TEQUILA SO
Jocsan Laguna

Digital Evidence Handling

Preserve, acquire, document, analyze and present

PRACTICAL MANUAL · 2026



Introduction to the manual

This manual explains how to receive, preserve, acquire, transfer, analyze, and present digital evidence using a method that others can review. It is written for police officers, forensic experts, lawyers, and organizational leaders. You do not need to be an engineer: each term is explained through an action and an example. It does not replace the authority, applicable law, or professional judgment required in each case.

The central rule is simple: do not open a device and search for whatever confirms a suspicion. Decide what must be established, locate where the evidence may be, choose the least invasive suitable method, and document what was done. A useful conclusion is not the one most confident in itself, but the one that clearly distinguishes facts, inferences, and open questions.

How to use this manual

If you are the first person to receive a case, go to Chapters 1, 3, 5, and 7. There you will learn how to define the assignment, decide who does what, choose an acquisition path, and document receipt without improvising. If you will acquire or analyze evidence, work through Chapters 4, 6, 8, 9, and 10. If you need to review a request, report, or presentation, use Chapters 2, 11, and 12 and Annexes A, K, L, and M.

The examples are fictitious and complete, intended to demonstrate the reasoning rather than prescribe a formula. The forms include fill-in fields and instructions. The legal matrix compares functions and does not claim that two articles are identical. Dates and versions matter: before applying a rule, verify that it is in force and applicable to the facts, subject, channel, and procedure.

Guiding principles

Principle	Practical application
Minimal alteration	Choose the method that causes the least alteration and document any unavoidable change.
Authority before access	Having permission is not the same as having the technical ability to gain access. Both are required.
Context before fragments	An isolated screenshot does not replace the file, complete message, or publication.
Ockham's razor	Start with the source that best distinguishes between hypotheses; do not accumulate tools.
Ego-free decision-making	If the evidence contradicts the initial account, correct the conclusion, not the original.
Reproducibility	Another qualified person must be able to locate, review, and repeat the procedure.
Explicit limitations	Declare what was not observed or established; do not fill gaps with assumptions.
Protecting individuals	Preserving evidence does not authorize disseminating data or revictimizing anyone.

Contents

Introduction to the manual 2
How to use this manual 3
Guiding principles 4
Contents 5
Chapter 1. Scope, questions, and authority 8
1.1 The question that governs all work 8
1.2 Authority, proportionality, and confidentiality 9
1.3 Initial source inventory 9
1.4 Complete example: a sales claim 9
Chapter 2. Integrity, originals, and context 11
2.1 The original is not always the device 11
2.2 Integrity, authenticity, attribution, and truthfulness 11
2.3 Hash as a control, not a dogma 12
2.4 Accessibility and context preservation 12
Chapter 3. Roles and responsibilities 13
3.1 Functions before job titles 13
3.2 Operational communication 14
3.3 Independence and review 14
Chapter 4. Lifecycle and forensic readiness 15
4.1 Prepare before receiving a case 15
4.2 Points of no return 15
4.3 Documented lifecycle 16
Chapter 5. Decision trees by scenario 17
5.1 Device powered on or off 17
5.2 Local, remote, or provider acquisition 17
5.3 Mobile devices and isolation 17
5.4 When to stop 18
Chapter 6. Modern sources and call detail records 19
6.1 Cloud, SaaS, and exports 19
6.2 Email and EML 19
6.3 Requesting and receiving call detail records 20
6.4 Example provider request body 20
6.5 Virtualization, IoT, and synthetic content 21
6.6 Regulation and applicability without isolated examples 21
Chapter 7. Initial receipt and preservation 22
7.1 A clear receipt record 22
7.2 Packaging and sealing 22
7.3 Labels and relationships between objects 23
7.4 Receipt of files and messages 23
Chapter 8. Acquisition and technical documentation 24

8.1 Physical, logical, volatile, and documentary acquisition 24
8.2 Tools and validation 24
8.3 Reproducible exports and queries 25
8.4 Errors and incidents 25
Chapter 9. Custody, transfer, and preservation 26
9.1 The chain that answers questions 26
9.2 Electronic transfers 26
9.3 Storage and subsequent access 26
Chapter 10. Examination, analysis, and hypotheses 28
10.1 Questions before tools 28
10.2 Timeline and time zones 28
10.3 Interpreting call detail records and logs 29
10.4 Repeatability and reproducibility 29
Chapter 11. Reporting, presentation, and challenge 30
11.1 Report structure 30
11.2 Language for a nontechnical audience 30
11.3 Citations and legal sources 31
11.4 Review for challenge 31
Chapter 12. Common errors and continuous improvement 32
12.1 Errors that change cases 32
12.2 Lessons learned 33
12.3 Minimum guidance for the entire organization 33
Annex A. Functional legal matrix summary 34
A.1 How to read the comparison 34
A.2 Update method 35
Annex B. Scope and authority form 36
B.1 Format 36
Annex C. Receipt record 37
C.1 Minimum data 37
Annex D. Acquisition record 38
D.1 Record for each object 38
Annex E. Chain of custody and transfers 39
E.1 Record for each event 39
Annex F. Provider request and EML delivery 40
F.1 Request fields 40
F.2 Verification on receipt 40
Annex G. File inventory and manifest 41
G.1 Manifest columns 41
Annex H. Timeline and time zones 42
H.1 Correlation table 42
Annex I. Hypothesis and analysis matrix 43
I.1 Reasoning template 43

Annex J. Review of synthetic content 44
J.1 Minimum record 44
Annex K. Technical report template 45
K.1 Writing structure 45
Annex L. Checklists 46
L.1 Receipt and acquisition 46
L.2 Report and publication 46
Annex M. Regulatory and manual version control 47
M.1 Change log 47
M.2 Closing note 47

Chapter 1. Scope, questions, and authority

Decide what must be established before handling evidence.



Figure 1. Decide what must be established before handling evidence.

1.1 The question that governs all work

A useful assignment does not say “review everything.” It states what happened, what needs to be established, how the result will be used, and what deadline applies. The answers determine which sources are needed and what level of alteration can be justified. Recovering files for operational continuity is not the same as a forensic examination that must withstand challenge in court, even if both use the same tools.

Record the facts in plain language: who is making the claim, what they assert, what the other party denies, and what evidence exists according to initial statements. Separate what someone saw from what someone assumes. This distinction prevents an initial hypothesis from becoming an instruction to search only for information that confirms it.

Question	What must be documented	A decision that prevents improvisation
What does each party allege?	Separate accounts by person 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, proportionality, and confidentiality

The authorization must identify the holder, scope, permitted actions, systems, responsible persons, and communication channel. If access to third-party information, a shared account, or a provider is required, document the lawful means of obtaining it. A forensic expert does not grant themselves access merely because they know how to obtain it.

Proportionality asks whether the source and method are necessary for the objective. If an administrative export provides a better answer than a complete device review, choose the former. Confidentiality is not an add-on: from the moment of receipt, decide who may view, copy, transfer, and publish information, especially when third-party or victim data is involved.

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

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.

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.

