ACCCF

ANGEWANDTES WISSEN · SPANISCHSPRACHIGES AMERIKA

SPANISCHSPRACHIGES HANDBUCH FÜR DIGITALE BEWEISE 2026 V1

Digitale Beweise im spanischsprachigen Raum bewahren, überprüfen und erläutern.



Erstellt und unterzeichnet von

Jocsan Laguna Romero

Präsident des ACCCF

Institutionelle Ausgabe des Rates

Inhalt

Allgemeine technische Anleitung. Keine Rechtsberatung oder forensische Begutachtung. Die Beispiele sind fiktiv oder anonymisiert; die Abbildungen sind redaktionelle Rekonstruktionen. Die sichtbare Seitennummerierung entspricht der PDF-Ausgabe. Word kann dieses Verzeichnis beim Öffnen des Dokuments aktualisieren; die interne Navigation der Überschriften bleibt erhalten.

Vorstellung des Handbuchs 6

So verwenden Sie dieses Handbuch 8

Kapitel 1. Umfang, Fragen und Befugnis 9

1.1 Die Leitfrage für die Arbeit 9
1.2 Befugnis vor Zugriff 10
1.3 Erstinventar der Quellen 10
1.4 Vollständiges Beispiel: eine Forderung im Zusammenhang mit Verkäufen 11
1.5 Begründung und Abschluss: Die Methode schützt auch Menschen 12

Kapitel 2. Integrität, Original und Kontext 14

2.1 Das Original ist nicht immer das Gerät 14
2.2 Integrität, Authentizität, Zurechnung und Wahrheitsgehalt 14
2.3 Der Hashwert als Kontrolle, nicht als Dogma 15
2.4 Interne Metadaten und Systemdaten: eine Unterscheidung, die Fehler vermeidet 16
2.5 Der Fall der Fotografien und der Bank 17
2.6 Zugänglichkeit und Erhaltung des Kontexts 17

Kapitel 3. Rollen, Verantwortlichkeiten und Entscheidungen 19

3.1 Funktionen vor Positionsbezeichnungen 19
3.2 Die erste Reaktion ohne Improvisation 19
3.3 Operative Kommunikation 20
3.4 Unabhängigkeit, Datenschutz und Dritte 21
3.5 Ein Syllogismus der Rollen 21

Kapitel 4. Lebenszyklus und forensische Vorbereitung 23

4.1 Vorbereitung vor der Entgegennahme eines Falls 23
4.2 Unumkehrbare Entscheidungen 24
4.3 Dokumentierter Lebenszyklus und Ergebnisse 26
4.4 Aufbewahrung und Longitudinalanalyse 27
4.5 Vorbereitung als gesellschaftliche Verantwortung 28

Kapitel 5. Entscheidungsbäume nach Szenario 29

5.1 Ein- oder ausgeschaltetes Gerät 29
5.2 Lokale, entfernte oder anbieterseitige Erfassung 30
5.3 Mobilgeräte und Isolation 30
5.4 Optische Datenträger: Kennung und Format 31

5.5 Wann die Arbeit auszusetzen ist 32
5.6 Der Baum als Argumentation, nicht als Dekoration 33
Kapitel 6. Moderne Quellen und Gesprächsdatensätze 35
6.1 Cloud, SaaS und Exporte 35
6.2 E-Mail und EML 36
6.3 Anforderung und Entgegennahme von Gesprächsdatensätzen 37
6.4 Beispiel für den Text einer Anbieteranfrage 38
6.5 Virtualisierung, IoT und synthetische Inhalte 39
6.6 Gültigkeit: das Beispiel einer aufgehobenen Reform 41
6.7 Die Quelle befindet sich nicht an einem Ort 42
Kapitel 7. Entgegennahme und anfängliche Sicherung 43
7.1 Nachvollziehbares Entgegennahmeprotokoll 43
7.2 Verpackung und Versiegelung 44
7.3 Kennzeichnung und Beziehung zwischen Objekten 45
7.4 Zubehör und Verbindungen als Teil der Entgegennahme 46
7.5 Entgegennahme von Dateien und Nachrichten 47
Kapitel 8. Erfassung und technische Dokumentation 49
8.1 Physische, logische, flüchtige und dokumentarische Erfassung 49
8.2 Tatsächliche Verbindung: Quelle, Schreibblocker und Arbeitsstation 49
8.3 Medien und Adapter: NVMe, SATA und optische Laufwerke 50
8.4 Logische Erfassung und Manifest 51
8.5 Live-Erfassung und Werkzeugvalidierung 52
8.6 Exporte und reproduzierbare Abfragen 53
8.7 Fehler und Vorkommnisse 53
Kapitel 9. Verwahrung, Transport und Aufbewahrung 55
9.1 Die Beweismittelkette als Antwort auf Fragen 55
9.2 Elektronische Übertragungen und Schlüssel 56
9.3 Speicherung und späterer Zugriff 57
9.4 Öffnen und Erneuern des Siegels 57
9.5 Zugriffe, gemeinsame Verwahrung und Interessenkonflikte 58
Kapitel 10. Untersuchung, Chronologie und alternative Hypothesen 60
10.1 Untersuchen heißt nicht, einen Schuldigen zu suchen 60
10.2 Metadaten: der Datei zuhören, ohne alles zu glauben 60
10.3 Chronologie: Uhren abgleichen, bevor Geschichten geordnet werden 62
10.4 Antennen, Abdeckung und Azimut: Geografie ohne Abkürzungen 63
10.5 Bestätigung, die tatsächlich unterscheidet 65
10.6 Hypothesenmatrix: Beweise widersprechen lassen 66
10.7 Wiederholen, Reproduzieren und wissen, wann aufzuhören ist 68
Kapitel 11. Bericht, Argumentation und Widerlegung 70
11.1 Der Bericht als Rückweg zur Quelle 70

11.2 Tatsache, Ergebnis, Ableitung und Meinung 71
11.3 Der Syllogismus und die falsche Konsequenz 71
11.4 Widersprüche erklären, ohne sie zu verbergen 72
11.5 Schlussfolgerungen formulieren, die die Beweise tragen 73
11.6 Widerlegung und unabhängige Überprüfung 74
11.7 Übermittlung, Anhänge und späterer Zugriff 75
Kapitel 12. Fehler, Lernen und öffentlicher Dienst 76
12.1 Fehler werden nicht durch Umschreiben der Vergangenheit korrigiert 76
12.2 Fehler bei Entgegennahme und Sicherung 77
12.3 Fehler bei Quelle, Erfassung und Export 77
12.4 Interpretationsfehler 78
12.5 Juristische Fehler und Fehler bei der Gültigkeit 79
12.6 Gelernte Lektionen, die das Verfahren verändern 80
12.7 Das letzte Ziel: den nächsten Übergriff verhindern 81
Anhang A. Funktionale juristische Entsprechungen 83
Zusammenfassung 83
1. Methode und Grenzen des Vergleichs 83
2. Zentrale Matrix nach Rechtsfunktion 84
3. Mexiko: Rechtsgrundlage und Übergang 91
4. Peru: verteiltes Regime und finanzielle Aktualisierung 94
5. Chile: Signatur, Datum und Sicherheitsregulierung 95
6. Argentinien: begrenzte Vermutungen und Zuverlässigkeit des Trägers 96
7. Kolumbien: Datennachrichten, Aufbewahrung und Empfangsbestätigungen 98
8. Ecuador: dokumentarische Entsprechung und Zahlungssystem 99
9. Spanien und Europäische Union: Nichtdiskriminierung, Vertrauensdienste und Verfahren 100
10. Funktionaler Vergleich von Aufzeichnungen und Finanzvorfällen 101
11. Internationale methodische Standards 105
12. Regeln für die Verwendung der Matrix ohne falsche Entsprechungen 106
A.13 Praktische Anwendung: Rechtsregime vor der Schlussfolgerung auswählen 107
A.14 Datenschutz während der Untersuchung in Mexiko 108
Anhang B. Formular für Umfang und Befugnisse 109
B.1 Inhalt des Formats 109
Anhang C. Protokoll der Entgegennahme und anfänglichen Sicherung 111
C.1 Beispiel eines physischen Protokolls 111
C.2 Entgegennahme von Dateien oder Nachrichten 112
Anhang D. Erfassungsprotokoll 113
D.1 Vollständiges Beispiel 113
Anhang E. Beweismittelkette und Übertragungen 115
E.1 Beispiel einer Abfolge 115
E.2 Elektronische Übertragung 115

Anhang F. Anfrage und Erfassung über einen Anbieter 116
F.1 Musteranfrage 116
F.2 Protokoll des Exports oder der API 116
Anhang G. Inventar und Manifest der Objekte 118
G.1 Beispiel eines Manifests 118
Anhang H. Chronologie und Zeitzonen 120
H.1 Beispiel einer Zeitachse 120
H.2 Regel für widersprüchliche Datumsangaben 120
Anhang I. Hypothesen- und Bestätigungsmatrix 121
I.1 Ausgearbeitetes Beispiel 121
Anhang J. Prüfung synthetischer Inhalte 123
J.1 Angewandtes Format 123
Anhang K. Berichtsstruktur und Schlussfolgerung 124
K.1 Empfohlene Abfolge 124
K.2 Beispiel einer vollständigen Schlussfolgerung 125
Anhang L. Operative Checklisten 126
L.1 Entgegennahme und Erfassung 126
L.2 Analyse, Bericht und Übermittlung 126
Anhang M. Kontrolle von Versionen, Quellen und Erkenntnissen 128
M.1 Normatives und technisches Protokoll 128
M.2 Lektion in Verbesserung umsetzen 128

Vorstellung des Handbuchs

Die Sicherung digitaler Beweise besteht nicht darin, Dateien aufzubewahren, bis sie ausreichend erscheinen. Es geht darum, die Möglichkeit zu bewahren, dass eine andere Person mit anderem Urteilsvermögen und anderen Werkzeugen zu einer mit den Tatsachen vereinbaren Schlussfolgerung gelangen kann. Ein Gerät ersetzt keinen Zeugen, ein Bildschirmfoto ersetzt nicht die Datei und eine Meinung ersetzt keine Methode. Die Arbeit beginnt lange vor dem Öffnen des ersten Objekts: Sie beginnt, wenn jemand entscheidet, welche Behauptung nachgewiesen werden muss und welche Folgen das Vorgehen hat.

Dieses Handbuch entstand aus einer unbequemen, aber notwendigen Frage: Wie viele Übergriffe ließen sich vermeiden, wenn die erste Person, die Beweise entgegennimmt, die einfachen Dinge richtig macht? Das Objekt identifizieren, seinen Zustand fotografieren, die Autorisierung abgrenzen, die native Datei anfordern, die vollständige Nachricht aufbewahren, Datum und Zeitzone notieren, eine Antenne nicht mit einer Person verwechseln und eine Intuition nicht als Wissenschaft darstellen. Die Grundlagen sind kein Beiwerk. Sie verhindern, dass eine Anklage auf einer Annahme aufgebaut wird und eine Verteidigung an einer vermeidbaren Unterlassung scheitert.

