ACCCF / Applied Knowledge Library

03

VOLUME

Containment with sound judgment and verified recovery

Spanish edition · 2026

Ransomware response manual: containment, evidence and business continuity

First minutes, preservation, eradication, recovery, and lessons learned

Respond quickly without destroying the information needed to understand the incident, protect people, and resume operations with verifiable controls.

For leadership, security, IT, business continuity, legal, insurance, first responders, and forensic specialists. Instructions are limited to defensive administration and preservation; they do not cover malware execution or negotiations with attackers.

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

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

Contents

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

Introduction: a crisis does not negate methodology 3
Chapter 1. The first fifteen minutes 3
1.1 Open the case file before opening files 3
1.2 Power off, disconnect, or keep running 4
Chapter 2. Scope, spread, and priorities 5
2.1 The visible device is not the entire incident 5
2.2 Prioritize services, not noise 5
Chapter 3. Preservation during containment 6
3.1 Memory, disk, logs, and system state 6
3.2 Logs before account suspension or reinstallation 6
3.3 Evidence of the ransom note and contact channel 6
Chapter 4. Investigation: origin, persistence, and exfiltration 7
4.1 A timeline that shows uncertainty 7
4.2 Entry and persistence hypotheses 7
4.3 Exfiltration: absence of evidence and evidence of absence 8
Chapter 5. Eradication and the ransom decision 8
5.1 Eradicate the cause, not just the symptom 8
5.2 To pay or not to pay: a documented decision, not an impulse 8
5.3 Communication and obligations 9
Chapter 6. Recovery and continuity 9
6.1 Select and validate the recovery point 9
6.2 Phased recovery 10
6.3 Reconciling information and lessons learned 10
Appendix A. Legal framework and sector-specific records 11
Appendix B. Response templates 12
B.1 Incident timeline 12
B.2 Containment decision matrix 13
B.3 Acquisition log 13
B.4 Recovery exit criteria 13
Appendix C. Exercise and checklist 13
C.1 Tabletop exercise with fictitious data 13
C.2 Short pre-closure checklist 14

Introduction: a crisis does not negate methodology

When files stop opening and a screen demands a ransom, the first reaction is often to power everything down, delete whatever appears infected, and restore any available backup. These actions may reduce damage in one context and destroy evidence in another. They can also return unreviewed persistence mechanisms to production. The task is not to choose between speed and evidence: it is to preserve what is needed while limiting damage, with one person accountable for each decision.

This manual follows two parallel tracks from the outset. The first protects people, services, and continuity. The second preserves sources, decisions, and evidence. The second must not paralyze urgent security action, and the first must not erase the ability to understand what happened without a record. Every action must answer: who authorized it, on the basis of what information, what changed, and what risk it introduced?

NIST SP 800-61 Rev. 3 organizes response into preparation, detection, response, recovery, and continuous improvement. NIST SP 800-86 links collection, examination, analysis, and reporting. Response becomes more than a list of buttons when the scope, tools, results, and limitations are documented. An encrypted file demonstrates encryption; on its own, it does not establish when access began, whether exfiltration occurred, or who was responsible.[1][2]

> **Guiding principle**
> Protect people first. Then contain the incident with as little damage as reasonably possible, preserve anything that could disappear, and do not claim you are clean simply because the system has restarted.

Chapter 1. The first fifteen minutes

1.1 Open the case file before opening files

The first person to detect the problem records the date, time, time zone, what they saw, the device involved, who reported it, and any actions already taken. They do not need to diagnose it. They should avoid opening the ransom note with unknown programs, running attachments, or following links to “check whether it is real.” Photograph or record the message without interacting with it, and preserve the original object whenever possible.

Designate an incident coordinator and a communication channel outside potentially compromised systems. The contact list includes the technical lead, business continuity, legal, privacy, communications, insurance, and vendor contacts. If corporate email may be affected, do not use it to share indicators, credentials, or sensitive reports. Record verbal decisions with the time and the person responsible.

Initial question	Minimum record	Why it changes the next decision
Are there critical people or services at risk?	Service, dependency, and immediate consequence.	Containment prioritizes life and safety over evidence.
What exactly was observed?	Message, extension, behavior, asset, and time.	Distinguishes an alarm from a hypothesis.

