidents.	Turn it into a documented procedure, not indiscriminate collection.
SBS 504-2021, Article 15	Significant incident reporting and forensic analysis made available to the Superintendency.	The report must contain an executive summary and technical detail.
SBS 504-2021, Articles 17.3–17.4	Maintain and protect enrolment records, authentication attempts and operations; monitor transactions.	These records are especially relevant for reconstructing sequence and authentication, not automatic proof of physical identity.
SBS 2286-2024, new 20.3	Corporate liability for certain unrecognised operations, except where the liability of the user is established.	It is the correct amendment to SBS 504-2021; do not cite incorrect numbering or the earlier text as though it remained intact.

Table sources:[87][88]

The financial comparison must reflect this 2024 update. Amended paragraph 20.3 covers unauthorized digital-channel transactions without the enhanced authentication requirement, in certain exemption cases or after the user reports theft or loss of credentials, unless the user's responsibility is established. This is different from asserting that the bank is always liable or that use of credentials always proves authorization. The examination must review factors, enrollment, logs, alerts, device context, and sequence, connecting the technical facts with the rule in force at the time of the transaction.[89]

5. Chile: signatures, dates, and security regulation

Law 19.799, in force in the compilation of the Library of the National Congress, regulates electronic documents and their effects. Article 1 establishes media equivalence, Article 2 defines documents and signatures, Article 3 recognizes form and effects with exclusions, Article 4 requires advanced electronic signatures for public instruments, and Article 5 distinguishes probative value. Private instruments with advanced signatures share the regime of full probative

[87]Peru. SBS 504-2021, Articles 12.6.g, 15, and 17.3–17.4: preservation, reporting, and forensic analysis, enrollment records, authentication, and operations.Official online source

[88]Peru. SBS 2286-2024: amendment of Article 20.3 concerning certain unauthorized transactions and liability, unless user responsibility is established.Official online source

[89]Peru. SBS 2286-2024: amendment of Article 20.3 concerning certain unauthorized transactions and liability, unless user responsibility is established.Official online source

value established by law, but their date is not accepted unless electronically certified by an accredited provider. Documents with non-advanced electronic signatures are assessed under general rules. This distinction avoids two errors: denying all value to a simple signature and automatically giving it the value of an advanced signature.[90]

On the banking front, the Updated Compilation of Rules distinguishes Chapter 20-10, Information Security and Cybersecurity Management, from Chapter 20-9 on continuity. Chapter 20-7 regulates outsourcing and requires confidentiality, integrity, traceability, and availability, as well as timely access to records and information required by authorities. Chapter 20-8 addresses reporting of operational incidents. For this guide, functional equivalence is formulated through controls and available evidence, not by asserting that a chapter reproduces 316 Bis. The current rule and the entity's scope must be requested before setting deadlines or minimum content.[91]

Case need	Chilean functional source	Caution
Attribution of document and signature	Law 19.799, Articles 2–5.	Separate formal identification, advanced signatures, and probative effect.
Establishing the date of a private instrument	Law 19.799, Article 5.2.	An advanced signature alone is not sufficient to establish the date.
Review provider/cloud and records	RAN 20-7 and 20-10; incidents, 20-8.	Do not confuse continuity, outsourcing and cybersecurity.

Table sources:[9293]

6. Argentina: limited presumptions and reliability of the medium

Law 25.506 recognizes electronic and digital signatures with different effects. Article 5 defines an electronic signature that lacks one or more requirements for a digital signature and, if disputed, requires the person invoking it to establish its validity. Articles 7 and 8 presume authorship and integrity for digital signatures under statutory conditions; Article 9 determines validity, and Article 6 recognizes written form. Decree 182/2019 regulates preservation and authenticated copies. Law 27.446 repealed former Article 4 of Law 25.506 and replaced other

[90]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
[91]Chile. Updated Compilation of Rules, Chapters 20-7, 20-8, and 20-10: outsourcing, operational incidents, information security, and cybersecurity.Official online source
[92]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
[93]Chile. Updated Compilation of Rules, Chapters 20-7, 20-8, and 20-10: outsourcing, operational incidents, information security, and cybersecurity.Official online source

provisions; the annex must therefore not reproduce historical exclusions as though they were the current text.[949596]

The Civil and Commercial Code provides cross-cutting evidentiary rules. Article 318 permits correspondence to be submitted regardless of the means of creation or transmission, with limits for confidential correspondence. Article 319 requires private instruments to be assessed by considering, among other criteria, congruence, technical clarity, usage, prior relationships, and the reliability of media and technical procedures. The guide can translate those criteria into concrete questions: which system generated the record, who administered the keys, what changes were possible, how it was exported, whether the sequence is congruent, and whether independent corroboration exists. A presumption of cryptographic integrity does not by itself answer those contextual questions.[97]

BCRA regulation	Function	Difference from Mexico
Communication A 7783	Transaction logs available in digital format for at least 90 days; real-time logging for certain messaging services; monitoring.	Its own period and scope; do not replace it with the Mexican 180 days.
Communication A 8280	Cyber incident response and recovery; final report within five calendar days after containment, recovery, and resolution.	The calculation depends on the event described by the rule; it is not identical to the CNBV notice.