Die Regel, die alles Weitere strukturiert, lässt sich so formulieren: Quelle, Befugnis, Zustand, Methode, Dokumentation, Überprüfung und begrenzte Schlussfolgerung. Zuerst wird bestimmt, welche Quellen Informationen liefern können. Anschließend wird geprüft, wer den Zugriff unter welchen Bedingungen autorisieren darf. Der Zustand bei Eingang des Objekts wird dokumentiert, eine geeignete Methode wird ausgewählt und alle Maßnahmen werden festgehalten. Erst danach wird überprüft und innerhalb der Möglichkeiten der Quellen eine Schlussfolgerung gezogen. Scheitert eine Phase, wird die nächste nicht durch Rhetorik korrigiert: Die Einschränkung wird anerkannt und entschieden, was ohne eine fehlerfreie Geschichte zu erfinden, wiederhergestellt werden kann.

Magischer Realismus ist hier kein literarischer Schmuck. Er bedeutet anzuerkennen, dass alltägliche Objekte etwas Außergewöhnliches erzählen können: Eine Bank kann eine Pause beschreiben, ein Zentralring kann einen Datenträger identifizieren, eine Tasche kann ein falsches Gefühl der Isolierung vermitteln und eine Uhr kann einer anderen widersprechen. Analogien sind Brücken zum Verständnis, kein Ersatz für Beweise. Die Seriosität liegt darin, stets zur Quelle zurückzukehren und zu fragen, was sie beweisen kann und was sie lediglich nahezulegen scheint.

Zweck dieses Werkes

Dieses Werk vermittelt Grundlagen, damit niemand den Umgang mit digitalen Beweisen auf schmerzhafte Weise erlernen muss. Es bietet eine Methode für Polizeibeamte, Sachverständige, Rechtsanwälte, Ingenieure und Verantwortliche in Organisationen, ohne schwierige Entscheidungen oder Unsicherheiten zu verschweigen.

Die Beispiele sind fiktiv oder anonymisiert. Die Bilder sind redaktionelle Rekonstruktionen: Sie zeigen Geräte und Handlungen, stellen aber keine tatsächlichen Beweise aus den Fällen dar. Rechtsnormen werden mit Funktion, Artikel, Geltungsbereich und Konsultationsdatum zitiert. Ist eine Entsprechung zwischen Ländern nur partiell oder sektoral, wird dies ausdrücklich angegeben, denn ein ähnlicher Wortlaut erzeugt nicht dieselbe Rechtswirkung.

So verwenden Sie dieses Handbuch

Wenn Sie die erste Person sind, die den Fall entgegennimmt, beginnen Sie mit den Kapiteln 1, 3, 5 und 7. Dort wird erläutert, wie Sie den Auftrag abgrenzen, Funktionen zuweisen, einen Weg nach dem Zustand des Objekts auswählen und den Eingang ohne Improvisation dokumentieren. Um die ersten Fehler zu vermeiden, müssen Sie kein Analyst werden: Sie müssen wissen, was zu sichern ist und wann Sie Unterstützung anfordern.

Wenn Sie erfassen oder analysieren, arbeiten Sie mit den Kapiteln 4, 6, 8, 9 und 10. Der technische Teil erläutert die Auswahl von Quellen, die Dokumentation von Erfassungen, die Prüfung von Dateien, die Erstellung von Chronologien und die Bewertung alternativer Hypothesen. Wenn Sie präsentieren oder prüfen, verwenden Sie die Kapitel 2, 11 und 12 sowie die juridischen und operativen Anhänge. Ziel ist nicht, ein Verfahren zu wiederholen, sondern zu verstehen, warum jede Entscheidung eine verwertbare Spur hinterlässt.

Die Formulare sind kein Selbstzweck. Ein leeres Protokoll mit einem ansprechenden Titel kann weiterhin eine Pseudo-Verwahrung sein, so wie ein Foto ohne URL nur ein unvollständiges Bild sein kann. Jedes Formular muss eine Entscheidung oder Überprüfung erfassen: Was wurde autorisiert, was empfangen, was verändert, wer hat überprüft und welche Einschränkungen bestehen? Felder, die zur Beantwortung dieser Fragen nichts beitragen, werden entfernt.

Die Lektüre ist kumulativ. Die Begriffe kehren wieder, weil jeder eine Ebene ergänzt: Eine Quelle kann nur in eingeschränktem Sinne original sein, ein Export kann eine bessere Quelle als das Gerät sein, eine Antenne beschreibt Abdeckung und keine Adresse, und eine Signatur kann Rechtskraft haben, ohne zu beweisen, welche Hand die Schaltfläche betätigt hat. Gehen Sie nicht vorschnell zu den Befehlen über. Geschwindigkeit entsteht, wenn das Urteilsvermögen bereits klar ist.

Kapitel 1. Umfang, Fragen und Befugnis

1.1 Die Leitfrage für die Arbeit

Ein unzureichend formulierter Auftrag führt zu einer aufgeblähten Untersuchung. „Prüfe alles“ sagt weder, was nachgewiesen werden soll, noch, wofür das Ergebnis verwendet wird oder welches Veränderungsrisiko akzeptabel ist. Eine präzise Frage ermöglicht dagegen zu entscheiden, welche Quellen erforderlich sind und welche unangetastet bleiben müssen: welche Vorgänge geltend gemacht werden, in welchem Zeitraum, aus welchen Systemen und mit welchen juridischen oder betrieblichen Folgen.

Dokumentieren Sie die Darstellungen getrennt. Eine Partei behauptet, nicht bezahlte Verkäufe getätigt zu haben; die andere bestreitet, diese Vorgänge erhalten zu haben. Vermischen Sie beide nicht zu einer einzigen Geschichte. Die erste Hypothese darf nicht zu einer Suchanweisung werden, nur um ihre Bestätigung zu finden. Die zweite darf nicht verworfen werden, weil sie unbequem ist. Die Methode soll beide prüfbar machen, nicht einer von ihnen vorab zum Sieg verhelfen.

Eine Wiederherstellung zur Aufrechterhaltung des Betriebs stellt nicht dieselben Anforderungen wie ein forensisches Gutachten für eine gerichtliche Auseinandersetzung. Im ersten Fall kann eine kontrollierte Kopie genügen, um die Arbeit fortzusetzen. Im zweiten sind Befugnis, Integrität, Kontext, Nachverfolgbarkeit, Überprüfbarkeit und eine Erklärung erforderlich, die nicht vom Ansehen des Unterzeichners abhängt. Eine Verwechslung dieser Ziele führt zu zwei Fehlern: zu viel Aufwand für eine einfache Wiederherstellung oder zu wenig für eine Behauptung mit schwerwiegenden Folgen.

Frage	Was dokumentiert werden muss	Entscheidung, die Improvisation vermeidet
Was behauptet jede Partei?	Getrennte Fassung nach Person, Sachverhalt und Datum.	Eine Darstellung nicht als erwiesene Tatsache behandeln.
Was muss nachgewiesen werden?	Sachverhalt, Zeitraum, System und erwartetes Ergebnis.	Quellen und Methode abgrenzen.
Wofür wird das Ergebnis verwendet?	Betriebskontinuität, interne Untersuchung, forensisches Gutachten oder Verfahren.	Umfang der Dokumentation festlegen.
Was kann ausgeschlossen werden?	Ausgeschlossene Daten, Geräte, Konten oder Zeiträume.	Unnötige Offenlegung verringern.

1.2 Befugnis vor Zugriff

Dass Sie eine Datei öffnen können, bedeutet nicht, dass Sie sie prüfen dürfen. Die Autorisierung muss Inhaber, zulässige Handlungen, Systeme, Verantwortliche, Ausschlüsse und Kommunikationskanal angeben. Ist Zugriff auf Daten Dritter, ein gemeinsam genutztes Konto oder einen Anbieter erforderlich, wird der rechtmäßige Weg dokumentiert. Technische Fähigkeit schafft keine Befugnis; sie ermöglicht lediglich, das auszuführen, was die Befugnis erlaubt.

Bei der Verhältnismäßigkeit ist zu prüfen, ob Quelle und Methode für das Ziel erforderlich sind. Ein administrativer Export kann die Frage mit weniger Veränderung und Offenlegung besser beantworten als eine vollständige Geräteprüfung. Alles zu sammeln ist keine Vollständigkeit: Es kann Rauschen und Datenexposition erzeugen und die Frage elegant verschwinden lassen. Gibt es eine Quelle mit größerer Unterscheidungskraft und geringerem Eingriff, ist sie der erste Kandidat.

Vertraulichkeit wird bereits bei der Entgegennahme festgelegt, nicht erst am Ende des Berichts. Bestimmt wird, wer Informationen einsehen, kopieren, übertragen und veröffentlichen darf, insbesondere bei Daten Dritter, Minderjähriger, Opfer oder Geschäftsgeheimnissen. Personenbezogene Daten müssen rechtmäßig und auf die erforderlichen, mitgeteilten Zwecke beschränkt verarbeitet werden, mit risikoangemessenen Sicherheits- und Vertraulichkeitsmaßnahmen. Das neue Gesetz verlangt außerdem, erhebliche Datenschutzverletzungen unverzüglich mitzuteilen, damit sich die Betroffenen schützen können.[1]

Handlungsregel
Sind Befugnis oder Umfang unklar, wird die Maßnahme ausgesetzt und die Frage geklärt. Dokumentieren Sie die Unklarheit, die erhaltene Antwort, die antwortende Person und den Zeitpunkt. „Ich wusste nicht, ob ich es durfte“ ist keine belastbare Beweismittelkette.

1.3 Erstinventar der Quellen

Erstellen Sie eine Liste der Geräte, Konten, Dateien, Server, Anbieter, Dokumente und Personen, die Kontext liefern können. Erfassen Sie auch nicht verfügbare Quellen und den Grund: verlorenes Gerät, unbekanntes Passwort, abgelaufene Aufbewahrungsfrist, nicht antwortender Anbieter oder nicht autorisierter Zugriff. Auch das Fehlen verändert die Planung und die möglichen Schlussfolgerungen. Eine unvollständige Akte darf nicht als vollständiges Universum dargestellt werden.

Priorisieren Sie nach der Eignung zur Prüfung von Hypothesen, der Volatilität und dem Verlustrisiko. Arbeitsspeicher, eine aktive Sitzung, ein rotierendes Protokoll und ein ablaufender Link können unterschiedliche Maßnahmen erfordern. Die Priorität richtet sich nicht

[1]Ley Federal de Protección de Datos Personales en Posesión de los Particulares, neues Gesetz vom 20-03-2025, geändert am 14-11-2025. Artikel 5–9, 18–20 und 31: Grundsätze, Sicherheit, Vertraulichkeit, Verletzungen und Fristen.Offizielle Online-Quelle

danach, welches Gerät wichtiger erscheint, sondern welche Informationen zuerst verschwinden können und welche Frage sie beantworten. Ockhams Rasiermesser beginnt mit der Quelle, die am besten unterscheidet, nicht mit der größten technischen Reputation.