[1] NIST SP 800-61 Rev. 3 (April 2025). Incident response recommendations integrated into CSF 2.0: preparation, detection, response, recovery, and improvement. It supersedes Revision 2. Official online source

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

Initial question	Minimum record	Why it changes the next decision
Is it still spreading?	Devices, segments, resources, and observed activity.	Determines isolation and urgency.
What can disappear?	Memory, sessions, logs, links, and backups.	Prioritizes preservation before changes.
Who decides and communicates?	Coordinator, authority, channel, and deputy.	Prevents contradictory actions and rumors.

1.2 Power off, disconnect, or keep running

There is no universal answer. Powering down can stop processes while also destroying memory, sessions, and keys needed for analysis or recovery. Disconnecting from the network can limit spread and exfiltration without destroying volatile data, but it can also trigger behavior anticipated by the attacker or interrupt a critical service. Keeping the system running allows live observation and acquisition, but can continue to alter data and increase the damage.

The decision is based on system state, spread, service criticality, encryption, volatile data, available tools, and authority. If live acquisition is possible, evaluate it before powering down. If it is not, document that limitation and choose the least destructive containment option compatible with security. A first responder should not improvise forensic memory acquisition without training; they can photograph the system state, isolate it according to procedure, and escalate.

> **Exceptional decision**
> If a life or essential service depends on the system, evidence preservation must not be used as an argument to delay protection. Record the need, the alternatives considered, and any evidence that could be preserved before and afterward.



Figure 1. Containment means choosing what to protect first. There is no universal order for powering down or disconnecting. Editorial reconstruction; not actual evidence.

Chapter 2. Scope, spread, and priorities

2.1 The visible device is not the entire incident

An endpoint with encrypted files may be the last link in a chain that began weeks earlier in another account. The map includes identities, VPNs, email, servers, hypervisors, backups, vendors, personal devices authorized for work, management systems, and cloud services. Expand scope based on evidence, not on the phrase “everything is compromised,” which can cause unnecessary outages and obscure priorities.

Build an asset matrix with criticality, owner, status, possible compromise, dependencies, log sources, and decisions. One device may be infected, another simply inaccessible because a switch was isolated, and another healthy but dependent on a stopped server. The report distinguishes these states so they are not all presented as a single confirmed infection.

Status	Evidence required	Documented decision
Confirmed	Artifact, execution, log, or verifiable encryption on the asset.	Contain and preserve according to priority.
Suspected	Related indicator, not sufficiently confirmed.	Monitor, selectively isolate or acquire.
Affected by a dependency	Service stopped by another action or system.	Restore the dependency without labeling the device as infected.
No indicators within scope	Query, filters, time period, and sources reviewed.	Do not declare it clean outside that coverage.
Unknown	Missing access, logs, or inventory.	Assign a responsible person and define the limits of the conclusion.

2.2 Prioritize services, not noise

The continuity matrix identifies essential processes, maximum tolerable downtime, minimum data required to operate, dependencies, responsible parties, and temporary manual workarounds. A server generating many alerts may be less of a priority than a directory service on which everyone depends. Decide what to restore first based on actual impact, not on which file appeared first in the ransom note.

The response and continuity teams work with the same timeline but have different deliverables. Security needs to know what persistence mechanisms are present; continuity needs to know which version is recoverable and what dependencies it has. Reconciliation prevents restoration of a system that will reconnect to the source of the incident or a healthy service being left offline because no one knows why.

> **Fictitious scenario**
> A company detects encryption on its document server. Payroll data is not encrypted, but payroll is unavailable because it depends on the same directory. The team does not label payroll as infected: it records a dependency-related impact. Recovery prioritizes identity and logs before reconnecting services.

Chapter 3. Preservation during containment

3.1 Memory, disk, logs, and system state

Preservation is prioritized by volatility and the ability to answer questions. Memory may contain processes, connections, keys, or session fragments; disk retains files and artifacts; logs explain events; configuration shows how the system was connected. Not every case requires full acquisition of every asset. Select the sources that can distinguish among origin, spread, persistence, exfiltration, and recovery.

Each acquisition identifies the source, method, tool and version, date and time zone, authority, coverage, output, errors, and verification. Open the output before accepting it as valid. A file that exists but cannot be read is not useful evidence. Keep incidents in the case file, including incomplete acquisitions and incompatible tools. Repeating an acquisition creates another related object; it does not erase the first attempt.[3][4]

3.2 Logs before account suspension or reinstallation

Before disabling an account, export sign-in logs, factor enrollment, recovery changes, mail rules, delegations, tokens, and available administrative activity. Before reinstalling, preserve an image, configuration, logs, tasks, and relevant artifacts. These actions may be impossible in an emergency; record what was lost and why rather than inventing an ideal sequence.