Table sources:[9899]

7. Colombia: data messages, preservation, and acknowledgments

Law 527 of 1999 offers a very clear functional correspondence with the Mexican model. Article 5 prevents effects from being denied because of electronic form; Article 6 covers writing and accessibility; Article 7, signing by a reliable and appropriate method; Articles 8–9, originals and integrity; 10–11, admissibility and evaluation; 12–13, direct or third-party preservation; 16–25, attribution, sending, receipt, acknowledgments, duplicates, time, and place. Article 28

[94]Argentina. Digital Signature Law 25.506, Articles 1 and 5–9: digital documents, burden of proof when invoking a disputed electronic signature, and limited presumptions.Official online source

[95]Argentina. Law 27.446: repeal of former Article 4 of Law 25.506 and replacement of other provisions. It prevents the historical text from being cited as currently in force.Official online source

[96]Argentina. Decree 182/2019: digital preservation and authenticated copies within the specified periods and conditions.Official online source

[97]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

[98]Argentina. BCRA Communication A 7783: digital transaction records available for at least 90 days and monitoring of security events.Official online source

[99]Argentina. BCRA Communication A 8280: cyber incident response and recovery; final report within five calendar days after containment, recovery, and resolution.Official online source

establishes attributes of digital signatures. Article 12 requires preservation of information that makes it possible to determine origin, destination, date, and time, an element that must be included in export and custody forms.[100]
The CPACA provides rules for administrative proceedings. Articles 57–58 require authenticity, integrity, and availability of electronic acts and archives; Article 61 requires control of received documents, date and time, security, and acknowledgment; Article 62 regulates proof of sending/receipt and records of service failures. These provisions do not replace Law 527: they address administrative procedure. For the financial sector, External Circular 033 of 2020 was identified as an instrument containing security and cybersecurity instructions, but the recovered sources did not allow all its operative provisions to be identified with certainty. For rigor, the matrix does not attribute deadlines or textual requirements that were not read.[101][102]

Application	Documentary rule	Suggested minimum record
Original message	Law 527, Articles 8–9.	Object in native format, integrity, generation process and display form.
Preservation	Law 527, Articles 12–13.	Format, origin, destination, date, time, custodian and third party involved.
Administrative receipt	CPACA 61–62.	Filing number, acknowledgment, date/time, and a verifiable record of any failure.
Financial cybersecurity	CE 033 of 2020 identified by SFC.	Confirm the provision numbers and official version before imposing specific obligations.

8. Ecuador: documentary equivalence and payment system

The Law on Electronic Commerce, Electronic Signatures, and Data Messages—Law 67—expressly regulates the core functions. Article 2 recognizes the same legal value for data messages in accordance with law and regulation; Article 6 covers accessible written information; Article 7, originals and integrity; Article 8, preservation with format, accessibility, origin, destination, dates, times, and integrity; Article 10, origin and identity with presumptions and exceptions; Article 11, sending and receipt; Articles 13–14, definition and effects of

[100]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
[101]Colombia. CPACA, Articles 57–58, 61, and 62: authenticity and integrity of electronic acts and archives, acknowledgment, and records of service failures.Official online source
[102]Colombia. Financial Superintendency. External Circular 033 of 2020, identified as a security and cybersecurity instruction; its provision numbers must be confirmed before imposing specific obligations.Official online source

electronic signatures. The Regulation addresses incorporation of annexes, dematerialization, integrity, and verification. The presumption in Article 10 does not authorize automatic identification of the individual who pressed a device: it requires analysis of verification, notices, and recipient diligence.[103][104]

In financial matters, Resolution JPRM-2025-006-M, published in Official Registry Supplement 104 of 18 August 2025, regulates payment systems. Articles 77–79 address operation, validity, clearing, and settlement; Article 82 requires individualization of wallet funds and movements and continuous availability; later provisions address participants and supervision. It is a useful source for understanding records and confirmation in the payment system, but does not establish the same log, preservation, and incident obligations as the CNBV. The guide must mark this equivalence as sector-specific and partial and request the regime applicable to the entity and channel before inferring responsibilities.[105]

Necessity	Ecuadorian source	Limitation
Preserve message and metadata	Law 67, article 8.	A display PDF is not enough if the format and the source data are lost.
Attribute a message	Law 67, Articles 10 and 13–14.	Signature and provenance alone do not identify the individual or prove every fact.
Reconstructing electronic payment	Resolution JPRM-2025-006-M.	Payment system regime, not a general equivalent of every CNBV obligation.

9. Spain and the European Union: non-discrimination, trust services, and procedure

Spain requires a combination of European and procedural law. eIDAS Article 25 prevents effects or admissibility from being denied to a signature because it is electronic or not qualified; a qualified signature has the equivalent effect of a handwritten signature; Article 26 defines requirements for advanced signatures; Article 46 prevents effects and admissibility from being denied to a document because of its format. Law 6/2020 regulates certain electronic trust services and repealed Law 59/2003 and Article 25 of the LSSI. Citing the former Electronic Signature Law as if it were in force would therefore be an updating error. Functional equivalence

[103]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
[104]Ecuador. Regulation under the Law on Electronic Commerce, Electronic Signatures, and Data Messages: incorporation of annexes, dematerialization, integrity, and verification. Official source published by the Judiciary.Official online source
[105]Ecuador. Resolution JPRM-2025-006-M, Official Registry Supplement 104, 18-08-2025: operation, validity, clearing, settlement, and availability of funds in payment systems.Official online source

focuses on non-discrimination, signature levels, and trust services, not on copying the Mexican structure.[106][107]