- Source identifier and current custodian.
- Data type, period and expected format.
- Relationship to the fact to be established.
- Status: available, restricted, uncertain, or inaccessible.
- Risk of alteration, loss or exposure.
- Authorization pathway and next contact.

1.4 Complete example: a sales claim

A retail chain claims that it made sales for which it was not paid. The objective 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.

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 plan already avoids an invasive review of personal devices and requires comparison of independent sources.

1. The assignment and each party's account documented separately.
2. Authorization and exclusions identified.
3. Sources prioritized by question and volatility.
4. Third-party data and confidentiality measures defined.
5. Expected outcome and initial limitations documented.

Chapter 2. Integrity, originals, and context

Understand what can and cannot be asserted about the file.

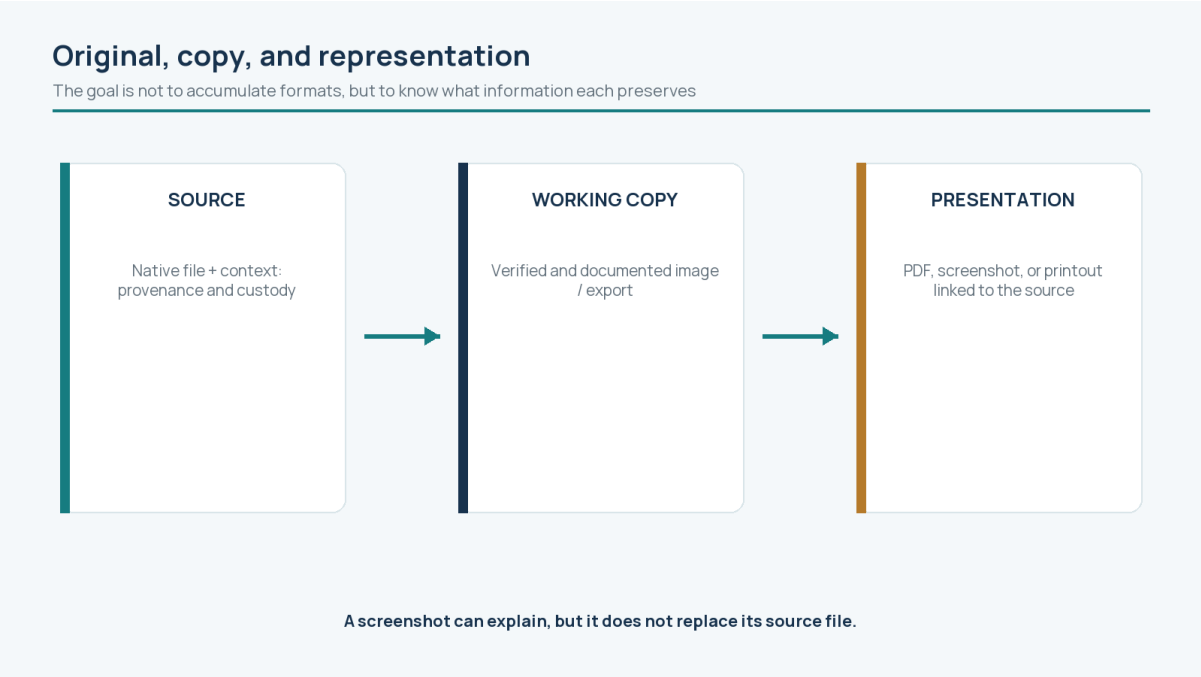


Figure 2. Understand what can and cannot be asserted about the file.

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 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.[1][2]

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.

[1] Mexico's Commercial Code, Articles 89–94 and 1205, official compilation. https://www.diputados.gob.mx/LeyesBiblio/pdf/CCom.pdf

[2] National Code of Civil and Family Procedure, Articles 348–350, compilation consulted with the amendment of 15-01-2026. https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPCF.pdf

The review must include the certificate, validity period, method, context, and possibility of key compromise, as well as independent corroboration.

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

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."

2.4 Accessibility and context preservation

An inaccessible object cannot be reviewed. Preservation requires the ability to open, read, interpret, and relate the 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.

NOM-151-SCFI-2016 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.[3]

[3] NOM-151-SCFI-2016, preservation and digitization of data messages. https://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017

Chapter 3. Roles and responsibilities

Know who decides, who executes, who documents, and who reviews.



Figure 3. Know who decides, who executes, who documents, and who reviews.

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.

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 on an incomplete telephone description.

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 Operational communication

Before acting, establish who can answer technical, legal, and custody questions. The contact directory includes name, role, channel, availability, and backup contact. Urgent decisions are recorded with a date and justification; an informal call must not be the only record of an irreversible action.

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.

3.3 Independence and review

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.

Ego is controlled by documenting hypotheses and adverse results. A review that merely seeks to confirm what the analyst has already written is not independent. The report must enable others to understand what was found, what was ruled out, and what remains open, even when the answer does not favor the client.

Chapter 4. Lifecycle and forensic readiness

Prevent losses before an incident occurs.

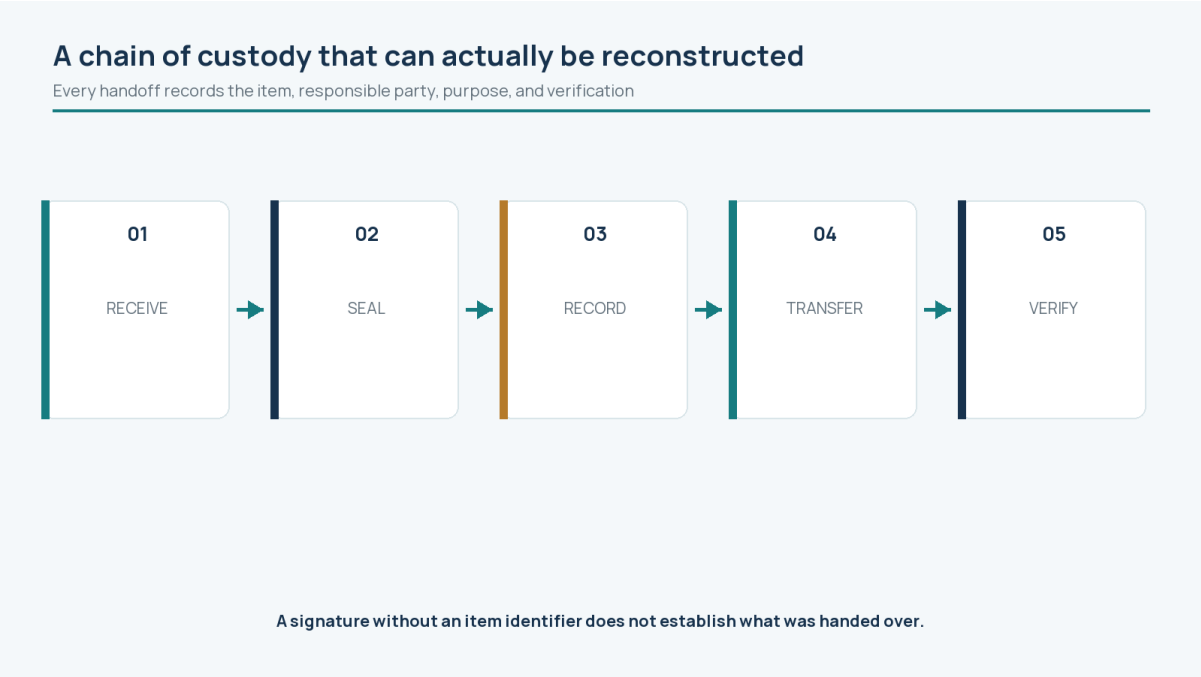


Figure 4. Prevent losses before an incident occurs.