Feld des Inventars	Beispiel einer nützlichen Aufzeichnung	Warum es wichtig ist
Kennung und Verwahrer	Abrechnungsdatei, Zahlungsabwickler, Bank und autorisierter Verantwortlicher.	Verhindert Anfragen an den falschen Verwahrer.
Typ, Zeitraum und Format	Vorgänge einer Woche, native CSV-Datei und Feldverzeichnis.	Ermöglicht den Vergleich von Struktur und Bedeutung.
Verfügbarkeit	Fehlende Datei, aktiver Link oder ausstehender Anbieter.	Einschränkungen von Anfang an ausweisen.
Risiko	Rotation, Fernlöschung, Offenlegung gegenüber Dritten oder physischer Verlust.	Bestimmt Priorität und Methode.
Autorisierung und Kontakt	Inhaber, sicherer Kanal und Vertretung.	Vermeidet zweifelhafte Zugriffe und undokumentierte Verzögerungen.

1.4 Vollständiges Beispiel: eine Forderung im Zusammenhang mit Verkäufen

Eine Handelskette behauptet, Verkäufe getätigt zu haben, für die keine Zahlung erfolgt sei. Die Frage ist nicht, „alle ihre Computer zu prüfen“, sondern festzustellen, ob die Vorgänge erfasst, übermittelt und abgerechnet wurden. Datum, Betrag, Referenz und Zahlungsabwickler werden abgegrenzt. Prioritäre Quellen sind Berichte des Händlers, Abrechnungsdateien, Protokolle des Zahlungsabwicklers, Netzwerkgeräte und Bankberichte. Jede Quelle beantwortet einen anderen Teil der Abfolge.

Die Autorisierung beschränkt sich auf diese Systeme und den entsprechenden Zeitraum. Erscheinen die Vorgänge nicht in der vom Geschäft selbst erstellten Abrechnungsdatei, gibt dieser Befund der Untersuchung eine Richtung, beweist aber noch nicht, wer die Abweichung verursacht hat. Möglich sind nicht vorhandene Vorgänge, eine unvollständige Abrechnungsdatei, ein anderer Kanal oder ein fehlerhafter Export. Die verantwortungsvolle Schlussfolgerung beginnt mit der dokumentierten Abwesenheit in der Quelle, nicht mit einer Anschuldigung gegen den ersten verfügbaren Verdächtigen.



Abbildung 1. Quellen vor dem Handeln abgrenzen: Was geprüft werden darf und was ausgeschlossen bleibt. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Was das Beispiel zeigt
Eine gut abgegrenzte Frage vermeidet eine invasive Prüfung persönlicher Geräte und erfordert den Vergleich unabhängiger Quellen. Beweise werden nicht nach Umfang gesammelt, sondern nach ihrer Eignung zur Prüfung einer Behauptung ausgewählt.

1.5 Begründung und Abschluss: Die Methode schützt auch Menschen

Identifizierung, Sammlung, Erfassung und Erhaltung sind nicht nur technische Vorgänge. ISO/IEC 27037 stellt sie als Entscheidungen dar, die für eine spätere Überprüfung dokumentiert werden müssen. Quelle und Befugnis bestimmen die Methode; ein Passwort oder ein Gerät in der Hand schafft keinen legitimen Zugriff. Diese Abfolge verhindert auch, dass eine Untersuchung für die Betroffenen zu einer zweiten Verletzung wird.[2]

In Mexiko können elektronische Informationen als Beweis zugelassen werden, wenn die Zuverlässigkeit der Methode, die Zurechnung, die Zugänglichkeit und die Integrität

[2]ISO/IEC 27037:2012. Leitlinien für Identifizierung, Sammlung, Erfassung und Erhaltung digitaler Beweise. Die Ausgabe wurde von ISO als gültig bestätigt.Offizielle Online-Quelle

nachgewiesen werden. Diese Anforderung ist mit einem isolierten Bildschirmfoto oder der Behauptung, ein Sachverständiger habe etwas auf einem Bildschirm gesehen, nicht erfüllt. Es muss erläutert werden, wie die Informationen erzeugt, übermittelt, empfangen oder archiviert und wie ihre Integrität seit ihrer Erzeugung bewahrt wurde. Diese Präzision begrenzt die später zulässigen Aussagen.[34]

Begrenzte Schlussfolgerung
Bevor Sie Beweise bearbeiten, müssen Sie beantworten können, welche Behauptung untersucht wird, wer autorisiert, welche Quellen am besten unterscheiden, welche Ausschlüsse Dritte schützen und welches Ergebnis erwartet wird. Fehlt eine Antwort, ist das erste Ergebnis keine Erfassung, sondern eine dokumentierte Klärung.

[3]Código Federal de Procedimientos Civiles, Artikel 210-A: Zuverlässigkeit der Methode, Zurechnung, Zugänglichkeit und Integrität elektronischer Informationen. Der Code wurde durch Dekret vom 07-06-2023 aufgehoben und unterliegt einem schrittweisen Übergangsregime.Offizielle Online-Quelle
[4]Código de Comercio de México, Artikel 89–94 und 1205: Neutralität, Zurechnung, Schriftform, Original, Integrität, Zugänglichkeit und Zulassung von Datennachrichten. Amtliche Zusammenstellung.Offizielle Online-Quelle

Kapitel 2. Integrität, Original und Kontext

2.1 Das Original ist nicht immer das Gerät

Bei digitalen Beweisen stützt sich der Begriff des Originals auf die Integrität ab der endgültigen Form und auf die Möglichkeit einer späteren Einsichtnahme, nicht allein auf die Aufbewahrung eines Geräts. Eine native Datei, ein bitweises Image, ein Export, ein Bildschirmfoto und ein Ausdruck sind unterschiedliche Darstellungen. Jede kann nützlich sein, wenn ihre Beziehung zum Ursprung und die erhaltenen oder verlorenen Informationen bekannt sind. Die Frage lautet nicht nur „Habe ich das Objekt?“, sondern „Was kann ich mit dieser Darstellung nachweisen?“ Ein bitweises Image des Mediums kann zugewiesene und nicht zugewiesene Sektoren enthalten; ein logischer Export kann nur bestimmte Dateien enthalten; ein Bildschirmfoto kann eine Darstellung ohne Struktur und Metadaten zeigen; ein Ausdruck kann den Inhalt lesbar machen, ohne die Originaldatei bereitzustellen. Keine Darstellung ist allgemein überlegen. Die Auswahl richtet sich nach der Frage und der erforderlichen Überprüfbarkeit. Vernichten Sie das Ausgangsobjekt nicht, um eine Darstellung zu erzeugen, die später unzureichend ist.
Der mexikanische Código de Comercio behandelt in den Artikeln 93 und 93 Bis Schriftform, Original, Integrität und Zugänglichkeit; die Artikel 348 bis 350 des CNPCF erfüllen eine ähnliche Funktion für elektronische Informationen. Diese Vorschriften machen weder jede Kopie zu einem Original noch jede PDF-Datei zu einer vollständigen Quelle. Es muss dokumentiert werden, welche Darstellung vorliegt und wie sie erlangt wurde.[56]

2.2 Integrität, Authentizität, Zurechnung und Wahrheitsgehalt

Integrität bedeutet, dass ein Objekt innerhalb des angegebenen Umfangs vollständig und unverändert bleibt. Authentizität erfordert zu belegen, dass das Objekt tatsächlich das ist, als was es ausgegeben wird. Zurechnung verbindet eine Handlung oder ein Dokument mit einem Ursprung; der Wahrheitsgehalt des Inhalts betrifft die Frage, ob sich das Geschilderte tatsächlich ereignet hat. Eine Verwechslung dieser Begriffe führt zu überzogenen Schlussfolgerungen: Eine Datei kann integer und dennoch von ihrer Erstellung an falsch sein.
Eine gültige Signatur kann im jeweiligen Rechtsregime Urheberschaft und Integrität vermuten lassen, beweist aber weder, dass eine natürliche Person eine bestimmte Schaltfläche betätigt hat, noch, dass alle Aussagen wahr sind. Die Prüfung muss Zertifikat, Gültigkeit, Methode, Kontext und die Möglichkeit kompromittierter Schlüssel sowie eine unabhängige Bestätigung umfassen. Selbst eine kryptografisch korrekte Abfolge kann eine Erläuterung dazu erfordern, wer den Schlüssel und das Gerät zu diesem Zeitpunkt kontrolliert hat.

[5]Código de Comercio de México, Artikel 89–94 und 1205: Neutralität, Zurechnung, Schriftform, Original, Integrität, Zugänglichkeit und Zulassung von Datennachrichten. Amtliche Zusammenstellung.Offizielle Online-Quelle
[6]Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350. Zusammenstellung mit Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von Erklärungen ab.Offizielle Online-Quelle

Belastbare Aussage	Erforderliche Beweise	Zu vermeidende Aussage
Die Hashwerte stimmen überein.	Derselbe Algorithmus, dasselbe Objekt und derselbe Zeitpunkt sind dokumentiert.	Der Inhalt ist wahr.
Die Datei wurde seitdem nicht verändert.	Hashwert bei Entgegennahme berechnet und später überprüft.	Die Datei wurde nie manipuliert.
Der Export enthält diese Felder.	Methode, Parameter und Format des Anbieters.	Der Export ist vollständig.
Im untersuchten Umfang wurde keine Aktivität festgestellt.	Quellen, Filter, Zeitraum und reproduzierbare Abfrage.	Diese Aktivität hat niemals stattgefunden.

2.3 Der Hashwert als Kontrolle, nicht als Dogma

Eine Hashfunktion erzeugt einen Wert, mit dem Objekte verglichen werden können. Weisen zwei Dateien mit demselben Algorithmus denselben Wert auf, stimmt ihr Inhalt im Rahmen dieses Vergleichs bit für bit überein. Verändert sich eine Datei, verändert sich auch der Wert. Dadurch lassen sich Ersetzungen oder Unterschiede erkennen; die Funktion erklärt jedoch nicht deren Ursache und bestätigt weder Herkunft, Datum oder Urheberschaft noch den Wahrheitsgehalt.

Dokumentieren Sie Algorithmus, Bearbeiter, Datum und Zeitzone, das genaue Objekt, den Speicherort und die Beziehung zum Beweismaterial. SHA-256 ist eine verbreitete Option zur Integritätskontrolle, kein Zauberwort. Zwei unterschiedliche Darstellungen derselben Information können verschiedene Werte haben, ohne dass dies Fälschung beweist: Eine Formatkonvertierung kann die Datei verändern, selbst wenn der sichtbare Inhalt ähnlich bleibt. Ein neu berechneter Hashwert belegt die Integrität erst ab dem Zeitpunkt seiner Berechnung.