Retention windows can lapse while scope is being debated. Ask the provider to preserve data with the period, accounts, fields, time zone, native format, data dictionary, filters, and limitations specified. Preserve the delivery with complete EML files, bodies, headers, and attachments. If the provider supplies a hash for each file, verify it locally and record any discrepancy without modifying the source.[5]

3.3 Evidence of the ransom note and contact channel

Preserve the ransom note as an object: a screenshot, the original file if available, location, filename, observation date, format, and relationship to the device. The text may contain false claims about exfiltration, surveillance, or access duration. Treat it as a statement by the attacker, not as a proven fact. Record payment and contact identifiers without making transactions or following instructions.

Item	Required record	Error avoided
Ransom note	Original item, location, date, relationship, and verbatim content.	Treating its text as a technical confession.
Encrypted file	Controlled sample, name, size, prior state, and preserved copy.	Opening many files and altering the scene.
Incident email	EML, attachments, headers, date, and recipient.	Saving only a screenshot of the message.
Support account	Role, permissions, activity, and export.	Sharing access or expanding the incident.
Backup	Date, version, coverage, location, and access status.	Connecting it without assessing contamination.

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

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

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

Laboratory safety

Do not run samples on personal devices or production networks. Dynamic analysis requires an isolated environment, a defined objective, authorization, network controls, and logging. For first response, preservation and escalation are usually sufficient.



Figure 2. Sources that must not disappear during containment. Each acquisition declares its coverage and limits. Editorial reconstruction; not actual evidence.

Chapter 4. Investigation: origin, persistence, and exfiltration

4.1 A timeline that shows uncertainty

The timeline preserves each literal date, time zone, source, precision, and conversion. A UTC log, a computer with an incorrect clock, and a local email must not be ordered as though they shared a clock without explaining the conversion. First detection is not necessarily first access. A file's modification date does not establish when the encryptor ran; it may indicate when the resulting output was written.

Separate observed events, events reported by a person, calculated events, and inferred events. Do not present inference as a log entry. If no source exists for a stage, write “not established within the scope.” Missing logs may result from rotation, configuration, filtering, or deletion, not necessarily because the event did not occur.

4.2 Entry and persistence hypotheses

Hypotheses may include stolen credentials, an exposed vulnerability, malicious email, a vendor, an external device, or a combination. Test each against sources that could weaken it: authentication, factor changes, rules, processes, scheduled tasks, services, new accounts, connections, and administrative activity. Choose the explanation compatible with the most facts and the fewest contradictions, not the most spectacular one.

Hypothesis	Source that confirms or weakens it	Limitation of the conclusion
Compromised legitimate account	Anomalous sessions, authentication factor, device, recovery, and approximate geography.	Using an account does not identify a person.
Public vulnerability	Version, exposure, logs, controlled testing, and patch date.	The presence of a vulnerability does not prove exploitation.
Malicious email	EML, attachments, opening and execution telemetry.	Receipt does not prove execution.
Compromised vendor	Remote access, roles, changes, and temporal correlation.	A contractual relationship does not prove the attack vector.
Persistence	Accounts, tasks, services, keys, rules, and artifacts.	Do not eradicate only the visible file.

4.3 Exfiltration: absence of evidence and evidence of absence

To assess exfiltration, review connections, destinations, volume, compression, cloud synchronization, email, rules, transfer services, proxy logs, DNS when available, and the attacker's statements as a separate hypothesis. High volume may reflect backups or legitimate activity; a lack of traffic may indicate missing logs, uninspected encryption, or a channel outside the scope.

The conclusion distinguishes among evidence of transfer, compatible indicators, insufficient data, and observed absence within defined coverage. Do not state “there was no exfiltration” merely because the firewall does not show it. Nor should “we will publish your data” be accepted as proof that data was exfiltrated. If a published sample is located, document it without redistributing it or downloading unnecessary information.

> **Defensible wording**
> “No transfers associated with the incident were observed in the proxy logs between these dates and with these fields. Coverage does not include uninspected encrypted channels, other providers, or earlier periods; therefore, a complete absence of exfiltration cannot be asserted.”

Chapter 5. Eradication and the ransom decision

5.1 Eradicate the cause, not just the symptom

Eradication covers accounts, recovery methods, rules, remote access, persistence mechanisms, vulnerabilities, secrets, and vendor access paths. Changing a password is insufficient if tokens, sessions, or keys remain. Deleting the encryptor does not remove the entry point. Verify measures with sources and tests, and record their effects on operations.