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.

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.

- Up-to-date inventory of assets and owners.
- Log sources, formats, and retention periods.
- Technical, legal, and provider contacts, with alternates.
- Documented time zone and synchronization.
- Available acquisition, sealing, and transfer procedure.
- Periodic exercises with fictitious 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.

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.

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

4.3 Documented lifecycle

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.

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 manual translates them into understandable actions and forms that make the work demonstrable.[4][5]

[4]ISO/IEC 27037:2012. Guidelines for the identification, collection, acquisition, and preservation of digital evidence. https://www.iso.org/standard/44381.html

[5]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. https://csrc.nist.gov/pubs/sp/800/86/final

Chapter 5. Decision trees by scenario

Choose a path based on condition, objective, and risk, not habit.

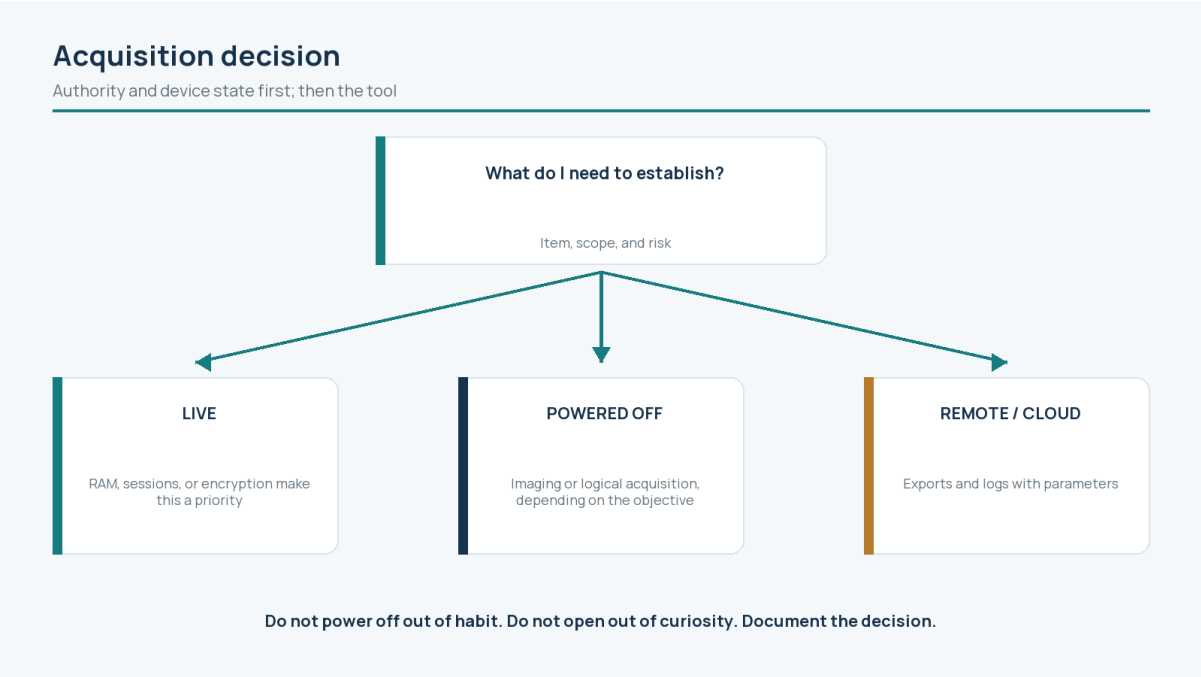


Figure 5. Choose a path based on condition, objective, and risk, not habit.

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 the available capabilities.

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.

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.

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.

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.

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.

5.4 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.

The stop record includes the reason, the condition in which the object was left, prior actions, identified risks, and the next person responsible. It should not be presented as a failure: it is a measure to preserve the possibility of analysis and avoid indefensible action.

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.

Chapter 6. Modern sources and call detail records

Work with cloud services, email, providers, logs, and synthetic content in context.

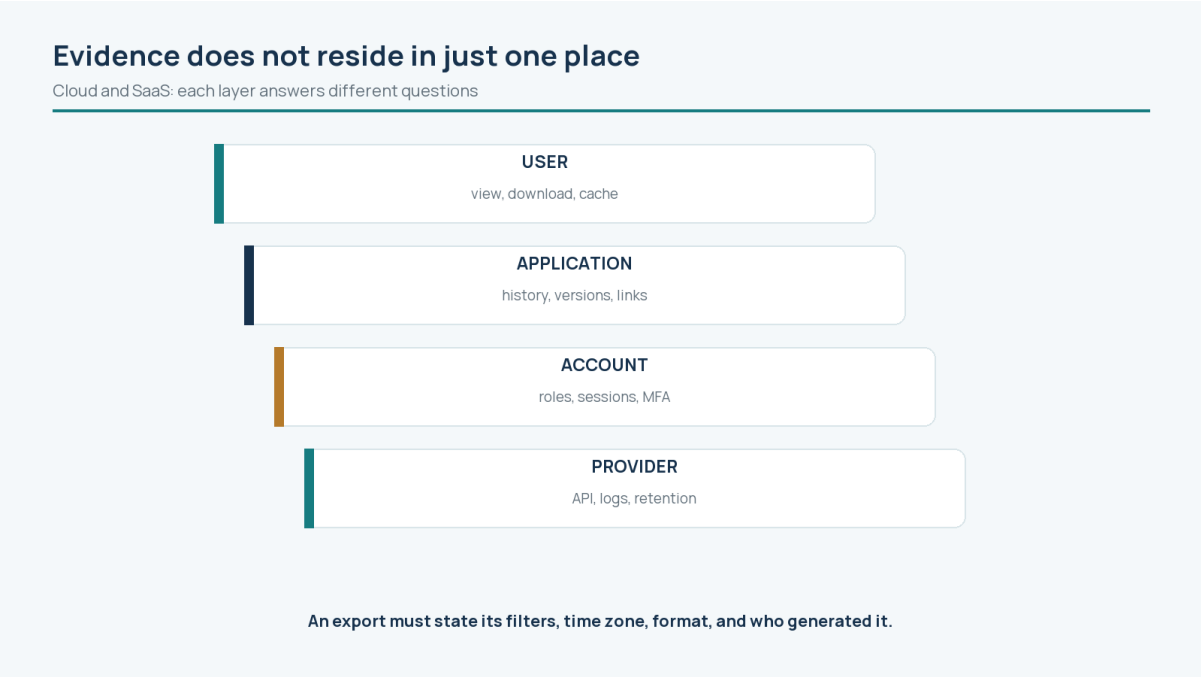


Figure 6. Work with cloud services, email, providers, logs, and synthetic content in context.

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.

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.

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.

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.

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.