Korrekte Formulierung für den Bericht
„Die empfangene Datei wies den SHA-256-Wert [Wert] auf, berechnet am [Datum und Zeitzone]. Die spätere Überprüfung ergab denselben Wert. Dies belegt, dass das Objekt zwischen den beiden Prüfungen nicht verändert wurde, nicht jedoch, dass es authentisch ist oder seit seiner Entstehung vollständig ist.“



Abbildung 2. Der Hashwert vergleicht Objekte; er bestätigt weder Urheberschaft noch Wahrheitsgehalt des Inhalts. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

2.4 Interne Metadaten und Systemdaten: eine Unterscheidung, die Fehler vermeidet

Die vom Betriebssystem angezeigten Eigenschaften können angeben, wann eine Datei auf diesem Computer kopiert, heruntergeladen oder geändert wurde, nicht jedoch, wann sie ursprünglich erstellt wurde. Diese Daten sind nicht nutzlos: Sie helfen, die Geschichte dieses Objekts in diesem System zu rekonstruieren. Der Fehler besteht darin, sie ohne weitere Prüfung als ursprüngliches Aufnahmedatum darzustellen. Es muss gelesen werden, was jedes Feld in welchem System und für welche Behauptung bedeutet.

Die internen Metadaten einer Fotografie können Aufnahmedatum, Gerätemodell und Koordinaten enthalten, sofern diese aktiviert waren. Werkzeuge wie ExifTool ermöglichen ihre Lektüre. Dennoch sind sie nicht unveränderlich und beweisen für sich allein nicht, dass sich die Szene wie beschrieben ereignet hat. Eine Datei kann bearbeitet und ihre Metadaten können geändert werden; auch die Uhr eines Geräts kann falsch gehen. Das Aufnahmedatum ist eine Quelle, die mit anderen abgeglichen werden muss: Inhalt, Anwendungsprotokolle, Sicherungskopien, Standorte, Abfolge und Zeugenaussagen.

Die NOM-151 konkretisiert Anforderungen an Aufbewahrung und Digitalisierung in Mexiko. Sie ersetzt weder die Methode des jeweiligen Falls noch bestätigt sie den Wahrheitsgehalt des Inhalts. Die Aufbewahrung muss Zugriffsbedingungen, Integrität, Beziehung zum Original,

verfügbare Metadaten, Verantwortliche sowie etwaige Bescheinigungen oder beteiligte Dritte umfassen. Das sichtbare Datum ist nur der Anfang einer strengeren Frage.[7]

2.5 Der Fall der Fotografien und der Bank

In einem vom Autor analysierten Fall lieferte ein Satz Fotografien Datums- und Koordinatenangaben, die mit einem anderen als dem von der Anklage genannten Ort vereinbar waren. Der Beschleunigungssensor des Telefons zeigte außerdem eine Pause, die zu dem Zeitpunkt passte, als eine Person angab, sich auf eine Bank gesetzt zu haben. Entscheidend war nicht die Bank als Objekt, sondern die Pause: ein alltägliches Muster, das die Prüfung einer Darstellung ohne dramatische Interpretation ermöglichte.

Die Sensoren registrierten weder Trauer noch Absicht und machten aus den Daten keine metaphysische Gewissheit. Sie konnten mit einer Abfolge vereinbar sein, doch die Schlussfolgerung erforderte eine Bestätigung: Fotografien, Nachrichten, Bewegungen, Cloud-Quellen, Zeugenaussagen und die Prüfung, ob die Daten von Sensoren erzeugt oder manuell eingegeben wurden. Die Wissenschaft formuliert nicht „das Mobiltelefon sagte die Wahrheit“, sondern „diese Quellen sind aufgrund ihrer Herkunft und ihres Verhaltens mit dieser Abfolge vereinbar und nicht mit der anderen“.[8]

Methodische Lehre
Eine Quelle wird nicht dadurch wahr, dass sie umfangreich oder technisch ausgefeilt ist. Metadaten helfen, wenn verstanden wird, was sie sind, wann sie erzeugt wurden, welche Veränderungen möglich sind und mit welchen anderen Quellen sie übereinstimmen. Vertrauen entsteht durch Konvergenz, nicht durch Adjektive.

2.6 Zugänglichkeit und Erhaltung des Kontexts

Ein unzugängliches Objekt kann nicht überprüft werden. Die Aufbewahrung erfordert, Informationen öffnen, lesen, interpretieren und ihrem Kontext zuordnen zu können. Für eine proprietäre Datei können eine bestimmte Softwareversion, eine Formatspezifikation oder ein ergänzender Export erforderlich sein. Eine visuelle Kopie erleichtert die Präsentation, darf jedoch nicht anstelle der nativen Datei oder der für die Überprüfung erforderlichen Daten aufbewahrt werden. Ein ansprechender Bericht, der die Quelle nicht auffindbar macht, ist eine Präsentation, keine vollständige Untersuchung.

[7]NOM-151-SCFI-2016, Aufbewahrung und Digitalisierung von Datennachrichten, veröffentlicht am 30-03-2017. Anforderungen an Bescheinigung, Integrität, Zugänglichkeit und digitalen Fingerabdruck.Offizielle Online-Quelle
[8]Jocsan Laguna. Buch für Rechtsanwälte, Kapitel 1. Vom Autor bereitgestelltes narratives Recherchematerial. Namen im Handbuch zum Schutz von Identitäten geändert.



Abbildung 3. Quelle, Export, Arbeitskopie und Ausdruck: Darstellungen mit unterschiedlicher Abdeckung. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Begrenzte Schlussfolgerung
Integrität ist nicht gleich Authentizität, Zurechnung ist nicht gleich physische Identität und ein Datum ist nicht gleich ein Ereignis. Dokumentieren Sie jeden Begriff getrennt, damit ein Kontrollwerkzeug nicht zu einer absoluten Schlussfolgerung wird.

Kapitel 3. Rollen, Verantwortlichkeiten und Entscheidungen

3.1 Funktionen vor Positionsbezeichnungen

Dieselbe Person kann mehrere Funktionen wahrnehmen, sofern der Fall dies zulässt; jede Handlung muss jedoch einer bestimmten Funktion zugeordnet sein. Autorisieren, Ausführen, Dokumentieren, Verwahren, Prüfen und Kommunizieren sind nicht dasselbe. Die Leitung erfasst nicht notwendigerweise selbst Beweise; die Technik entscheidet nicht allein, was veröffentlicht wird; die Rechtsabteilung ersetzt nicht die technische Überprüfung; der Verwahrer verändert die Quelle nicht, um die Analyse zu erleichtern.
Für eine Strafverfolgungsbehörde ermöglicht diese Unterscheidung, dass auch Personal ohne ingenieurtechnische Ausbildung den Fall entgegennehmen und schützen kann, ohne als improvisierter Analyst zu agieren. Die erste einschreitende Person dokumentiert Zustand und Risiko, schützt das Objekt und fordert Unterstützung an. Der Spezialist wählt die Methode auf Grundlage dieser Entgegennahme, nicht auf Grundlage einer unvollständigen telefonischen Beschreibung. Der unabhängige Prüfer prüft unabhängig davon, wer den Bericht vorgelegt hat, ob Behauptung und Beweise zusammenhängen.

Funktion	Hauptverantwortung	Erwartete Dokumentation
Zuständige Stelle für den Auftrag	Legt Umfang, Befugnisse und Ausschlüsse fest.	Autorisierung und genehmigte Änderungen.
Erste einschreitende Person	Erfasst den Zustand, verhindert Verluste und fordert Unterstützung an.	Erstprotokoll und Fotografien.
Spezialist	Wählt die Methode aus und führt sie durch.	Erfassung, Werkzeug und Vorkommnisse.
Verwahrer	Kontrolliert Zugriff, Standort und Übertragungen.	Beweismittelkette.
Prüfer	Prüft Methode, Ergebnisse und Grenzen.	Anmerkungen und Entscheidung.

3.2 Die erste Reaktion ohne Improvisation

Die erste einschreitende Person benötigt keine forensischen Erfassungskenntnisse, um richtig zu handeln. Sie darf Geräte nicht ohne Autorisierung einschalten, durchsuchen oder verbinden; sie muss den Zustand fotografieren, Sichtbares notieren und Unterstützung anfordern. Wurden bereits Dateien geöffnet, wird auch dies dokumentiert und nicht verschwiegen, damit das

Protokoll fehlerfrei erscheint. Die Entgegennahme muss das tatsächliche Vorgeschehen dokumentieren, nicht die Version, die eine ideale Abfolge vortäuscht.
Eine Sichtung kann Orientierung bieten, wird aber nicht durch eine Tabelle, ein Bildschirmfoto oder eine Schlussfolgerung zu einem Gutachten. Der Informatik-Sachverständige muss Methode, Quelle, Werkzeug, Parameter, Überprüfungen und Einschränkungen erläutern. Wenn eine Person ohne diese Fachkenntnis eine Wahrnehmung als wissenschaftliche Analyse darstellt, liegt das Problem nicht im Wortschatz: Es betrifft die methodische Befugnis und die Überprüfbarkeit.



Abbildung 4. Die unabhängige Überprüfung vergleicht Quelle, Methode und Schlussfolgerung; sie korrigiert nicht nur den Stil. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

3.3 Operative Kommunikation

Vor jeder Maßnahme wird festgelegt, wer technische und rechtliche Fragen sowie Fragen zur Verwahrung beantworten kann. Das Verzeichnis enthält Name, Funktion, Kanal, Verfügbarkeit und Vertretung. Dringende Entscheidungen werden mit Datum und Begründung dokumentiert; ein informeller Anruf darf nicht der einzige Nachweis einer unumkehrbaren Handlung sein. Die Kommunikation ist Teil des Entscheidungsnachweises und keine separate administrative Notiz. Wird Material an einen Anbieter übermittelt, wird die Kommunikation in einem rekonstruierbaren Format aufbewahrt. Sendet der Anbieter Dateien per E-Mail, wird die EML-Datei mit Nachrichtentext, Kopfzeilen und Anhängen gespeichert. Wird ein Ausschluss oder ein neuer Export vereinbart, wird dies in die Autorisierung und das Änderungsprotokoll aufgenommen.

Erfolgt die Antwort per Link, werden die Person, die ihn geöffnet hat, ihre Berechtigungen, das Datum und die heruntergeladene Version dokumentiert.

Mindestdokumentation der Kommunikation
Wer hat was von wem angefordert, was wurde autorisiert, über welchen Kanal, mit welchem Datum, welche Änderungen entstanden und welche nachträgliche Überprüfung liegt vor? Die Kommunikation ist kein optionaler Kontext: Sie erklärt, warum eine Entscheidung getroffen wurde.