The consolidated LEC, updated on 7 October 2026, distinguishes authenticity from evaluation. Article 326 regulates private documents and their challenge; paragraphs 3 and 4 address electronic documents and nonqualified and qualified trust services, with presumptions in the specified case. Article 384 regulates instruments for archiving, accessing, or reproducing data: examination with the parties' participation, documentation and custody, and evaluation according to sound judicial assessment. The law itself permits challenges to authenticity, integrity, accuracy of date and time, or other characteristics. Presenting an electronic document therefore does not close the technical debate; it opens it with a verifiable object that can be challenged.[108]

Payment services	Spanish rule	Technical application
RD-ley 19/2018, Article 45	Refunds for unauthorised transactions subject to the conditions and exceptions provided for, including a reasoned suspicion of fraud reported in writing.	Distinguish absence of legal authorization from a mere discrepancy concerning a device or credentials.
Article 66	Risk management framework, controls and incident management/classification procedures; at least annual assessment.	Request relevant assessments and controls; do not assume they establish a specific transaction.
Article 67	Immediate notification to the Bank of Spain of serious incidents; information to users without undue delay where their interests are or may be affected.	Preserve a timeline of detection, classification, notification, and mitigation measures.

Table sources:[109]

[106]Regulation (EU) No 910/2014 (eIDAS), Articles 25–26 and 46: non-discrimination of electronic signatures and documents based on format, advanced electronic signatures, and effects of qualified electronic signatures.Official online source

[107]Spain. Law 6/2020 on electronic trust services: repeal of Law 59/2003 and Article 25 of the LSSI; the earlier regime is not cited as being in force.Official online source

[108]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

[109]Spain. Royal Decree-Law 19/2018, Articles 45, 66, and 67: refunds for unauthorized transactions, risk management, and immediate notification of serious incidents.Official online source

10. Functional comparison of financial records and incidents

The following table avoids a frequent simplification: presenting any cybersecurity rule as "the equivalent" of Articles 316 Bis and following. In reality, there are several functions: issuing receipts, notifying the user, controlling access, recording authentication, preserving logs, investigating incidents, informing the regulator, and allocating responsibility for unrecognized transactions. A jurisdiction may cover these functions in separate instruments. The examination must first build a list of necessary data and only then locate its legal basis, not begin with a generic request for "all existing records."

The deadlines shown are deliberately few and tied to the text read. The Mexican 180-day period is not transferred to Argentina, nor the CNBV five-calendar-day period to Peru or Spain. Where a deadline has not been verified, the cell does not invent one. For evidentiary preservation, the guide may recommend immediately preserving a copy and requesting the data from the custodian without waiting for the minimum retention period, because regulatory retention does not guarantee indefinite availability or coverage of every relevant event.

Mexico

Jurisdiction	Rule, scope, and limitation
Records/authentication	CNBV 316 Bis 11 and 15: access and logs.
Incidents	316 Bis 12: investigation and notification.
Unrecognised operations	316 Bis 14: Unrecognized incidents and operations.
Verified period and scope	180 days for logs under 316 Bis 15; five years for 316 Bis 14; five-calendar-day notice under 316 Bis 12, within their respective scopes.

Table sources:[110]

Peru

Jurisdiction	Rule, scope, and limitation
Records/authentication	SBS 504-2021, 17.3–17.4: enrollment, attempts, and operations; monitoring.
Incidents	12.6.g and 15: preservation, reporting and forensic analysis.

[110]General provisions applicable to credit institutions, Articles 316 Bis, 316 Bis 1, and 316 Bis 10 to 17: receipts, encryption, access, incidents, irregularities, logs, and reviews.Official online source

Jurisdiction	Rule, scope, and limitation
Unrecognised operations	SBS 2286-2024 amends 20.3 and liability unless user responsibility is established.
Verified period and scope	Do not extrapolate a single deadline; read the applicable rule and amendments.

Table sources:[111]

Chile

Jurisdiction	Rule, scope, and limitation
Records/authentication	RAN 20-10; outsourcing and records in 20-7.
Incidents	RAN 20-8.
Unrecognised operations	Requires rules specific to the product and channel.
Verified period and scope	Unverified time limits are not assigned.

Table sources:[112]

Argentina

Jurisdiction	Rule, scope, and limitation
Records/authentication	BCRA A 7783: security transactions and events.
Incidents	BCRA A 8280: response, recovery and final report.
Unrecognised operations	Channel rules and user regulations; do not infer them only from authentication.
Verified period and scope	Digital records retained for at least 90 days under A 7783; final report within five calendar days in the case described by A 8280.

[111]Peru. SBS 2286-2024: amendment of Article 20.3 concerning certain unauthorized transactions and liability, unless user responsibility is established.Official online source
[112]Chile. Updated Compilation of Rules, Chapters 20-7, 20-8, and 20-10: outsourcing, operational incidents, information security, and cybersecurity.Official online source

Table sources:[113]

Colombia

Jurisdiction	Rule, scope, and limitation
Records/authentication	Law 527 for general preservation; SFC for supervision.
Incidents	CE 033 of 2020 identified as an instruction in this area.
Unrecognised operations	No sufficiently verified textual rule was established in this review.
Verified period and scope	Confirm provision numbers and the official text before using deadlines or mandatory fields.