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.[6]

Request element	What to request from the provider	What to check 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.

[6]Mexico. General provisions applicable to credit institutions, Articles 316 Bis and related provisions. https://www.cnbv.gob.mx/Prensa/Presentaciones%20Seminario%20Corresponsales/i.%20Circular%20%C3%9Anica%20de%20Bancos.pdf

```
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.

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.[7]

6.6 Regulation and applicability without isolated examples

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.

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 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.[8][9][10]

[7] Regulation (EU) 2024/1689 on artificial intelligence, Article 50, consolidated text as of 27-07-2026. https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/spa/pdf

[8] Federal Criminal Code, Articles 199 Octies and 199 Nonies, compilation including the amendment of 13-03-2026. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

[9] Congress of San Luis Potosí. Approval of the reform on the misuse of AI, 14-11-2025. https://congresosanluis.gob.mx/content/aprobada-reforma-para-sancionar-uso-indebido-de-inteligencia-artificial

[10] Parliamentary Gazette of San Luis Potosí. Repeal of Article 187 Ter and the chapter containing Articles 272 Bis and 272 Ter, published on 30-07-2026. http://congresosanluis.gob.mx/sites/default/files/unpload/tl/gpar/2026/07/%C3%9ANICO.pdf

Chapter 7. Initial receipt and preservation

Record the object and its condition before any analysis.



Figure 7. Record the object and its condition before any analysis.

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.

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.

- Unique case and object identifier.
- Date, time, time zone, location, delivery, and receipt.
- Physical description, serial number, capacity, and accessories.
- Power, lock, and network status, and visible damage.
- General photographs and photographs of identifiers.
- Known previous actions and immediate risks.

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.

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.

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.

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 physical label and receipt record must match the digital inventory and final report.