If the cause is unknown, state that explicitly. The organization may choose to rebuild from a trusted environment rather than “clean” the existing system. Base the decision on risk and evidence, not apparent cost savings. A reinstalled system receives new configuration, credentials, and monitoring; it is not returned to the same state that enabled the incident.

5.2 To pay or not to pay: a documented decision, not an impulse

The decision to pay belongs to the organization and its legal advisers, insurers, and competent authorities. It must consider legality, sanctions, the origin and destination of funds, continuity capacity, protection of people, the possibility of further extortion, and the lack of any recovery guarantee. This manual does not

recommend paying or contacting the attacker; it provides a structure so the decision does not rest with one person under pressure.

Factor	Question to answer	Evidence for the decision
Lawfulness	Is there any prohibition, sanction or restriction applicable?	Up-to-date legal analysis and approval channel.
Continuity	Is there another viable route, and how long will it take?	Backup tests, alternatives, and interruption cost.
Recovery	What is promised, and what can be verified?	No verbal guarantees; technical assessment and limitations.
Risk to people	Is there any additional threat or sensitive data?	Safety priority and protection of affected people.
Recurrence	What incentive or exposure is left?	Documented risk and follow-up plan.
Authority	Who can decide and communicate?	Quorum, record, and single authorized channel.

5.3 Communication and obligations

Notification assessment distinguishes among customers, data subjects, regulators, insurers, partners, and authorities. Each jurisdiction and contract has different thresholds and deadlines. Prepare technical information so it explains facts, uncertainty, and measures without revealing details that could increase harm. Public communication must not get ahead of preservation or turn a suspicion into an announced cause.

In Mexico, credit institutions have specific obligations under applicable provisions to investigate and report incidents and to maintain and retain records; in Peru, the SBS requires supervised entities to preserve evidence and conduct forensic analysis; in Argentina, Communication A 8280 addresses response and final reporting under its regime. Do not apply these deadlines to every organization or to other countries.[6][7][8]

> **Do not manufacture certainty**
> The executive report can state what is known, what is being done, and what remains to be determined. It need not choose between panic and artificial reassurance. It needs a defensible timeline and clearly assigned responsibilities.

Chapter 6. Recovery and continuity

6.1 Select and validate the recovery point

The most recent backup may contain persistence mechanisms or damaged files; an older one may not include legitimate operations. Compare date, coverage, integrity, access, history, and compatibility. Preserve the original backup and work from a controlled copy in an isolated environment. Deliver keys through a separate channel and do not write them in the record.

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

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

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

Validation confirms that the copy opens, contains the expected objects, can be mounted, has consistent versions, and shows no known indicators of compromise. It does not prove the copy is completely clean; it proves that it passed the defined tests. If the copy contains errors, decide whether they affect the objective and retain their details.

6.2 Phased recovery

Start with minimum services in isolation, using fictitious data or test accounts. Then test identity, permissions, applications, integration, reading and writing, export, and monitoring. Only then authorize gradual expansion. Do not use the production network as a laboratory for initial recovery.

Stage	Acceptance criterion	Evidence
Minimum infrastructure	Verified components and versions, with no known persistence.	Inventory and configuration.
Data	Readable files, correct coverage, and correct relationships.	Sample, manifest, and count.
Application	Functions and permissions work with fictitious accounts.	Test cases and results.
Integration	Authorized dependencies respond without unplanned routes.	Logs and connections.
Observation	No abnormal activity appears during the defined period.	Alerts, queries, and limitations.
Exit	Responsible party accepts residual risk and subsequent review.	Exit record and monitoring.

6.3 Reconciling information and lessons learned

It may be necessary to reconstruct operations created between the last intact backup and detection. Reconcile external logs, receipts, emails, messages, and third-party documents without altering the source. Record discrepancies; do not fill them with estimates presented as actual data.

Lessons learned must change procedures: new retention rules, phishing-resistant authentication, segmentation, immutable backups, restore testing, contact directories, privilege restrictions, or exercises. If the incident ends with a presentation but no behavior changes, the next crisis will repeat the same sequence.

> **Closeout criterion**
> Recovery means resuming operations with evidence that controls work and an honest explanation of what remains unknown. Closeout covers people, systems, data, vendors, and subsequent review.