3.4 Unabhängigkeit, Datenschutz und Dritte

Die unabhängige Prüfung sucht Fehler, nicht Schuldige. Sie prüft, ob das Objekt korrekt ist, ob die Methode dem Auftrag entspricht, ob die Datumsangaben kohärent sind und ob die Schlussfolgerung über die Feststellungen hinausgeht. Der Prüfer kann die Wiederholung einer Abfrage oder die Einbeziehung einer weiteren Quelle verlangen, verändert jedoch nicht das Original, um es an die vorläufige Version anzupassen. Eine Prüfung, die nur bestätigen soll, was der Analyst bereits geschrieben hat, ist nicht unabhängig.
Datenschutz erfordert, den Zweck der Untersuchung von unnötiger Offenlegung zu trennen. Daten Dritter müssen verhältnismäßig, sicher und vertraulich behandelt werden. Der Datenschutzhinweis ist kein rituelles Dokument: Er erläutert, welche Daten zu welchem Zweck verarbeitet werden, wer darauf zugreifen kann und wie Rechte ausgeübt werden. Sind personenbezogene Daten betroffen, muss der Verantwortliche erforderliche und ausreichende Maßnahmen treffen, ohne das Gutachten zu einer öffentlichen Informationsübermittlung zu machen.[9]
Seit 2025 ist die Secretaría Anticorrupción y Buen Gobierno die Bundesbehörde für den Schutz personenbezogener Daten, nicht das INAI. Dieser Wechsel beseitigt die Schutzpflichten nicht und macht nicht jede Untersuchung zu einer Ausnahme: Es muss aktualisiert werden, an wen gegebenenfalls ein Antrag oder eine Beschwerde gerichtet wird, und das historische Institut darf nicht als aktuelle Behörde zitiert werden.[10]

3.5 Ein Syllogismus der Rollen

Obersatz: Ein Gutachten erfordert Fachkenntnis, Methode und Überprüfbarkeit. Untersatz: Eine Sichtung ohne Identifizierung der Quelle, Parameter und Überprüfung bietet keine dieser drei Voraussetzungen. Schlussfolgerung: Der Anschein einer Analyse genügt nicht, um eine Wahrnehmung zu einem Gutachten zu machen. Die Antwort besteht nicht darin, die sichtende Person zu entlassen, sondern die Funktionen richtig zuzuweisen und das nachweisbar zu dokumentieren, was belegt werden kann.

[9]Ley Federal de Protección de Datos Personales en Posesión de los Particulares, neues Gesetz vom 20-03-2025, geändert am 14-11-2025. Artikel 5–9, 18–20 und 31: Grundsätze, Sicherheit, Vertraulichkeit, Verletzungen und Fristen.Offizielle Online-Quelle
[10]Secretaría Anticorrupción y Buen Gobierno. Comunicado 011, 21-03-2025: Übergang der Aufgaben des INAI zum Schutz personenbezogener Daten an das Sekretariat.Offizielle Online-Quelle

Die erste Reaktion kann Zustand und Verwahrung dokumentieren, ohne sich als Analyse auszugeben. Der Spezialist kann anschließend methodisch erfassen. Der Prüfer kann kontrollieren, was getan wurde und was nicht. So wird verhindert, dass aus guter Absicht eine unhaltbare Behauptung entsteht, und jede Person kann das beitragen, was ihre Funktion tatsächlich tragen kann.[11][12]

Begrenzte Schlussfolgerung
Fachkompetenz wird durch Funktion und Methode nachgewiesen, nicht durch eine Positionsbezeichnung. Kann eine Person Quelle, Verfahren und Überprüfung nicht erläutern, muss ihr Beitrag als das bezeichnet werden, was er ist: Entgegennahme, Orientierung oder Sichtung, nicht technisches Gutachten.

[11]ISO/IEC 27037:2012. Leitlinien für Identifizierung, Sammlung, Erfassung und Erhaltung digitaler Beweise. Die Ausgabe wurde von ISO als gültig bestätigt.Offizielle Online-Quelle
[12]Jocsan Laguna. Sinaloa. Entwicklung und Schlussfolgerungen eines technischen Gutachtens zur Informatikforensik. Vom Autor bereitgestelltes Material; Fehler werden verallgemeinert, ohne personenbezogene Daten offenzulegen.

Kapitel 4. Lebenszyklus und forensische Vorbereitung

4.1 Vorbereitung vor der Entgegennahme eines Falls

Forensische Vorbereitung bedeutet zu wissen, welche IT-Assets vorhanden sind, welche Protokolle sie erzeugen, wer sie exportieren kann, wie lange sie aufbewahrt werden und wie Unterstützung angefordert wird. Eine vorbereitete Organisation zeichnet nicht alles für immer auf: Sie bestimmt relevante Quellen, legt eine verhältnismäßige Aufbewahrungsdauer fest und prüft, ob Protokolle mit ihrem Kontext wiederhergestellt werden können. Aufbewahrung ist keine unbegrenzte Ansammlung, sondern die Entscheidung, welche Informationen wie lange benötigt werden können.
Sie hält außerdem Formulare, Notfallzugangsdaten, Anbieterkontakte sowie Verfahren zur Zeitsynchronisation und Beweissicherung bereit. Die erste Reaktion sollte nicht davon abhängen, erst im Internet nachzuschlagen, wie ein Gerät versiegelt wird oder wer ein Konto verwaltet. Der richtige Kontakt, die Notfallautorisierung und eine Protokollkopie müssen bereits vor dem Vorfall vorhanden sein, nicht erst, wenn Protokolle rotieren oder der Zugriff verloren geht.

Mindestvorbereitung	Was geprüft werden muss	Fehler, der vermieden wird
Inventar der IT-Assets und Eigentümer	Verantwortlicher, Quelle, Format und Standort aktuell.	Anfragen an den falschen Verwahrer.
Aufbewahrung und Format	Verfügbarer Zeitraum, Felder, Zeitzone und Exportprozess.	Erst spät festzustellen, dass die Daten nicht mehr existieren oder nicht verstanden werden.
Verzeichnis und Vertretung	Technische und juristische Kontakte, Verwahrer und Anbieter einschließlich Vertretungen.	Abhängigkeit von einer einzigen Person.
Zeitsynchronisation	Zeitquelle, Abweichung und regelmäßige Überprüfung.	Aufbau einer falschen Chronologie durch inkompatible Uhren.
Übungen	Fiktives Beweismaterial, Entgegennahme, Erfassung, Übertragung und Überprüfung.	Improvisation des Verfahrens während der Krise.

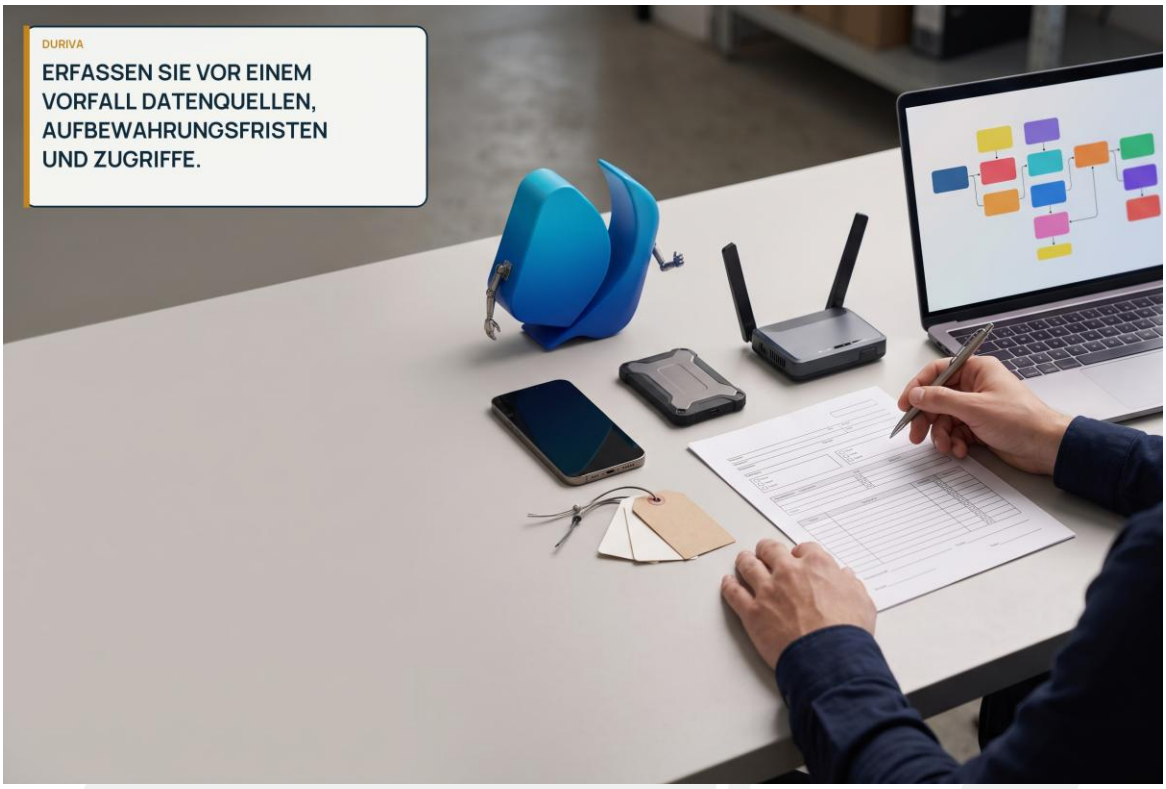


Abbildung 5. Vorbereitung vor dem Vorfall: Inventar der Quellen, Aufbewahrung und Zugriffe. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

4.2 Unumkehrbare Entscheidungen

Bestimmte Handlungen können eine spätere Analyse verhindern: ein Telefon zurücksetzen, das Betriebssystem neu installieren, ohne Schlüsselaufbewahrung verschlüsseln, ein Konto löschen, die Rotation von Protokollen zulassen oder einen Link ersetzen, ohne die frühere Version zu speichern. Bei der Eindämmung müssen diese Folgen bewertet werden; sie darf nicht reflexartig erfolgen. Ausschalten kann einen Zustand erhalten oder Speicherinhalte und Sitzungen vernichten; das Sperren eines Kontos kann Aktivität stoppen oder den Zugriff auf den einzigen verfügbaren Export beseitigen.

Ist eine unumkehrbare Handlung zum Schutz von Personen oder der Betriebskontinuität erforderlich, wird dokumentiert, wer sie autorisiert hat, warum sie unerlässlich war, welche Beweise zuvor gesichert wurden und welche Analysemöglichkeiten verloren gingen. Gute Absichten stellen gelöschte Daten nicht wieder her. Die Eindämmung wird nicht nur an dem vermiedenen Schaden gemessen, sondern auch daran, ob erklärt werden kann, was warum und mit welchem beweisrechtlichen Preis getan wurde.