```
Fictitious example:
ED-20261109-DEMO-MBL-003-A00

ED = digital evidence
20261109 = receipt
DEMO = fictitious case
MBL = mobile source
003 = third object
A00 = initial acquisition
```

7.4 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.

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.

Chapter 8. Acquisition and technical documentation

Obtain data methodically, with validation and traceability.

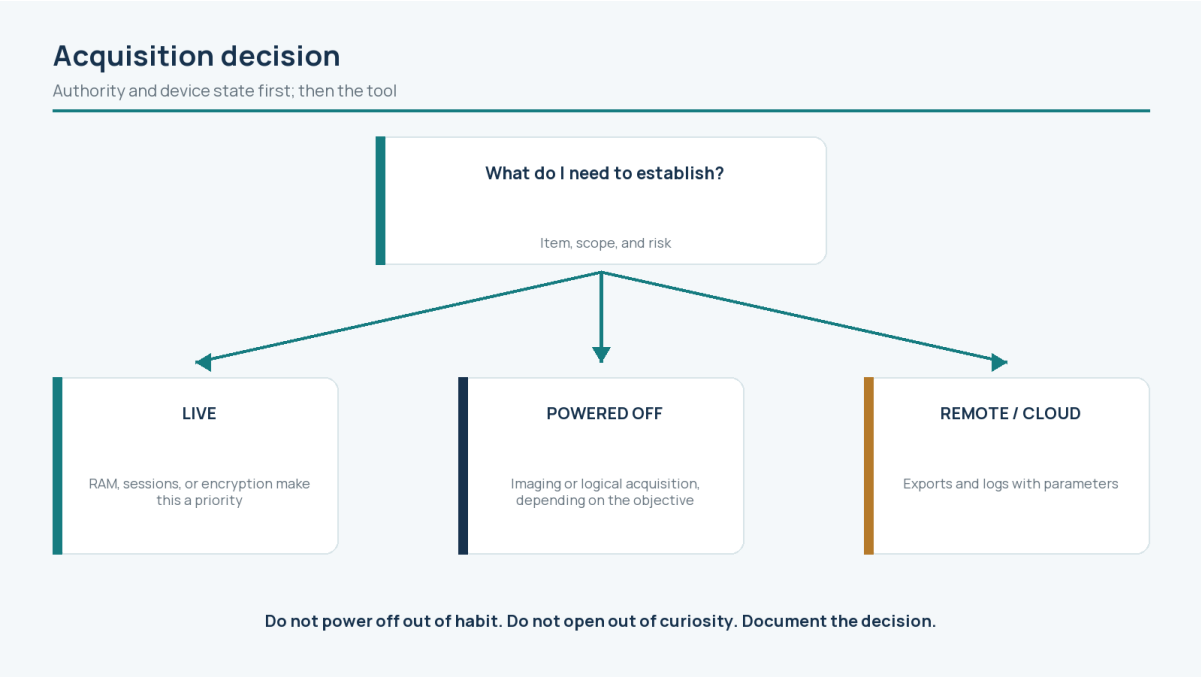


Figure 8. Obtain data methodically, with validation and traceability.

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.

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.

8.2 Tools and validation

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.

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. If a tool produces an error, preserve the message and assess its effect rather than concealing it.

Acquisition field	Fictitious example	What it establishes
Source	DEMO-SSD-003 disk	Exact object and custodian.

Acquisition field	Fictitious example	What it establishes
Method	Bit-for-bit image of a controlled copy	Type of coverage.
Tool	Name and version validated in the laboratory	Conditions of execution.
Date and time zone	2026-11-09T14:32:07-06:00	Temporal sequence.
Integrity	SHA-256 of the acquired object	Object to which the value corresponds.
Incidents	Documented unreadable sector	Scope and limitations of the result.

8.3 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.

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.

8.4 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.

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.

Chapter 9. Custody, transfer, and preservation

Maintain the relationship among the object, responsible person, location, and verification.

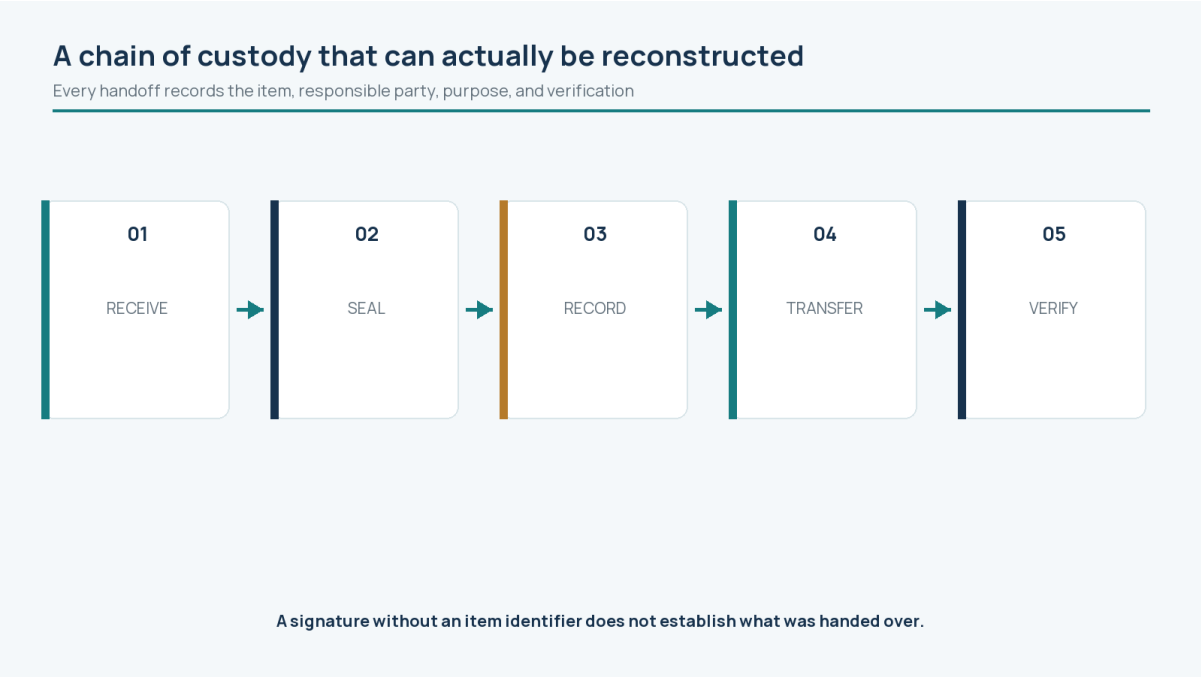


Figure 9. Maintain the relationship among the object, responsible person, location, and verification.

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.

The chain also records legitimate access without physical transfer: opening the container, making a working copy, temporary loan, change of location, or remote download. Documenting only the final delivery leaves gaps that prevent the history from being reconstructed.

9.2 Electronic transfers

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.

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.

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.

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.

Chapter 10. Examination, analysis, and hypotheses

Turn artifacts into explanations without leaps of faith.

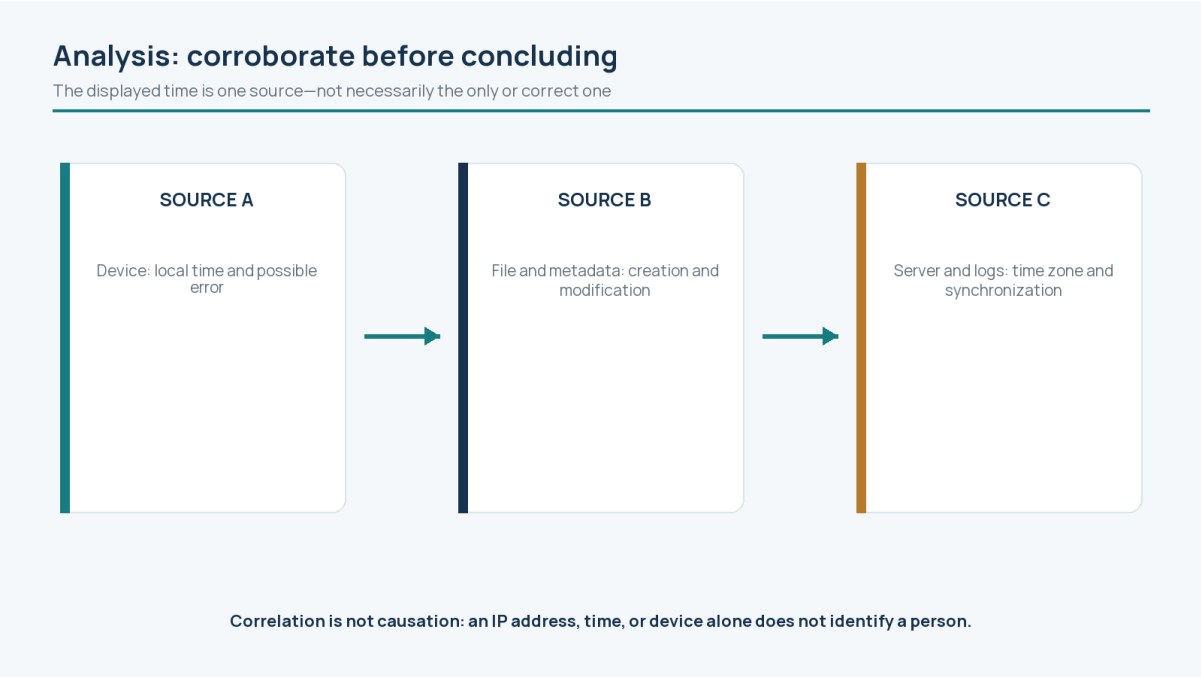


Figure 10. Turn artifacts into explanations without leaps of faith.

10.1 Questions before tools

Analysis begins with assertions that can be corroborated or weakened. Each is linked to sources and tests. The objective is not to find a match and stop, but also to seek alternative explanations and results that may contradict the initial account.

A hypothesis matrix records the assertion, source, method, finding, alternative, and limitation. This practice reduces the risk of selecting artifacts by intuition and makes it possible to explain why a conclusion changed. The absence of evidence in a source can be important, but must be interpreted within its coverage.

Assertion	Source and test	Alternative	Limited result
The video is a single continuous recording.	Names, dates, chapters, and continuity.	Selection or subsequent conversion.	The sequence does not support continuity within the scope reviewed.
The operation was carried out from the account holder’s device.	Access, device, and session logs.	Credentials used by someone else.	Use of the credentials is established, not physical identity.
No exfiltration occurred.	Network and transfer logs.	Incomplete coverage or an encrypted channel.	Not observed in the sources reviewed.

10.2 Timeline and time zones

A timeline records the date, time zone, temporal source, and precision. The device clock may be misconfigured; a file timestamp may indicate creation, modification, or download; a server may use another time zone. Preserve the original value and its conversion without treating them as the same event.

A filename sequence can help assess chapters and continuity, as with certain cameras, but does not by itself prove that a video is complete. Compare the naming convention, dates, structure, content, and provenance. A missing chapter raises a question; it does not automatically establish malicious editing.

10.3 Interpreting call detail records and logs

For call detail records, review event type, start, duration, direction, participants, cells, and blank fields. An incoming call is not the same as an outgoing call, and the cell can change during the event. Technical identifiers do not automatically correspond to individuals. Interpretation compares the period and context, not merely number matches.

A cell's location does not prove a person's exact location. It requires documentation of coverage, technology, timing, and other sources. If a route is asserted, present levels of precision and alternatives. The analysis must not use an attractive map to create certainty that the evidence does not support.

10.4 Repeatability and reproducibility

Repeatability seeks the same result in the same environment; reproducibility seeks it in another documented environment. ISO/IEC 27037 distinguishes between these properties. The report identifies conditions that may change: tool, version, system, filters, or source. Agreement between tools does not eliminate a common underlying assumption.

The analysis records positive, negative, and inconclusive results. Do not promise to repeat results that depend on a provider or volatile source. Preserve relevant queries and outputs so that others can check the reasoning and identify errors.[4]

Chapter 11. Reporting, presentation, and challenge

Explain the work clearly without overstating certainty.

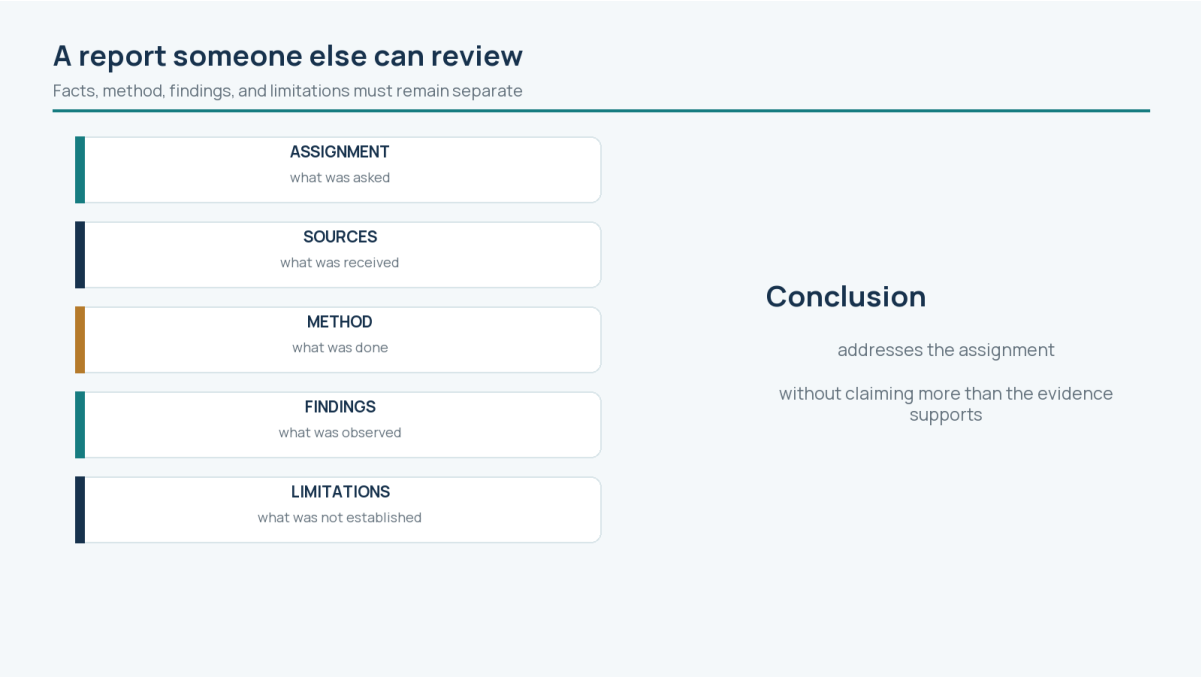


Figure 11. Explain the work clearly without overstating certainty.

11.1 Report structure

The report begins with the assignment and scope, identifies sources and objects, explains the method, presents findings, analyzes alternatives, concludes within scope, and declares limitations. Annexes contain receipt records, manifests, hashes, logs, and figures. The conclusion answers the questions without introducing new accusations or unsolicited legal advice.