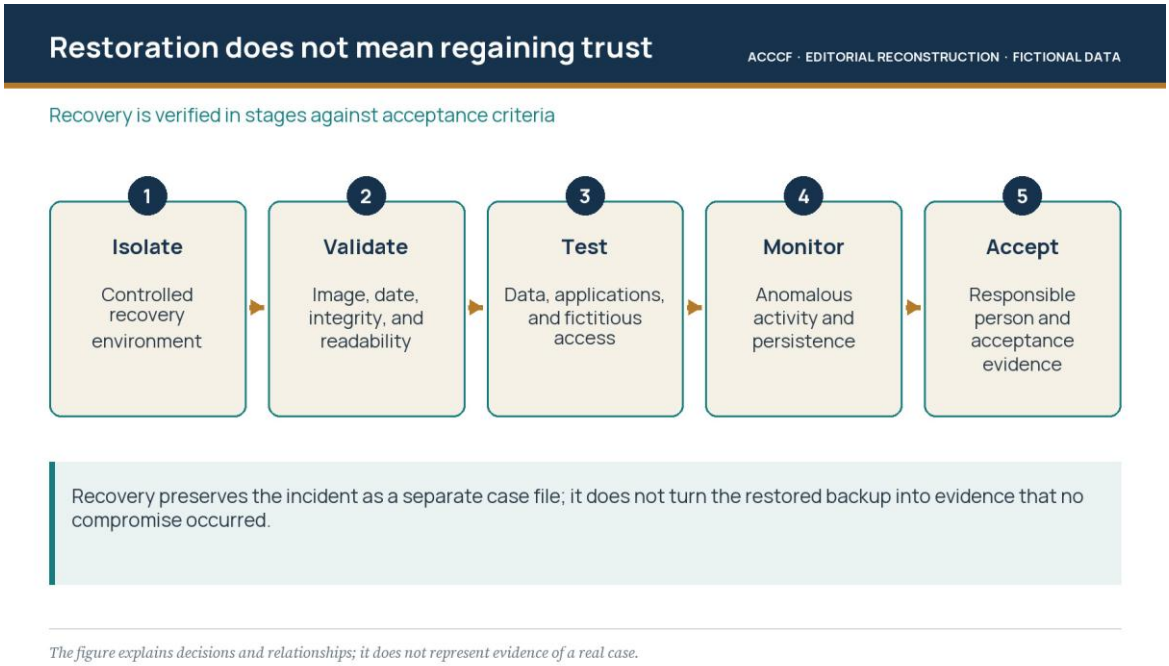


Figure 3. Restoration does not equal restored trust. Exit is verified in stages against acceptance criteria. Editorial reconstruction; not actual evidence.

Appendix A. Legal framework and sector-specific records

The incident may involve electronic evidence, data protection, contracts, financial obligations, and continuity rules. These areas must be analyzed separately. A sector-specific rule does not create a universal obligation, and a retention period does not authorize retaining everything indefinitely. Document review current as of November 10, 2026; an actual case file requires verification of the law in force, covered entity, subject matter, and reporting channel.

Jurisdiction	Relevant sources	Limitation on use
Mexico	CCom 89–94 and 1205; CFPC 210-A / CNPCF 348–350, depending on the transition; CNBV 316 Bis series for covered entities; LFPDPPP for personal data.	Distinguish electronic documents, legal procedure, banking, and privacy. Review the CNPCF declaration.
Peru	IOFE Regulations; CPC 188–197; SBS 504-2021 and 2286-2024 for supervised entities.	Do not attribute a complete documentary regime to Law 27269 or copy CNBV deadlines.
Chile	Law 19.799; RAN 20-7, 20-8, and 20-10, depending on the entity and service.	Do not confuse continuity, outsourcing, and incidents.
Argentina	Law 25.506; CCyC 318–319; BCRA A 7783 and A 8280.	Specific deadlines and covered entities; authentication is not authorization.
Colombia	Law 527; CPACA for administrative proceedings; SFC regulations to be confirmed for the specific provision.	Do not invent incident requirements from an unread circular.
Ecuador	Law 67; LOPDP; payment system regime where applicable.	Notification and retention depend on the data processing and sector.
Spain / EU	eIDAS; LEC 326 and 384; RGPD; RD-ley 19/2018 for payment services.	Distinguish among documents, procedure, privacy, and unauthorized transactions.