Dringende Entscheidung	Beweisrisiko	Empfohlene vorherige Maßnahme
Ausschalten oder neu starten	Verlust von Arbeitsspeicherinhalten und Sitzungen.	Live-Erfassung prüfen und Zustand dokumentieren.
Konto sperren	Verlust des Zugriffs auf Protokolle oder Inhalte.	Protokolle exportieren und den Anbieter um Aufbewahrung ersuchen.
Gerät sperren	Mögliche Verschlüsselung oder Fernlöschung.	Schlüssel und autorisierte Zugriffsmethode bestätigen.
Server wechseln	Überschreiben oder Verlust von Protokollen.	Images, Protokolle und Konfiguration sichern.
Link entfernen	Verlust der Version oder des Download-Kanals.	URL, Berechtigungen, Version, Datum und empfangene Datei aufbewahren.



Abbildung 6. Unumkehrbare Entscheidungen: Handlungen, die eine spätere Analyse verhindern können. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

4.3 Dokumentierter Lebenszyklus und Ergebnisse

Der Lebenszyklus umfasst Befugnis, Identifizierung, anfängliche Sicherung, Erfassung, Verwahrung, Untersuchung, Analyse, Bericht und Aufbewahrung. Jede Phase erzeugt ein Ergebnis, das in die nächste eingeht. Fehlt in einer Phase die Dokumentation, erhält die nächste eine Annahme statt einer überprüfbaren Grundlage. Eine Mappe, die nur eine Schlussfolgerung enthält, trägt diese Kette nicht.

ISO/IEC 27037 bietet Orientierung für Identifizierung, Sammlung, Erfassung und Erhaltung; NIST SP 800-86 strukturiert Sammlung, Untersuchung, Analyse und Bericht. Dies sind methodische Referenzen, keine Gesetze oder Garantien der Validität. Das Handbuch überträgt sie in verständliche Handlungen und Formulare, mit denen sich die Arbeit nachweisen lässt, ohne die Methodik zu einer automatischen Bestätigung des Inhalts zu machen.[13][14]

[13]ISO/IEC 27037:2012. Leitlinien für Identifizierung, Sammlung, Erfassung und Erhaltung digitaler Beweise. Die Ausgabe wurde von ISO als gültig bestätigt.Offizielle Online-Quelle

[14]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodischer Leitfaden, weder Rechtsvorschrift noch Garantie für die Zulässigkeit.Offizielle Online-Quelle

Phase	Mindestens erforderliches Ergebnis	Abnahmefrage
Befugnis	Umfang, Befugnisse, Ausschlüsse und Verantwortliche.	Dürfen wir dies mit diesem Ziel und Umfang tun?
Identifizierung	Objekt, Zustand, Verwahrer, Kennungen und Fotografien.	Wissen wir genau, was wir haben und wie es eingegangen ist?
Erfassung	Methode, Werkzeug, Parameter, Ausgabe und Vorkommnisse.	Kann eine andere Person es wiederholen und dem Objekt zuordnen?
Verwahrung	Übertragungen, Zugriffe, Siegel und Überprüfungen.	Können wir rekonstruieren, wer warum zugegriffen hat?
Analyse	Hypothesen, Quellen, Ergebnisse und Alternativen.	Suchen wir auch nach Umständen, die der ersten Version widersprechen?
Bericht und Aufbewahrung	Schlussfolgerung, Einschränkungen, Anhänge und späterer Zugriff.	Kann es künftig geprüft, geöffnet und verstanden werden?

4.4 Aufbewahrung und Longitudinalanalyse

Ein isoliertes Ereignis kann nur deshalb anomal erscheinen, weil die Routine unbekannt ist. Die Aktivität eines Tages muss mit früheren und späteren Zeiträumen verglichen werden, wenn die Frage nach ungewöhnlichem Verhalten, Vorbereitung oder Wiederholung besteht. Ein kurzer Zugriff kann die letzte Stufe einer langen Vorbereitung sein; viele kleine Zugriffe können auf verteiltes Verhalten hindeuten. Die Longitudinalanalyse verhindert, dass eine Momentaufnahme des Vorfalls als vollständige Erklärung der Vergangenheit dient.

Die Aufbewahrung von Protokollen ist weder unbegrenzt noch einheitlich. In Mexiko unterscheidet die Ley en Materia de Telecomunicaciones y Radiodifusión einen ersten Zeitraum von zwölf Monaten in Systemen, die den zuständigen Behörden Abfrage und Übermittlung in Echtzeit ermöglichen, und weitere zwölf Monate in elektronischen Speichersystemen, deren Übermittlung innerhalb von achtundvierzig Stunden nach Mitteilung der Anfrage erfolgt. Entscheidend ist nicht, die Frist auswendig zu lernen, sondern die Quelle

anzufordern, bevor sich Aufbewahrung und Abdeckung auf die Analysemöglichkeiten auswirken.[15]

Entscheidung über die Aufbewahrung
Warten Sie nicht bis zum Ablauf der Mindestaufbewahrungsfrist, um die Protokolle anzufordern. Die gesetzliche Aufbewahrung garantiert weder unbegrenzte Verfügbarkeit noch Abdeckung aller Ereignisse. Sichern Sie frühzeitig, dokumentieren Sie den Zeitraum und vergleichen Sie Muster, bevor Sie etwas als ungewöhnlich bezeichnen.

4.5 Vorbereitung als gesellschaftliche Verantwortung

Vorbereitung verhindert, dass ein Notfall zu einer willkürlichen Entscheidung wird. Eine Organisation, die weiß, wer antwortet, was aufbewahrt wird, wie exportiert wird und was unangetastet bleiben muss, zerstört seltener brauchbare Beweise oder legt Daten Dritter offen. Vorbereitung demokratisiert die Arbeit auch: Die erste einschreitende Person kann methodisch handeln, selbst ohne Ingenieurausbildung, weil Verfahren und Kontakte bereits vorhanden sind.

Begrenzte Schlussfolgerung
Vorbereitung bedeutet nicht, alles aufzuzeichnen, sondern Relevantes mit seinem Kontext wiederherstellen zu können. Fehlt bei einer kritischen Quelle ein Verantwortlicher, eine bekannte Aufbewahrungsfrist, ein dokumentiertes Format oder ein autorisierter Zugriff, muss diese Schwäche vor einem Vorfall behoben werden.

[15]Ley en Materia de Telecomunicaciones y Radiodifusión, veröffentlicht am 16-07-2025. Artikel 182 und 183: Anforderungen und Aufbewahrung von Daten, Abfrage in Echtzeit und Übermittlung innerhalb von 48 Stunden je nach Abschnitt. Offizielle Online-Quelle

Kapitel 5. Entscheidungsbäume nach Szenario

5.1 Ein- oder ausgeschaltetes Gerät

Ein eingeschaltetes Gerät kann flüchtige Speicherinhalte, Sitzungen, Schlüssel, Verbindungen und Prozesse enthalten, die beim Ausschalten verloren gehen. Es kann außerdem während der Beobachtung weiter Daten verändern. Ein ausgeschaltetes Gerät kann für die Image-Erstellung stabiler sein, doch Verschlüsselung und Ruhezustand verändern die Optionen. Die Entscheidung richtet sich nach der Fragestellung und den verfügbaren Fähigkeiten, nicht nach überkommener Gewohnheit.

Es gibt weder eine allgemeine Regel, immer auszuschalten, noch einen Grund, das Gerät aus Verunsicherung eingeschaltet zu lassen. Dokumentieren Sie Zustand, sichtbare Aktivität, bekannte Verschlüsselung, Verbindungen, Befugnisse und den Bedarf an Speicherinhalten. Fehlt die Fähigkeit zu einer sicheren Live-Erfassung, dokumentieren Sie dies und fordern Unterstützung an, bevor Sie den Zustand ändern. Die erste Entscheidung ist nicht die Wahl eines Werkzeugs: Sie müssen verstehen, was mit jeder Option verloren geht.

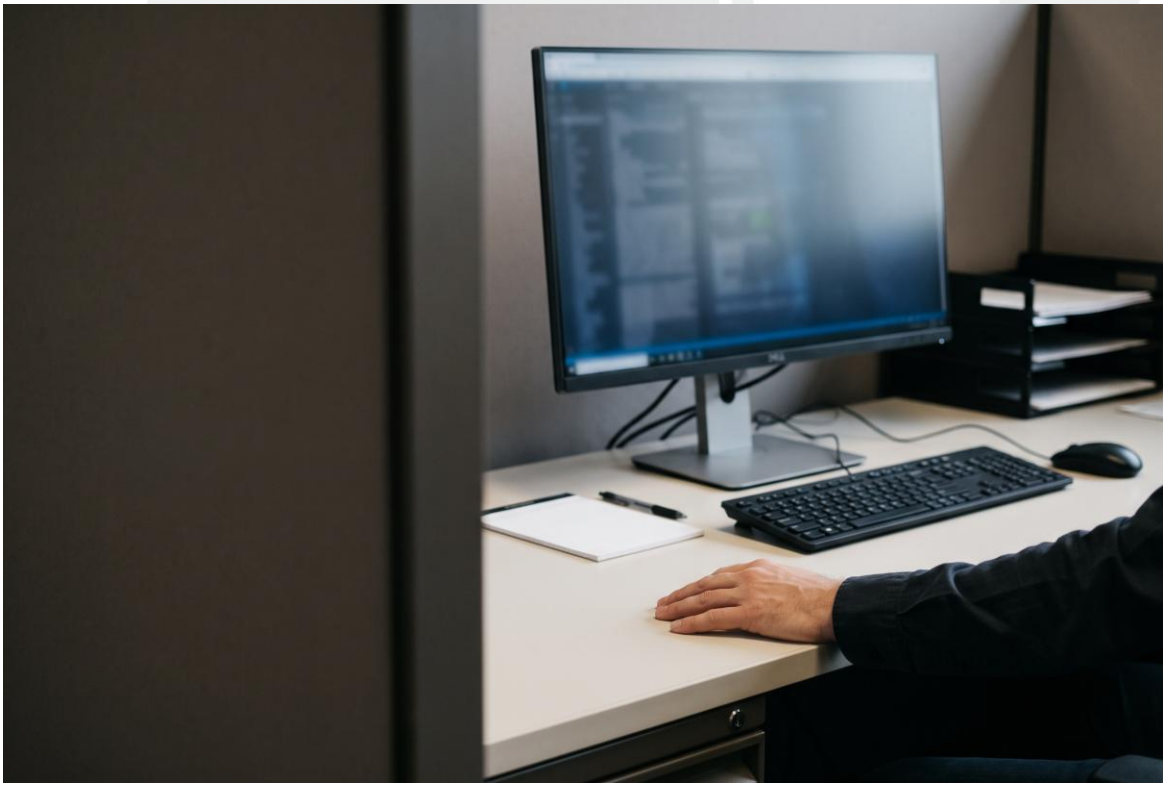


Abbildung 7. Eingeschaltetes Gerät: Zustand und Aktivität vor der Entscheidung dokumentieren. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

5.2 Lokale, entfernte oder anbieterseitige Erfassung

Die lokale Erfassung ermöglicht, Gerät und Kontext zu beobachten, ist jedoch nicht immer die beste Quelle. Ein administrativer Export kann Ereignisse enthalten, die das Gerät nicht speichert oder die lokal bereits gelöscht wurden. Bei einer entfernten Erfassung müssen Identität der ausführenden Person, Parameter, Datum, Zeitzone, Format und Übertragungskanal dokumentiert werden. Die Frage ist nicht, wo die sichtbare Datei liegt, sondern welche Quelle die größte Abdeckung bei der geringsten Veränderung bietet.
Vom Anbieter wird die geeignete Quelle angefordert, nicht „alle Informationen“. Die Anfrage grenzt Zeitraum, Konto, Felder, Format, Bedeutung der Spalten und Erzeugungsprozess ein. Bei einem offiziellen Portal wird dokumentiert, wer es mit welcher Rolle und welchen Filtern verwendet. Liefert der Anbieter eine Datei ohne Erklärung ihrer Erstellung, wird diese Einschränkung schriftlich festgehalten. Eine native Datei des Anbieters kann besseres Beweismaterial sein als ein Ausdruck derselben Datei durch eine andere Person.