Table sources:[114]

Ecuador

Jurisdiction	Rule, scope, and limitation
Records/authentication	Law 67.8 for message; JPRM-2025-006-M for payment system.
Incidents	No comprehensive equivalence with the CNBV was established.
Unrecognised operations	Requires the regime specific to the entity and channel.
Verified period and scope	Do not invent a log or incident deadline.

Table sources:[115]

Spain

Jurisdiction	Rule, scope, and limitation
Records/authentication	RD-Law 19/2018, 66: risks and controls.

[113]Argentina. BCRA Communication A 7783: digital transaction records available for at least 90 days and monitoring of security events.Official online source
[114]Colombia. Financial Superintendency. External Circular 033 of 2020, identified as a security and cybersecurity instruction; its provision numbers must be confirmed before imposing specific obligations.Official online source
[115]Ecuador. Resolution JPRM-2025-006-M, Official Registry Supplement 104, 18-08-2025: operation, validity, clearing, settlement, and availability of funds in payment systems.Official online source

Jurisdiction	Rule, scope, and limitation
Incidents	Article 67: serious incidents and notification to users.
Unrecognised operations	Article 45: refund under conditions and exceptions.
Verified period and scope	Serious incident: immediate; risk assessment at least annually; statistical data at least yearly.

Table sources:[116]

11. International methodological standards

ISO/IEC 27037:2012 provides guidelines for the identification, collection, acquisition, and preservation of potential digital evidence. ISO's official record states that the edition was reviewed and confirmed in 2018 and remains in force. Its definitions make it possible to specify identification, preservation, bit-for-bit imaging, repeatability, and reproducibility. The standard is used to build procedures and controls, not to declare a document authentic or admissible merely because a particular tool was used. Nor does it replace the rules of each jurisdiction or judicial assessment.[117]

NIST SP 800-86 organizes the process into collection, examination, analysis, and reporting and connects files, operating systems, traffic, and applications with incident response. The guide cautions that it is not a universal procedure or legal advice. For this guide, its contribution is to structure sources and documentation; for the legal annexes, it is a technical guide. Good practice is to map each phase to working evidence: source and authority identification, documented acquisition, verification, findings, alternative hypotheses, and bounded conclusions. The goal is not to manufacture certainty, but to make visible what was done, what can be repeated, and what remains unproven.[118]

Guide phase	Methodological reference	Required quality evidence
Identification	ISO/IEC 27037	Source, custodian, condition, authority, risk of alteration, and priority.
Acquisition	ISO/IEC 27037 and NIST SP 800-86	Method, tool/version, date and time zone, hash where applicable, incidents, and original/copy relationship.

[116]Spain. Royal Decree-Law 19/2018, Articles 45, 66, and 67: refunds for unauthorized transactions, risk management, and immediate notification of serious incidents.Official online source

[117]ISO/IEC 27037:2012. Guidelines for the identification, collection, acquisition, and preservation of digital evidence. Edition confirmed by ISO as remaining in force.Official online source

[118]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodological guidance, not legislation or a guarantee of admissibility.Official online source

Guide phase	Methodological reference	Required quality evidence
Examination and analysis	NIST SP 800-86	Working copy, hypotheses, tests, negative results, and reproducibility.
Report	NIST SP 800-86 and local procedural law	Facts, method, findings, limitations, annexes, and possible challenge.

12. Rules for using the matrix without false equivalences

The first rule is to cite function + instrument + article + scope + version, not “the equivalent law.” The second is to preserve distinctions: simple, advanced, digital, or qualified signatures; electronic originals and printed copies; presumptions of integrity and proof of authorship; archival preservation and forensic custody; authentication records and consent; admissibility and probative force. The third is to record the consultation date and review later reforms when the case requires. The fourth is not to use a banking rule to justify any private investigation outside its personal scope, or an administrative rule to resolve every civil or criminal proceeding. The second check is substantive. Before closing the guide’s annex, verify that every link opens the source, that the article exists in the downloaded text, that Peru has not been assigned a general regime absent from Law 27269, that the Peruvian amendment is SBS 2286-2024, that Argentina does not reproduce as current the article repealed by Law 27.446, and that Spain does not cite Law 59/2003 as current. The Mexican transition must keep the CNPCF compilation, the bill to extend the deadline to 2030, and any decree actually published separate. AI regulation in San Luis Potosí is documented in a separate case file because it contains a reform and subsequent repeal, not a custody rule.

Editorial control	Acceptance question	Action on failure
Identity	Do the instrument and the article literally appear in the source?	Remove the citation or mark it as unverified.
Function	Does the rule actually regulate the function described?	Reclassify as partial/sector-specific and explain the limitation.
Legal currency	Are the version and reforms applicable to the act?	Record the date and conduct a specific review in the official gazette.
Scope	Are the subject, channel, and procedure covered?	Do not extend the rule; request the special regime.

Editorial control	Acceptance question	Action on failure
Effect	Are admission, authenticity, value, and burden of proof distinguished?	Rewrite the conclusion without automatic presumptions.
Technical test	Does the format permit verification of what the rule requires?	Preserve the native file, context, metadata, and export process.

Operational conclusion: the guide does not need a table of similar phrases, but a guide for demonstrating the same problem under different rules. Useful functional equivalence makes it possible to decide what to preserve, request, verify, and limit. Anything that cannot be supported by a verified source and scope must be excluded or expressly marked as not established.