The writing distinguishes observed facts, tool results, inferences, and legal assessment. The reader must know the basis for each statement. A figure summarizes a sequence or contradiction; it is not used to make the report appear more technical than it is.

- Assignment, scope, and exclusions.
- Objects, provenance, and custody.
- Tools, versions and parameters.
- Findings with verifiable locations.
- Alternative hypotheses and negative results.
- Conclusion, limitations, and complete annexes.

11.2 Language for a nontechnical audience

A technical explanation can be precise without being inaccessible. Instead of “forensic acquisition of evidence was carried out,” write “a controlled copy of the disk was created and its integrity was documented.” Define necessary terms once and use them consistently. Acronyms are no substitute for an explanation.

The executive presentation summarizes what was reviewed, what was found, and what decision can be made. Technical detail remains available without requiring executives to interpret it. Police officers and lawyers must be able to follow the sequence without knowing commands; the specialist must be able to repeat it using the annexes.

11.3 Citations and legal sources

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. When a rule has been repealed, explain it as historical background, not as law in force.

The review verifies that the technical assertion and citation address the same issue. A rule on documentary evidence does not establish authorship in every case; a preservation rule does not establish truthfulness; an incident rule does not prove a specific transfer. Do not use a source to decorate a conclusion already reached.

11.4 Review for challenge

Before delivery, ask whether another person can locate the object, repeat the query, understand the inferential step, and find the limitations. Difficult questions are answered with the case file, not personal authority. If something is not documented, acknowledge it and correct the scope.

The review covers headings, text, annexes, images, and metadata in the delivery file. Do not claim visual validation without opening the final output. Calculate the delivered file’s SHA-256 hash and retain a manifest so that source and destination can be compared without confusing this with proof of the content.

Chapter 12. Common errors and continuous improvement

Avoid known flaws and update without fabricating certainty.

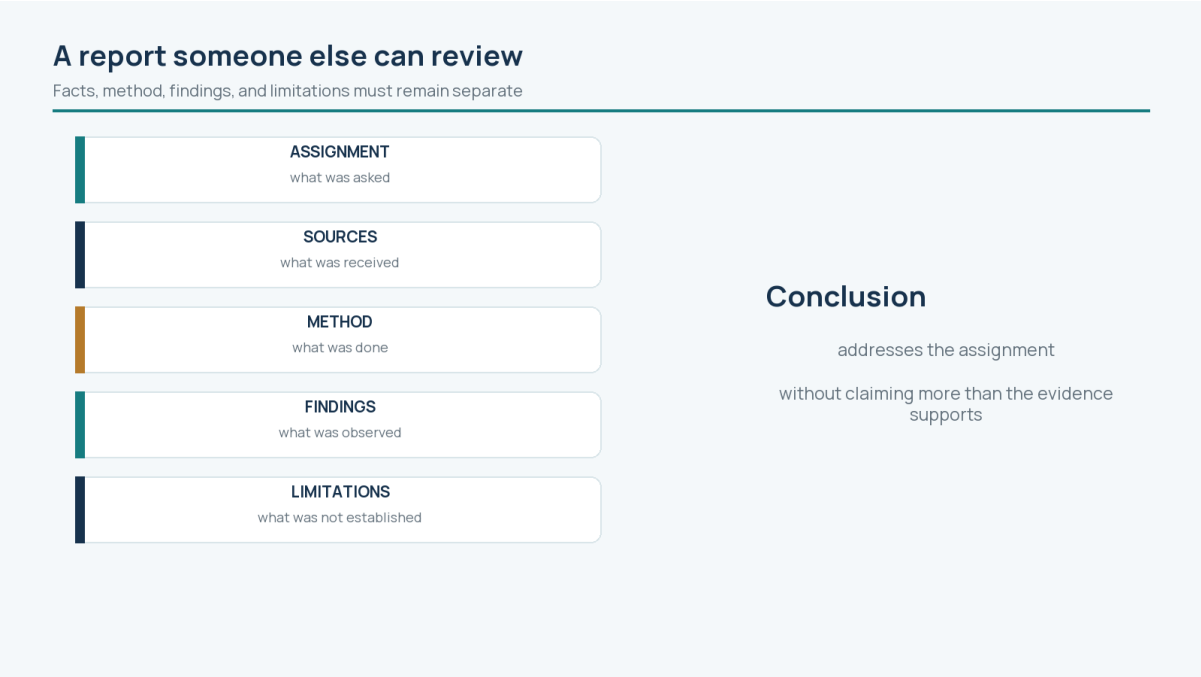


Figure 12. Avoid known failures and update without fabricating certainty.

12.1 Errors that change cases

The most costly errors are often simple: opening devices out of curiosity, powering down by habit, capturing without a URL, exporting without a time zone, confusing an original with a printout, attributing an IP address to a person, presenting a hash as complete proof, and citing a repealed rule. Prevention begins with clear procedures and trained first responders.

When an error has already occurred, document it without inventing a perfect chain. Assess what changed, what can still be verified, and which conclusions must be limited. Rewriting earlier records to conceal it destroys trust and can harm the case file more than the original error.

Error	Consequence	Correct response
Powering down as a universal rule	Loss of memory or sessions.	Assess the state before deciding.
Treating antistatic packaging as Faraday isolation	A false sense of isolation.	Use and verify genuine isolation.
Copy hash into a separate note	The link to the delivery is lost.	Preserve the EML, body, and attachments.
Relying on an AI detector	A false conclusion about origin or falsity.	Corroborate with source, method and context.
Citing an outdated reform	Asserting a nonexistent rule.	Check whether rules are in force and whether they have been repealed.

12.2 Lessons learned

A subsequent review identifies failures in sources, decisions, tools, communication, and presentation. Improvements are assigned to responsible persons and verified through exercises. Do not fabricate evidence of prior compliance: record when the new practice took effect.

A new version of the manual retains the history and reason for the change. If a platform changes its export, update Chapter 6 or 8; if a law changes, update Annex A and Register M. Contradictory notes must not be allowed to accumulate without reviewing the main text.

12.3 Minimum guidance for the entire organization

The organization must be able to answer five questions without relying on one person: who authorizes, where the evidence is, how it was obtained, who has handled it, and what can be asserted. If any question has no answer, the plan states how to recover it or how to limit the conclusion.

The manual is a starting point, not an immutable text. Practice is adapted to the case, documented, and reviewed. The goal is for any team to work methodically, share knowledge, and support an explanation, even when the outcome is not the expected one.

Annex A. Functional legal matrix summary

Locate the function without inventing equivalences between countries.

A.1 How to read the comparison

Comparable means functional equivalence, not identical content, presumptions, subjects, time limits, or procedural effects. The complete matrix is supplied as a separate file so that it can be updated without rebuilding the manual. Before applying a rule, verify the instrument, article, personal scope, channel, subject matter, and version at the time of the event.

The table summarizes starting points, not an exhaustive catalog. If research has not substantiated a function, mark it accordingly and do not fill the gap by analogy. Civil, criminal, administrative, archival, and financial rules are not interchangeable.[121112131415166]

Jurisdiction	Functional starting point	Key warning
Mexico	CCom 89–94 and 1205; CNPCF 348–350; NOM-151; CNBV 316 Bis and related provisions.	Gradual transition; each CNBV article has a different purpose and time limit.
Peru	Law 27269 and its Regulation; CPC 188–197; archival regime; SBS 504-2021 and 2286-2024.	The regime is distributed across instruments; do not attribute everything to Law 27269.