Bedingung	Bevorzugter Weg	Unverzichtbare Dokumentation
Erforderliche Speicherinhalte oder Sitzungen	Live-Erfassung, sofern autorisiert und validiert.	Zustand, Prozess, Ausgabe, Uhrzeit und unvermeidliche Veränderung.
Gerät ausgeschaltet und stabil	Image oder logische Erfassung je nach Ziel.	Quelle, Verbindung, Methode, Abdeckung und Vorkommnisse.
Ereignisse auf einer Plattform oder bei Dritten	Administrativer Export oder Anbieter.	Rolle, Filter, Zeitzone, Format, Felder und EML-Übermittlung.
Eingeschränkter Zugriff oder nicht validiertes Werkzeug	Aussetzen und weiterleiten, ohne den Zustand zu verändern.	Grund, Zustand, Risiko und nächster Verantwortlicher.

5.3 Mobilgeräte und Isolation

Bei einem Telefon werden Betriebszustand, Sperrung, Verschlüsselung, Netzwerk, Synchronisation, Fernlöschung und Akkuzustand bewertet. Eine Isolierung kann entfernte Änderungen verhindern, aber auch eine rechtmäßige Erfassung verhindern oder Sperrungen auslösen. Das Entfernen des Akkus ist keine allgemeingültige Anweisung; viele Geräte lassen dies ohne Schaden oder Veränderung nicht zu. Konnektivität kann für den Export oder die Sicherung eines Kontos erforderlich sein, daher ist Isolierung nicht immer die erste Maßnahme.

Die Isolierungslösung muss tatsächlich wirksam und überprüft sein. Eine antistatische Tasche ist kein Faradayscher Käfig. Dokumentieren Sie die verwendete Technik, ihre Überprüfung, verbleibende aktive Verbindungen und akzeptierte Risiken. Fehlen die Voraussetzungen für eine sichere Entscheidung, bewahren Sie den Zustand und leiten den Fall weiter. Die Kennzeichnung „Faraday“ genügt nicht, wenn das Verpackungsmaterial die Funktion nicht erfüllt oder seine Wirksamkeit im konkreten Szenario nicht nachgewiesen wird.



Abbildung 8. Antistatik und Hochfrequenzabschirmung sind nicht dieselbe Funktion. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

5.4 Optische Datenträger: Kennung und Format

Ein optischer Datenträger erfordert eine genaue Identifizierung. Es genügt nicht, „eine CD“ oder „eine DVD“ zu vermerken, wenn Kennzeichnung, Begleitschreiben und Sichtung nicht übereinstimmen. Dokumentiert werden Trägertyp, gegebenenfalls Marke und Modell, Kapazität, Zustand, verfügbare Lesegeräte und alle sichtbaren Kennungen. Der Zentralring kann einen Code oder eine Herstellerkennung enthalten; er wird ohne Berührung der Datenoberfläche geprüft und mit Kontext fotografiert.

Nicht jeder Datenträger weist dieselbe eindeutige Kennung auf, und nicht jeder sichtbare Code ist eine beweiskräftige Seriennummer. Der Zentralring ist zu prüfen und sein Inhalt genau zu dokumentieren, ohne eine fehlende Kennung zu erfinden. Wiederbeschreibbare und nur lesbare Träger sind ebenfalls zu unterscheiden: Eine DVD-RW ist keine rein ästhetische

Variante, denn sie verändert die Möglichkeiten des Überschreibens und muss als solche dokumentiert werden.



Abbildung 9. Prüfung des Zentralrings: Kennungen und Codes, die den Datenträger identifizieren können. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Kennung vor Schlussfolgerung
Wenn Sie den Datenträger nicht identifizieren können, können Sie nicht behaupten, das richtige Objekt analysiert zu haben. Pseudo-Verwahrung beginnt mit „da ist ein Datenträger“; Verwahrung beginnt mit Kennungen, Zustand, Format, Fotografien und Bezug zum Protokoll.

5.5 Wann die Arbeit auszusetzen ist

Auch das Aussetzen ist eine fachliche Entscheidung. Fehlende Befugnisse, Risiken für Personen, unmögliche Beweissicherung, fehlende validierte Werkzeuge oder die Gefahr einer Beweisvernichtung erfordern eine Pause und eine Weiterleitung. Weiterzumachen, nur um „zu sehen, ob etwas auftaucht“, kann mehr Schaden als Erkenntnisgewinn verursachen. Der dokumentierte Abbruch ist kein Misserfolg: Er erhält Analysemöglichkeiten und verhindert nicht vertretbare Handlungen.

Das Protokoll des Abbruchs enthält den Grund, den verbleibenden Zustand des Objekts, frühere Handlungen, erkannte Risiken und den nächsten Verantwortlichen. Wird die Unklarheit

später aufgelöst, werden die antwortende Person und die Methode ergänzt. Die Pause schreibt die Vergangenheit nicht um: Sie erklärt, warum keine Verschlechterung des Falls gewählt wurde.

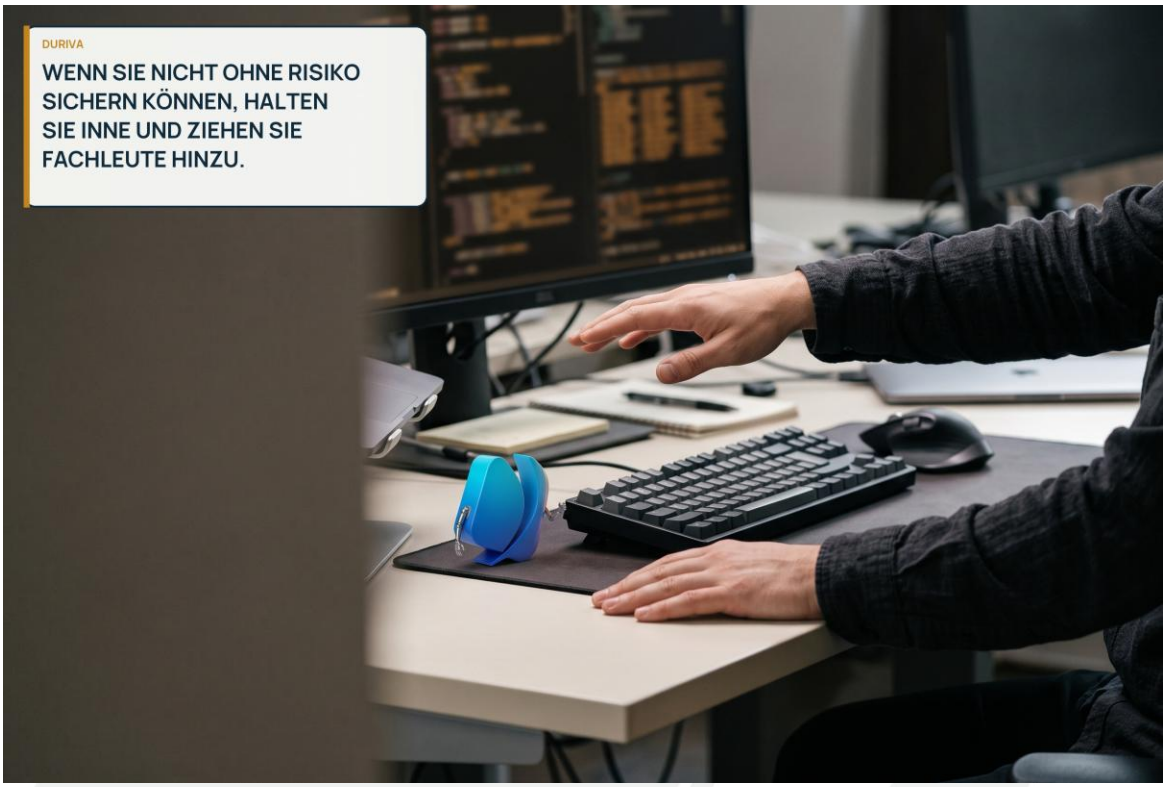


Abbildung 10. Aussetzen und weiterleiten: Wenn Fortfahren mehr Beweise vernichtet als einbringt. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Sicherheitsregel
Führen Sie unbekannte Dateien nicht auf persönlichen Geräten oder in Produktionsnetzen aus. Verwenden Sie eine isolierte Umgebung und kontrollierte Kopien mit Autorisierung und definiertem Ziel. Neugier rechtfertigt keine Gefährdung Dritter.

5.6 Der Baum als Argumentation, nicht als Dekoration

Ein Entscheidungsbaum ist nützlich, wenn er Eingangsbedingungen, Handlungen und Dokumentation verlangt, nicht wenn er nur eine Abfolge von Symbolen zeigt, die niemand befolgt. Jeder Zweig muss mit einer begründeten Maßnahme, ihrer Begründung und einem Protokoll enden. Ändert sich die Bedingung, ändert sich der Weg. Ein verschlüsseltes Gerät, ein verbundenes Telefon oder ein Anbieter mit einem besseren Export dürfen nicht standardmäßig zum selben Vorgang führen.

Begrenzte Schlussfolgerung
Der richtige Weg hängt von Zustand, Ziel, Befugnis und Risiko ab. Wird eine Entscheidung nur mit Gewohnheit begründet, ist der Baum falsch aufgebaut oder angewendet. Die Bedingung, die zu einem Weg geführt hat, ist ebenso wichtig zu dokumentieren wie die abschließende Handlung.

Kapitel 6. Moderne Quellen und Gesprächsdatensätze

6.1 Cloud, SaaS und Exporte

Die Benutzeransicht ist nur eine Ebene. Eine Plattform kann Versionsverläufe, Zugriffsprotokolle, Rollen, Token, IP-Adressen, administrative Aktivitäten, freigegebene Links, Benachrichtigungen und Sicherungskopien auf weiteren Ebenen enthalten. Beim Export müssen die erstellende Person, ihre Rolle, Filter, Zeitzone, Format, Zeitraum und Einschränkungen angegeben werden. Das Herunterladen einer Oberfläche entspricht nicht der Erfassung des vollständigen Kontoverlaufs.