Scope of the study
Legal notice: this document is general research and editorial-design material. It does not constitute legal advice, an expert opinion, or an opinion on a specific case. Application to a case file requires review of the law in force at the time of the events, jurisdiction, subject matter, channel, and applicable procedural rules.

A.13 Practical application: select the regime before the conclusion

A case file may touch several countries without all their rules applying to every act. An account administered in Mexico, a provider in Chile, and a transaction challenged in Spain require separation of the place of the act, regulated person, channel, contract, procedure, and temporal version. The first step is not to translate Article 210-A, but to identify the function needed: preserve the message, establish attribution, obtain logs, reconstruct authentication, or review an incident obligation. Then locate the rule that performs that function for that person and procedure.

Step	Applied question	Documented result
Define	Which act, person, channel, and procedure is being analyzed?	Jurisdiction and scope map.
Locate	Which rule covers the function in that subject matter?	Instrument, article, version and official source.
Classify	Is the equivalence direct, partial, or sector-specific?	Express limitation and complementary rules.

Step	Applied question	Documented result
Preserve	Which object permits verification of the requirement?	Native file, context, metadata, export, and custody.
Conclude	Which effect is established and which is not?	Limited assertion without importing external presumptions.

A.14 Data protection during an investigation in Mexico

Forensic custody is not a general exception to data protection. Processing must maintain purpose, proportionality, security, and confidentiality; the complete case file is not shared merely for convenience. Separate working and disclosure versions, restrict access, and avoid retaining third-party data that does not answer the assignment. Significant breaches must be handled with the diligence required by law, including information to affected individuals so that they can defend their rights. The current federal authority is the Secretaría Anticorrupción y Buen Gobierno, under the transition begun in March 2025.[119][120]

Compared rule
Useful legal equivalence ends in a verifiable decision: what to preserve, what to request, what to check, and what not to assert. If the analysis changes none of those answers, the citation is decorative.

[119]Federal Law on the Protection of Personal Data Held by Private Parties, new law published on 20-03-2025 and amended on 14-11-2025. Articles 5–9, 18–20, and 31: principles, security, confidentiality, breaches, and time limits.Official online source
[120]Secretaría Anticorrupción y Buen Gobierno. Communiqué 011, 21-03-2025: transfer of personal data protection functions from the INAI to the Secretariat.Official online source

Annex B. Scope and authority form

Complete this form before accessing the source. Its function is to prevent the assignment from expanding impulsively or technical capability from being confused with permission. If the object, period, or purpose changes, create a new version and retain the previous one. Every unavailable field must explain why and identify the person who can resolve it.

B.1 Form content

Field	Required content	Complete fictitious example
Identifier	Case code with no client name or sensitive data.	EXP-DEMO-2026-001.
Purpose	Intended use: operational continuity, internal investigation, forensic examination, or proceedings.	Determine the recording, transmission, and settlement of the sales claimed.
Separate accounts	What each party alleges, without presenting it as a proven fact.	Merchant: unpaid sales. Processor: transactions not received.
Period	Start, end, time zone, and required precision.	1 to 3 November 2026, local time −06:00.
Sources included	Authorized systems, files, accounts and devices.	Remittances, processor reports, and bank credits for three references.
Exclusions	What will not be reviewed, and why.	Personal devices and mail outside the case references.
Authority	Authorizing holder, instrument, permitted actions, and validity period.	Authorized representative; documented administrative consultation and export.
Risks	Volatility, privacy, continuity, third parties and points of no return.	Log rotation and personal data of unrelated buyers.
Deliverable	Product, format, recipients, channel and review.	Technical report, manifest and exports; encrypted delivery to the person responsible.

Field	Required content	Complete fictitious example
Control of changes	Version, date, requester, authorizer, and effect on sources.	A01: the processor field dictionary is added without expanding the devices.

Starting condition
Do not perform acquisition until scope, authority, and exclusions can be answered. If urgency requires action, record the exceptional decision, its basis, and the limits of what was done.

Annex C. Receipt and initial preservation record

Complete the record when the object is received, not when analysis ends. Describe observations and the deliverer's statements separately. Link photographs to the identifier, but do not use them to replace the description. If a prior action is unknown, write "unknown" with an explanation; do not replace it with a reassuring assumption.

C.1 Example physical receipt record

Field	Fictitious record
Case and evidence	EXP-DEMO-2026-001 · ED-20261109-DEMO-SSD-003-R00.
Object	2.5-inch SATA SSD, declared capacity 512 GB; visible serial number DEMO-003.
Delivery	Custodian A, authorised administrative officer; 9 November 2026, 14:32 −06:00.
Receipt	Analyst B, assigned specialist; receiving laboratory.
Observed condition	Powered off and disconnected; casing with no visible deformation; connector with no apparent residue.
Accessories	SATA cable and power supply registered as related objects ACC-003-01 and ACC-003-02.
Declared history	The unit was removed by system personnel; it is unknown if it was connected after the incident.
Photographs	FOT-003-01 general; FOT-003-02 serial number; FOT-003-03 connectors and accessories.
Packaging and seal	Antistatic bag inside a rigid container; seal SL-DEMO-003 intact.
Initial decision	Preserve, validate the write blocker, and prepare authorized physical acquisition.
Observations	The device was not powered on or explored during receipt. No passwords written in the record.