Chile	Law 19.799; RAN 20-7, 20-8 and 20-10.	Advanced signature and date are separate issues.
Argentina	Law 25.506; CCyC 318–319; BCRA A 7783 and A 8280.	Presumptions apply only within their regime; check for repeals.
Colombia	Law 527; CPACA; applicable SFC instructions.	Preserve origin, destination, date, and time; confirm SFC provision numbers.
Ecuador	Law 67; Resolution JPRM-2025-006-M for payments.	The payment system does not replicate the entire CNBV regime.

[11] Peru. Law 27269 and the Regulation on Digital Signatures and Certificates. https://www.gob.pe/institucion/indecopi/normas-legales/5570542-ley-27269

[12] Chile. Law 19.799 on electronic documents and electronic signatures. https://www.bcn.cl/leychile/navegar?idNorma=196640

[13] Argentina. Digital Signature Law 25.506. https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

[14] Colombia. Law 527 of 1999 on data messages and electronic commerce. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

[15] Ecuador. Law on Electronic Commerce, Electronic Signatures, and Data Messages. https://ventas.icert.fje.gob.ec/documents/10181/11670/leyComercioElectronico.pdf/e0a3116a-acd9-42ce-97ac-4d28b32a2f2e

[16] Spain. Civil Procedure Law, Articles 326 and 384, consolidated text. https://www.boe.es/buscar/act.php?id=BOE-A-2000-323

Jurisdiction	Functional starting point	Key warning
Spain / EU	eIDAS; LEC 326 and 384; RD-ley 19/2018, 45, 66, and 67.	Simple, advanced, and qualified signatures do not have identical effects.

A.2 Update method

The update records the official source, consultation date, article read, and operational change. Do not replace a rule with a news item or a bill with a decree. The complete matrix retains citations for recognition, writing, attribution, integrity, originals, accessibility, preservation, admissibility, burden of proof, and financial regulation.

ISO/IEC 27037 and NIST SP 800-86 are cited as methodologies, not national legislation. The annex is intended to guide what to preserve, request, verify, and limit, not to resolve a case using a table of similar phrases.[45]

Annex B. Scope and authority form

Initial form for defining the work.

B.1 Format

Complete it before acting. If information is unavailable, record the reason and the person who must confirm it. Do not leave critical blanks to be completed after acquisition.

Field	Content to be recorded	Fictitious example
Identifier	Unique assignment code.	EXP-DEMO-2026-001
Question	Fact to be established.	Determine whether the sales were transmitted and settled.
Period	Start, end and time zone.	1–3 Nov 2026, UTC−06:00.
Sources included	Authorized systems, files, and custodians.	Remittance, processor and bank reports.
Exclusions	Data or devices outside the authorization.	Unrelated personal devices.
Authorization	Holder, actions, and channel.	Authorized address; registered secure channel.
Deliverable	Type of report and annexes.	Technical report, manifest, and receipt records.
Risks	Alteration, loss and confidentiality.	Log rotation and third-party data.

Annex C. Receipt record

Document the condition before any analysis.

C.1 Minimum data

The receipt record is accompanied by general photographs and photographs of identifiers. Prior actions are recorded even if they were incorrect; do not rewrite them retrospectively to create the appearance of an ideal receipt.

Field	Required content
Object and identifier	Type, make, model, serial number, capacity, and assigned code.
Delivery and receipt	Name, role, date, time, time zone, and location.
Condition	Power state, lock status, network status, damage, and accessories.
Seal and packaging	Type, identifier, condition, and photographs.
Prior actions	Opening events, connections, copies, changes, or unknowns.
Risks	Volatility, remote wiping, third-party data, and priority.
Initial decision	Preserve, escalate, acquire, or request clarification, and identify the responsible person.

Annex D. Acquisition record

Link the source, method, output, and verification.

D.1 Record for each object

Each acquisition has its own record. If repeated, assign a new related identifier and explain why without deleting the first attempt.

Field	Required content
Source and custodian	Exact identifier and person who retains it.
Method and justification	Physical, logical, volatile, remote, or documentary, and the reason.
Tool	Name, version, environment and validation.
Parameters	Filters, fields, date, time zone, and configuration.
Output	Name, path, format, size, and original/copy relationship.
Integrity	Algorithm, value, date and object covered.
Incidents	Errors, omissions, sectors, access, and effect on scope.
Verification	Opening, comparison, repetition, and reviewer.

Annex E. Chain of custody and transfers

Reconstruct every access and movement.

E.1 Record for each event

Record container opening, remote downloads, and working copies as well. A transfer is not complete until receipt and the object's condition have been confirmed.

Date and time zone	Object	Delivery	Receipt	Purpose	Seal/integrity
09 Nov 14:32 −06	ED-DEMO-003	Custodian A	Analyst B	Acquisition	Seal 01 intact
09 Nov 16:05 −06	ED-DEMO-003-A00	Analyst B	Custodian C	Safekeeping	Matching hash
10 Nov 09:10 −06	ED-DEMO-003-A01	Custodian C	Reviewer D	Review	Access logged

Annex F. Provider request and EML delivery

Ensure format, context and integrity in remote records.

F.1 Request fields

Adapt the request to the provider and authorized channel. Do not write passwords or credentials in the record or email body. Identify the secure channel by reference, without including secrets.

Element	Content to be included
Case file and authorization	Code, holder, and reference to the secure channel.
Account and scope	Authorized identifiers, period, time zone, and exclusions.
Format	Available native format and reference copy, data dictionary, and extraction process.
Integrity	Algorithm and hash for each file in the response body.
Delivery	EML with body, headers, and attachments; link and permissions where applicable.
Limitations	Retention, missing fields, coverage, errors and clarifications.

F.2 Verification on receipt

Save the EML before working with attachments. Calculate hashes for the EML and files separately and compare them with the values in the body. Record discrepancies and request clarification. If the provider omits a hash, record its absence and calculate a local hash without attributing it to the provider.