Sources for the table:[9][10][11][12][13][14][15][16][17][18][19][20][21][22][23][24][25][26][27]

For a log request, specify the purpose, period, reference, fields, format, time zone, and delivery method. The goal is not to request every server, but the events that can answer specific questions. The chain of custody records who delivers, who receives, what the item contains, how it is verified, and what limitations exist.

Appendix B. Response templates

B.1 Incident timeline

Field	Required record	Control
Event	Observed, declared, calculated or inferred.	Do not mix categories.
Literal date and time zone	Original text, conversion and precision.	Do not overwrite the source.
Asset and source	Item, system, identifier, and location.	Traceability to the manifest.
Action and responsible party	What happened, who decided, and who carried it out.	Authority and evidence.
Result	Output, errors, and state changes.	Do not hide incidents.
Next check	Open question and responsible party.	Avoid premature closure.

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

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

[11] 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

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

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

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

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

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

[17] Chile. Updated Compilation of Standards, Chapters 20-7, 20-8, and 20-10: outsourcing, operational incidents, information security, and cybersecurity. Official online source

[18] Argentina. Digital Signature Law 25.506, Articles 1 and 5–9: digital documents, the burden on a party invoking an unrecognized electronic signature, and limited presumptions. Official online source

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

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

[21] 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

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

[23] Ecuador. Organic Law on Personal Data Protection, Official Registry Supplement 459 of 26-05-2021. Articles 10 and 37–44: principles, security measures, data protection by design, risks, and incident handling. Official online source

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

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

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

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

B.2 Containment decision matrix

Fictitious decision sheet

```
Incident: DEMO-RANSOM-2026-001
Asset and service: [identifier, function, dependencies]
Observed state: [screen, processes, network, encryption]
Options assessed: [power off, isolate network, keep running, suspend account]
Risk to people and continuity: [priority]
Volatility and evidence at risk: [memory, logs, sessions]
Decision and authority: [action, person, date, and time zone]
Prior preservation: [item, method, and output]
Change made: [final state and collateral effect]
Outstanding: [what could not be preserved or confirmed]
Review: [responsible party and next assessment time]
```

B.3 Acquisition log

Technical manifest

```
Source / acquisition ID: DEMO-SRV-001 / A01
Authority and scope: [document and exclusions]
Initial status: [photographs and observations]
Objective and coverage: [memory, image, logical acquisition, export]
Tool and validation: [version, environment and test]
Start / end with time zone: [literal values]
Output: [files, format and size]
Integrity: [algorithm and exact object]
Issues: [errors and missing coverage]
Verification: [opening, relationship, and review]
Custody: [safekeeping, access, and transfers]
```

B.4 Recovery exit criteria

Check	Yes / no / not applicable	Evidence and observation
Backup preserved before use	[ ]	Identifier and custody.
Readable data and consistent coverage	[ ]	Sample and count.
Reconstructed accounts and factors	[ ]	No previous sessions.
Persistence assessed	[ ]	Sources and limitations.
Tested functions and integrations	[ ]	Fictitious cases.
Monitoring and responsible party assigned	[ ]	Alerts and checks.
Communications completed	[ ]	Versions and recipients.
Accepted residual risk	[ ]	Responsible party's signature and date.

Appendix C. Exercise and checklist

C.1 Tabletop exercise with fictitious data

Simulate a company with three servers, two administrative accounts, nightly backups, and an email provider. At 08:12, encryption is reported in documents; at 08:16, another device shows the same extension; at 08:20, a forwarding rule is discovered in an account. The team must decide on isolation, initial acquisitions, vendor contact, data assessment, and a recovery path without running any files.

Assessment is based on the quality of decisions and records: if the team restores without preserving evidence, it loses the opportunity to explain the forwarding; if it suspends the account before exporting, it documents the limitation; if it leaves a critical service without an alternative, it must justify that decision. At the end, review the decisions rather than rewarding the fastest response.

C.2 Short pre-closure checklist

Question	Expected result
Are the people protected?	Priorities addressed and essential services maintained.
Was priority volatile evidence preserved?	Items, methods, and limitations recorded.
Were origin, persistence and exfiltration assessed?	Hypotheses and sources, no absolutes.
Were the ransom and communication decisions authorized?	Quorum, rationale, and versions.
Was the recovery tested?	Data, functions, access, and observation.
What changed for next time?	Implemented control, responsible party, and validation.

Closeout

Calm does not mean saying everything is fine. It means knowing what is being done, on what evidence, who decides, and what remains to be verified.