C.2 Receipt of files or messages

For electronic receipt, replace physical-condition fields with channel, account, apparent sender, URL or message, permissions, original filenames, sizes, and download date. Preserve the file before renaming or converting it. If it comes from email, preserve the EML and calculate separate hashes for the message and attachments. If it comes from a link, record who accessed it and which version was available.

Control	Fictitious example
Channel and message	Provider email received on 9 November 2026, 15:02 −06:00.
Complete object	entrega_001.eml preserved with body, headers, and two attachments.
Attachments	registros.csv and diccionario.pdf; original filenames preserved in the manifest.
Provider statement	The body declares algorithm SHA-256 and a value for each attachment.
Verification	Documented local calculation: registros.csv matches; diccionario.pdf does not match.
Action	Do not edit any attachment; request clarification and a second delivery of the PDF.
Limitation	The CSV match establishes equality with the delivery, not truthfulness or complete coverage.

Annex D. Acquisition record

The record must allow understanding what was copied, with what coverage and under what conditions. The tool is not cited as a trusted mark: it is accompanied by version, configuration, validation and result. Errors are kept along with the output. If the acquisition is repeated, a new identifier is created and the relationship is explained.

D.1 Complete example

Field	Fictitious record
Case and acquisition	EXP-DEMO-2026-001 · ED-20261109-DEMO-SSD-003-A01.
Related source	ED-20261109-DEMO-SSD-003-R00, identified in the receipt record.
Objective and coverage	Physical image of the complete medium, including unallocated space, for further examination.
Authority	Form A01; scope limited to the SSD received and the defined incident.
Connection	Source connected to the write blocker and the blocker to the workstation; model and ports recorded in the log.
Tool	Tool validated for a test image; name, version, and configuration recorded in the technical record.
Date and time zone	Start 2026-11-09T15:21:08−06:00; end 2026-11-09T16:47:52−06:00.
Output	ssd003_A01.e01 and log file; working copy separate from the preserved original.
Integrity	Algorithm SHA-256; value associated with the image file in the controlled manifest.
Incidents	Twelve unreadable sectors documented; do not suppress the message or declare a perfect acquisition.
Verification	The output opens, the size is consistent with the medium and the verification value matches.

Field	Fictitious record
Closure	Original resealed with a new identifier; previous seal and opening recorded in custody.

Acceptance criterion
It is not enough for the file to exist. It must open, be linked to the source, have its coverage described, and preserve incidents. If a stage cannot be verified, record it before continuing.

Annex E. Chain of custody and transfers

The log records events, not just transfers. Opening a seal, creating a copy, downloading a file, or accessing a container can also change who is responsible and what must be verified. Each row links the object, responsible persons, purpose, location, seal, and integrity. Keys are never written in this form.

E.1 Example of sequence

Event	Responsible persons and purpose	Verification and outcome
Receipt 09-11 14:32 −06	Custodian A delivers the SSD-003 to analyst B for preservation.	Serial number and photographs match; seal SL-003 intact.
Opening 09-11 15:18 −06	Analyst B opens the container for authorized acquisition.	The previous seal and reason are preserved; the object has not changed.
Acquisition 09-11 15:21 −06	Analyst B generates A01 on a validated workstation.	Output, incidents, and hash are recorded in D.
Resealing 09-11 16:55 −06	Analyst B returns the source to the container.	New seal SL-003-B; original kept separate from the working copy.
Transfer 10-11 09:10 −06	Custodian C delivers copy A01 to reviewer D through an encrypted channel.	Recipient, permissions, download and hash verification confirmed.
Consultation 10-11 11:42 −06	Reviewer D opens the copy to review the hypothesis matrix.	Access logged; no modification to the original.

E.2 Electronic transfer

A link-based transfer includes the sender, recipient, permissions, expiration date, version, key delivery channel, and download verification. Receipt is not presumed merely because the system says “sent.” The recipient confirms the object’s identity, size, and hash where applicable. If the link is replaced, preserve the history of both deliveries.

Annex F. Request and acquisition through a provider

This format avoids asking for “all the information” and receiving a table without context. The request defines the question, fields, and delivery method. Authorization is sent through a secure channel; the example contains no real data. If the provider cannot meet a requirement, it must state this in the response so that the limitation travels with the evidence.

F.1 Model request

Fictitious request for records and verifiable delivery
Subject: EXP-DEMO-2026-001 · Records for 1 to 3 November 2026

Through the authorized secure channel, I request the events associated with the references included in the case file, from 2026-11-01T00:00:00−06:00 through 2026-11-03T23:59:59−06:00. Please indicate the time zone used by the system, daylight saving time, and the conversion rule.

Please include, where available: date/time, event type, direction, duration, identifiers, cell, technology, result, and an explanation of blank fields. Include native CSV/XLSX format, a PDF reference copy, field dictionary, extraction process and date, filters, coverage, and retention limitations.

In the body of the response, indicate the algorithm and hash value for each file. Preserve the delivery in EML format with body, headers, and attachments. Do not send keys or credentials in that email.

Authorized technical officer · EXP-DEMO-2026-001

F.2 Export or API record

Field	Fictitious example
Account and role	DEMO administrative account; read-only and export role.
System and version	Supplier portal; documented interface version or date.
Query	Period, references, and event types; filters preserved in the log.
Time zone and format	UTC declared; native CSV and field dictionary.