6. Complete EML preserved and readable.
7. Native files received and related to the body.
8. Algorithm and values compared and recorded.
9. Fields, units, time zone, and extraction process understood.
10. Documented limitations and discrepancies.

Annex G. File inventory and manifest

Maintain the relationship among sources, derivatives, and deliverables.

G.1 Manifest columns

The manifest records the identifier, name, path, object type, origin, method, size, format, hash, and observations. It must not disclose sensitive data or secrets. The path may be abbreviated in the public version if it reveals protected information.

Identifier	Relationship	File	Format	Integrity
ED-DEMO-003	Original received	sabanas.csv	CSV	SHA-256 calculated on receipt
ED-DEMO-003-A00	Related delivery	entrega.eml	EML	Object independent of the CSV
ED-DEMO-003-A01	Working copy	sabanas_trabajo.csv	CSV	Different hash if the structure changes
ED-DEMO-003-R01	Presentation	informe.pdf	PDF	Hash of the delivered file

Annex H. Timeline and time zones

Avoid hidden conversions and false matches.

H.1 Correlation table

Preserve the original value from each source and add the conversion without replacing it. If the device clock is unreliable, record the known offset or uncertainty.

Event	Time source	Original value	Time zone	Conversion and limitation
Video capture	Device clock	06:04:16	Unknown	Do not assume UTC; compare with another source.
Export	Server	2026-11-01T12:04:16Z	UTC	06:04:16 in UTC−06; record daylight saving time.
EML receipt	Email client	09 Nov 07:05	UTC−06	Time of receipt, not of the event under investigation.

Annex I. Hypothesis and analysis matrix

Document confirmation, alternatives, and limitations.

I.1 Reasoning template

Test each assertion against sources capable of corroborating or weakening it. The reviewer adds alternatives the analyst had not considered, and any resulting change in the conclusion is recorded.

Assertion	Source/test	Alternative	Result
The file is an original.	Provenance, metadata, and custody.	Prior export or editing.	Only the received representation is supported.
The user authorized the operation.	Authentication, device and session.	Compromised credentials.	Use of credentials does not establish physical identity.
There are no other files.	Documented query and coverage.	Filter, retention, or format.	None were observed within the scope queried.

Annex J. Review of synthetic content

Distinguish generation, editing, conversion, and publication.

J.1 Minimum record

The goal is not to declare something a “deepfake” based on appearance. Record every known transformation, its evidence, and its limitations. Identify the detector’s version and known error characteristics when available; do not use it as the sole evidence.

11. Original file received and provenance.
12. Available tool, version, and generation/editing history.
13. Codec, compression, metadata, and versions compared.
14. URL, publication, tag, audience and context.
15. Consent, identity, purpose, and applicable law in force reviewed.
16. Detectors and corroboration with explicit limitations.

Annex K. Technical report template

Present findings without conflating facts and inferences.

K.1 Writing structure

The final report includes a cover, assignment identification, table of contents, executive summary, scope, sources, method, findings, analysis, conclusion, limitations, and annexes. Every assertion identifies the location of the supporting evidence and uses wording commensurate with its strength.

Section	Content to be addressed
Assignment	What was requested, for what purpose, and with which exclusions.
Sources	What was received, from whom, and in which representation.
Method	What was done, with what tool and parameters.
Findings	What was observed and where it can be located.
Analysis	Which explanations are supported or weakened.
Conclusion	What can be asserted within the scope.
Limitations	What was not established and which sources are missing.
Annexes	Receipt records, manifest, hashes, logs, and figures.

Annex L. Checklists

Check the work before each delivery.

L.1 Receipt and acquisition

Check the list using evidence, not intention. If an item does not apply, record the reason and its approval. Do not leave a critical criterion unanswered.

17. Authority, scope and exclusions documented.
18. Object, condition, photographs, and responsible persons identified.
19. Method justified by source and risk.
20. Tool, version and parameters recorded.
21. Hashes, EML and related files preserved.
22. Incidents and limitations included in the case file.

L.2 Report and publication

The final review is performed on the opened file, not the working draft. Review images at full size and as thumbnails when they will be published.

23. Conclusion consistent with sources and scope.
24. Current citations, articles, and functions verified.
25. No customer names, credentials or unnecessary data.
26. Table of contents, figures, tables, and annexes are legible.
27. Final files opened and visually reviewed.
28. Matching source and destination SHA-256 hashes, with the manifest preserved.

Annex M. Regulatory and manual version control

Update without accumulating contradictions.

M.1 Change log

Each regulatory or methodological change records the source, date, affected chapter, editorial decision, and reviewer. If a rule is repealed, revise the main text and frequently asked questions, not merely add a note at the end.

Date	Source	Change	Editorial action	Review
30 July 2026	SLP Official Gazette	187 Ter, 272 Bis and 272 Ter repealed.	Explain as historical background; update posts and Annex A.	Complete
27 July 2026	EUR-Lex	Consolidated text of the AI Regulation reviewed.	Cite Article 50 with the correct scope and exceptions.	Complete
09 Nov 2026	Manual	Language and format review.	Incorporate EML, call detail records, and checklists for first response.	Complete

M.2 Closing note

This manual is a general guide. It does not constitute legal advice or an expert opinion on a specific case. Application requires analysis of authority, jurisdiction, facts, channel, and the law in force. This edition is supplied with resources and a separate matrix so that updates can be reviewed without losing the volume's design.