Field	Fictitious example
API, if applicable	Endpoint, version, parameters, pagination and limits; no secrets in the report.
Result	Two files, with row counts and export errors recorded.
Delivery	Full EML, URL or controlled channel and download date.
Verification	Hash of each object and relation to the supplier's declaration.
Coverage and limitation	Available retention, missing data, and period not covered.

Annex G. Inventory and manifest of objects

The manifest links objects and prevents a folder from becoming a collection without provenance. Each row corresponds to a file, image, export, visual representation, or report. Path and size help identify it; the hash controls that specific object. Sensitive data is omitted from public versions without destroying the complete working version.

G.1 Example of manifest

Identifier	Relationship and object	Control
DEMO-EML-001-R00	Original email received; body, headers, and attachments.	Name, size, receipt date, and SHA-256 in the controlled record.
DEMO-CSV-001-R00	Attachment registros.csv extracted from the EML without modification.	Matches the hash declared in the body; 18,420 rows.
DEMO-PDF-001-R00	Attachment diccionario.pdf from the first delivery.	Hash does not match; preserved for comparison and clarification.
DEMO-PDF-001-R01	Second delivery of the dictionary; a distinct related object.	New date and new hash; it does not silently replace R00.
DEMO-CSV-001-W01	Working copy of the CSV for consultation.	Derived from R00; analysis changes are stored separately.
DEMO-INF-001-V10	Report version 1.0 and referenced annexes.	Encrypted delivery; distribution hash and recipient documented.

Naming rule
The operational name does not erase the original. The manifest preserves the received name and adds the internal identifier, so organizing never means altering the source.

Annex H. Timeline and time zones

The timeline separates what the source states from the conversion performed by the analyst. Never replace the original value with a “corrected” date. Precision is expressed using available granularity: day, minute, second, or window. If synchronization is not established, record it as a limitation instead of turning time into fictitious certainty.

H.1 Example of timeline

Source and literal value	Normalization	Permitted interpretation
Server: 2026-11-03 20:14:07 UTC	2026-11-03 14:14:07 −06:00; second-level precision.	Event observed on the server; physical authorship not established.
Email: 03 Nov 2026 14:20:11 −06:00	No conversion; header preserved in EML.	Reception six minutes later; proximity does not prove causation.
Photograph: 2026:11:03 14:16:00	Time zone not declared; device clock pending verification.	Compatible only if the time zone and clock are confirmed; not ordered as certain.
Testimony: “after eating”	Approximate window; no exact time is assigned.	Context declared by a person, not a technical record.
Export: 1 to 3 November	Limited coverage; no query outside that period.	Absence of events outside the scope cannot be asserted.

H.2 Rule for conflicting dates

First check whether the events concern the same object and meaning; then check time zone, clock, conversion, format, and export process. Only then assess manipulation. Preserve the contradiction with both values and their possible explanation. A useful timeline shows where the doubt lies instead of hiding it beneath an ordered cell.

Annex I. Hypothesis and corroboration matrix

Formulate the matrix before writing conclusions. It must include a test capable of weakening each hypothesis, not only data that supports it. When two sources come from the same file, mark their dependency; counting them as independent corroboration would artificially inflate the weight of the evidence.

I.1 Worked example

Element	Fictitious development
Assertion	The file was created for the first time on 3 November in the former employee's account.
Hypothesis A	New creation on that date using the assigned account.
Hypothesis B	Copy or subsequent modification of a previous document.
Hypothesis C	Use of the account by another person or uncontrolled session.
Sources	Native file, cloud history, sessions, second factor, previous backup.
Test	Compare version, application author, session, and device; review the preceding sequence.
Finding	Previous version dated 28 October and a session from an unregistered device.
Effect	Weakens new creation and automatic attribution to the account holder.
Limitation	It does not yet identify who controlled the device or the intent.
Additional action	Request enrollment and device activity records within the authorized scope.
Provisional conclusion	The visible date does not establish initial creation; the account alone does not identify the person.

Ego-free decision-making
If a finding contradicts the initial hypothesis, change the hypothesis or conclusion. Do not alter the object or omit the finding to preserve a convenient account.

Annex J. Review of synthetic content

The goal is not to obtain an “AI” percentage, but to document origin, transformations, and publication. Generation, editing, transcoding, and re-recording are distinct events. If a detector is used, record its name, version, configuration, and limitations. A positive or negative result does not replace the file or its context.

J.1 Applied format

Field	Fictitious example
Object received	video_publicado.mp4; link, account, date and copy preserved.
Earlier source	The generation file is unknown; request it from the holder and platform.
History	Publication, download, and conversion documented as separate events.
Declared tool	There is no statement from the publisher; do not presume a specific tool.
Technical analysis	Encoding, frames, audio, continuity, and available metadata.
Detector	Indicative result; version and limitations documented, with no automatic verdict.
Corroboration	Camera original, editing history, and early publication requested.
Legal context	Consent, identity, use, conduct, date, and law in force assessed separately.
Permitted conclusion	The file shows transformations consistent with editing; origin and author are not established.
Source that would change the outcome	Original file with verifiable history or records of the generation service.

Annex K. Report structure and conclusion

The template organizes content but does not replace reasoning. Each chapter of the report answers a reader's question and refers to specific annexes. Personal data is limited to what is necessary. The executive and technical reports may be separated to support management reading and specialist review without losing their relationship.

K.1 Recommended sequence

Section	Question to be answered	Minimum content
Assignment and scope	What was requested and what was excluded?	Questions, purpose, jurisdiction, period and exclusions.
Authority and roles	Who authorized and who executed?	Authorizations, roles, communications, and declared conflicts.
Sources	What objects were received or acquired?	Manifest, identifiers, conditions, representations, and absences.
Method	How was it examined and with what coverage?	Tools, versions, parameters, dates, queries and incidents.
Findings	What was observed?	Positive, negative, and inconclusive results with reference to the object.
Analysis	What explanations were compared?	Hypotheses, corroboration, contradictions, and false consequences avoided.
Conclusions	What can be asserted within the scope?	Answer by question, degree of assertion, and basis.
Limitations	What was not established?	Missing sources, coverage, clock, formats, errors and access.
Annexes and delivery	How is it checked?	Receipt records, acquisitions, manifest, timeline, queries, and version control.

K.2 Example of a complete conclusion

Fictitious conclusion
The registros.csv file received as an attachment to message DEMO-EML-001-R00 matched the SHA-256 value declared by the provider in the email body. This establishes equality between the attachment received and the file to which that statement refers. The export contains 18,420 rows covering 1 to 3 November 2026, expressed in UTC according to the dictionary provided. No events involving the three references queried were observed within that coverage. This result does not establish that no transactions occurred outside the period, through other channels, or in records not supplied, nor does it identify the person who may have performed them.

The conclusion above does not need the phrase “with full legal certainty” or a promise of judicial success. Its strength lies in the fact that every component can be located: message, file, hash, rows, period, references, and limitation. If the opposing party finds another source, the analysis can be expanded without destroying the earlier work.

Annex L. Operational checklists

The checklists are used as a final control, not as a substitute for professional judgment. Every affirmative answer requires locatable evidence. “Not applicable” requires a reason. If a control fails, record who decides to continue, why, and with what limitation. The questions may be printed and adapted to the procedure without becoming a retrospective declaration of actions not performed.

L.1 Receipt and acquisition

Control	Expected evidence	If it fails
Are scope and authority documented?	Signed form or verifiable authorization.	Stop and clarify; record the exception if any.
Does the object have an identifier and condition?	Receipt record, serial number, photographs, and accessories.	Do not analyze until identity is resolved or a limitation is declared.
Are the source and the copy separate?	Original/derivative relationship and location.	Create a controlled copy without rewriting the receipt.
Are the method and coverage clear?	Acquisition record, filters and format.	Complete the log with what was actually done.
Does the output open and verify?	Opening test, manifest, and relevant hash.	Repeat as a new object and preserve the incident.
Were errors and exclusions recorded?	Incidents, filters, missing fields, and reason.	Do not declare exhaustiveness; limit the conclusion.

L.2 Analysis, reporting and delivery

Control	Question for review	Required result
Traceability	Does every conclusion lead back to a finding and source?	Full route and matching annexes.
Timeline	Are literal values, time zones, and precision preserved?	Explained conversion and visible uncertainty.

Control	Question for review	Required result
Hypothesis	Was evidence sought that contradicts the initial account?	Alternatives, negative and inconclusive results.
Language	Are integrity, authorship, and truthfulness separated?	No absolutes or false consequences.
Challenge	Did another person attempt to identify flaws?	Observations, response and changes recorded.
Legal currency	Do the rules correspond to the subject, matter, and date?	Official source, version, function and scope.
Delivery	Does it open, is it readable, and does it contain the cited annexes?	Package verified, channel and receipt confirmed.
Privacy	Does the published version prevent unnecessary exposure?	Access, minimization and controlled versions.

Annex M. Version, source, and lesson control

Version control distinguishes the historical case file from the procedure currently in force. A past record is not modified to appear updated; a guide is corrected when the rule or tool changes. Each change identifies the reason, source, responsible person, date, and effect. Unverified sources are not presented as verified.

M.1 Regulatory and technical record

Element	What to record	Example
Instrument or tool	Full name, subject matter, jurisdiction or version.	CNPCF, Articles 348–350; tool and validation version.
Source and consultation	Official URL, date, compilation, and responsible person.	Chamber of Deputies portal, documented consultation.
Change detected	Reform, repeal, declaration, or change of behavior.	Bill separated from decree; new export version.
Functional effect	What requirement or decision changes and for whom.	Update the transition regime or field dictionary.
Editorial action	Chapter, table or modified format.	Replace current text and keep history.
Review	Person, date, test, and next risk-based review.	Verify the article in the source and test the fictitious example.

M.2 Turning a lesson into improvement

Field	Fictitious example
Incident	An export was received without a time zone or dictionary.
Impact	A reliable timeline could not be constructed and blank fields could not be interpreted.
Cause	The earlier request asked for a “complete report” without format or context.
Case correction	A new delivery was requested while preserving the first and its limitation.

Field	Fictitious example
Preventive change	Annex F requires time zone, dictionary, filters, native format, hash, and EML.
Verification	Exercise with a fictitious provider: all fields arrive and can be opened.
Responsible person and version	Methodological reviewer; Form F moves from 1.0 to 1.1 with date and reason.

Continuity rule
A new version does not hide the previous one. It shows what was believed, what changed, based on which source, and how this affects future cases, without altering case files already closed.