Ein PDF-Download kann zum Lesen nützlich sein, reicht jedoch nicht zur Analyse von Struktur und Metadaten aus. Fordern Sie verfügbare native Formate zusammen mit der Dokumentation der Felder und des Erzeugungsprozesses an. Wenn die Plattform eine API anbietet, dokumentieren Sie Endpunkt, Version, Parameter, Paginierung, Grenzen und Antwort, ohne Geheimnisse in den Bericht aufzunehmen. Die Ausgabe muss nachvollziehen lassen, welche Abfrage mit welcher Abdeckung ausgeführt wurde.



Abbildung 11. Export durch Anbieter oder API: Filter, Felder, Zeitzone, Format und Übermittlung. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

6.2 E-Mail und EML

Die EML-Datei bewahrt Nachrichtentext, Anhänge und Kopfzeilen, die ein Bildschirmfoto nicht vollständig erfasst. Dies ist besonders wichtig, wenn der Nachrichtentext eine Referenz, eine Erläuterung der Felder oder einen Hashwert für die Anhänge enthält. Anhand der EML-Datei lässt sich prüfen, was bei der Übermittlung erklärt wurde, und jede Datei dieser Erklärung zuordnen. Werden nur die Anhänge gespeichert, geht die Verbindung zwischen Datei und Integritätserklärung verloren.

Bewahren Sie die ursprüngliche Nachricht und dokumentieren Sie ihre Beschaffung: Export aus dem Client, Download vom Server oder Übermittlung durch eine andere Person. Berechnen Sie Hashwerte der EML-Datei und der Anhänge getrennt und dokumentieren Sie deren Beziehung. Die EML-Datei belegt den Inhalt der empfangenen Nachricht, jedoch weder die Wahrheit aller Angaben des Absenders noch die physische Identität des Absenders. Die Authentizität des Kanals wird anhand von Kopfzeilen, Server und Kontext geprüft, nicht anhand eines Bildschirmfotos des Postfachs.

Objekte nicht verwechseln
Der Hashwert der EML-Datei ist nicht der Hashwert des Anhangs, und der Hashwert des Anhangs ist nicht der Hashwert des Systems, das die Daten erzeugt hat. Jeder Wert bezieht sich auf ein anderes Objekt und muss mit Name, Algorithmus, Datum und Beziehung dokumentiert werden.



Abbildung 12. Die EML-Datei bewahrt Nachrichtentext, Kopfzeilen und Anhänge; ein Bildschirmfoto ersetzt sie nicht. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

6.3 Anforderung und Entgegennahme von Gesprächsdatensätzen

Eine Gesprächsdatenliste ist ein Export von Telekommunikationsprotokollen. Für ihre Interpretation genügt keine Tabelle mit Nummern: Erforderlich sind Zeitraum, Zeitzone, Ereignistyp, Richtung, Dauer, Kennungen, Funkzellen, Technologie, leere Felder und Extraktionsmethode. Die Anfrage muss verfügbare native Formate, eine Dokumentation der Spalten und einen Nachweis des Systems umfassen, das die Datei erzeugt hat.

Im Nachrichtentext der Übermittlungs-E-Mail muss der Anbieter für jede gelieferte Datei den entsprechenden Hashwert und den verwendeten Algorithmus angeben. Dieser Wert ermöglicht zu prüfen, ob der empfangene Anhang mit der Datei übereinstimmt, auf die sich der Anbieter bezieht. Außerdem muss die EML-Datei mit diesem Nachrichtentext, den Kopfzeilen und den Anhängen vorgelegt und aufbewahrt werden. Es genügt nicht, den Hashwert in eine separate Notiz zu kopieren oder nur die Tabelle zu speichern.

Bei der Entgegennahme wird geprüft, ob der Wert im Nachrichtentext mit dem Anhang übereinstimmt. Bei Übereinstimmung wird dies dokumentiert; bei Abweichung wird die Differenz registriert und eine Klärung angefordert, ohne die Datei zu bearbeiten. Liefert der Anbieter keinen Hashwert, wird dies vermerkt und bei Empfang ein eigener Wert berechnet; dieser belegt die Integrität erst ab diesem Zeitpunkt. Kein Hashwert beweist für sich allein die Wahrheit der Anrufe oder die Identität der Person, die das Telefon benutzt hat.

Element der Anfrage	Was vom Anbieter angefordert wird	Was bei Empfang geprüft wird
Zeitraum und Zeitzone	Beginn, Ende, Zeitzone und Sommerzeit.	Ereignisse innerhalb des Zeitraums und kohärente Konversionen.
Format und Felder	Verfügbare Formate CSV/XLSX/PDF, Feldverzeichnis und Extraktionsprozess.	Native Datei, Spalten, Leerfelder und Einheiten.
Integrität	Hashwert jeder Datei und Algorithmus im Nachrichtentext.	Lokale Berechnung und dokumentierte Übereinstimmung oder Abweichung.
Übermittlung	EML-Datei mit Nachrichtentext, Kopfzeilen und Anhängen.	Vollständige EML-Datei und zugehörige Dateien, ohne die Objekte zu trennen.
Kontext	Netzwerktyp, Ereignisse, Roaming, Funkzellen und verfügbare Kennungen.	Was aus jedem Feld abgeleitet werden kann und was nicht.

6.4 Beispiel für den Text einer Anbieteranfrage

Das folgende fiktive Beispiel kann angepasst werden, ohne sensible Daten über einen gewöhnlichen Kanal zu übermitteln. Autorisierung und Fallakte werden über den entsprechenden sicheren Kanal gesendet. Ziel ist eine Antwort mit ausreichendem Kontext für die Analyse und mit Objekten, deren Integrität überprüft werden kann.

Beispiel für eine Anfrage
Betreff: EXP-DEMO-2026-001 · Anforderung von Protokollen und Integritätsnachweis

Sehr geehrtes Verwahrungsteam,

Über den bereits autorisierten sicheren Kanal bitte ich um die Protokolle vom 1. bis 3. November 2026 mit ausdrücklicher Angabe der Zeitzone und der geltenden Sommerzeit. Bitte fügen Sie, sofern verfügbar, Datum und Startzeit, Dauer, Ereignistyp, Richtung, Kennungen von Leitung und Gerät, Funkzelle, Technologie sowie eine Erklärung leerer Felder bei.

Ich bitte um die Dateien im verfügbaren nativen Format (CSV und/oder XLSX), eine PDF-Lesekopie, das Feldverzeichnis und eine Beschreibung des Extraktionsprozesses und des Extraktionsdatums. Bitte geben Sie für jede Datei im Nachrichtentext den Algorithmus und den zugehörigen Hashwert an.

Bei der Übermittlung muss diese E-Mail im EML-Format mit Nachrichtentext, Kopfzeilen und Anhängen aufbewahrt werden. Einschränkungen von Format, Aufbewahrung oder Abdeckung sind ausdrücklich anzugeben.

Mit freundlichen Grüßen
Autorisierter technischer Verantwortlicher · EXP-DEMO-2026-001

6.5 Virtualisierung, IoT und synthetische Inhalte

Bei der Virtualisierung werden Host, Gastsystem, Snapshots, gemeinsam genutzter Speicher und Verwaltungsprotokolle unterschieden. Bei IoT werden Gerät, Anwendung, Hub, Cloud, Firmware und Synchronisation getrennt betrachtet. Die Anzeige von Daten auf einem Bildschirm sagt nichts darüber aus, wo sie erzeugt wurden oder wie viele Kopien existieren. Bei der Erfassung muss die Ebene benannt werden, nicht nur das Produkt: Eine Kamera ist nicht das gesamte Beweismaterial und ein Router nicht das gesamte Netzwerk.



Abbildung 13. Virtualisierung: Host, Gastsysteme, Snapshots und gemeinsam genutzter Speicher. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Bei KI-generierten oder KI-manipulierten Inhalten werden Erstellung, Bearbeitung, Konvertierung und Veröffentlichung getrennt betrachtet. Original, Verlauf, Werkzeug und Version werden, sofern verfügbar, zusammen mit Autorisierungen und menschlicher Prüfung aufbewahrt. Ein Detektor liefert Hinweise, kein Urteil. Die juristische Analyse prüft Einwilligung, Identität, Verhalten, Nutzung und Gültigkeit; sie macht „KI“ nicht zu einem allgemeingültigen Straftatbestand.

Die Artikel 199 Octies und 199 Nonies des mexikanischen Bundesstrafgesetzbuchs regeln bestimmte Verhaltensweisen im Zusammenhang mit intimen sexuellen Inhalten ohne Einwilligung, einschließlich des Falls, dass das Material nicht der identifizierten Person entspricht. Artikel 50 der europäischen KI-Verordnung behandelt die Transparenz von Deepfakes und passt bestimmte Pflichten für kreative Werke und redaktionelle Prüfung an. Es handelt sich um unterschiedliche Rechtsregime, die nicht zu einem angeblichen weltweiten KI-Verbot vermischt werden dürfen.[16][17]

[16]Mexiko. Código Penal Federal, Artikel 199 Octies und 199 Nonies, Zusammenstellung mit Reform vom 13-03-2026: bestimmte Verhaltensweisen mit intimen sexuellen Inhalten ohne Einwilligung, auch wenn das Material nicht der identifizierten Person entspricht.Offizielle Online-Quelle

[17]Reglamento (UE) 2024/1689 de inteligencia artificial, Artikel 50, konsolidierter Text vom 27-07-2026: Transparenz bestimmter Deepfakes und Anpassung für kreative, satirische, künstlerische oder fiktive Werke.Offizielle Online-Quelle

6.6 Gültigkeit: das Beispiel einer aufgehobenen Reform

San Luis Potosí zeigt, warum die Gültigkeit geprüft werden muss: Die im November 2025 verabschiedete Reform führte besondere KI-bezogene Straftatbestände ein, doch die Artikel 187 Ter, 272 Bis und 272 Ter wurden am 30. Juli 2026 aufgehoben. Das Beispiel dient nur als lokaler historischer Hinweis, nicht als allgemeingültige Regel oder allgemeine Autorisierung. Das Verhalten muss anhand der geltenden Vorschrift und weiterer möglicherweise anwendbarer Tatbestände analysiert werden.[18]

Aktualisierungsregel
Eine Quellenangabe enthält Rechtsinstrument, Artikel, Funktion, Version und offizielle Quelle. Ein Gesetz wird nicht wegen eines ähnlichen Namens zitiert und ein Gesetzesvorhaben nicht als Dekret dargestellt. Die vergleichende Entsprechung beschränkt sich auf Funktion und Umfang und impliziert nicht dieselben prozessualen Wirkungen.

[18]San Luis Potosí. Gaceta Parlamentaria, 30-07-2026: Aufhebung von 187 Ter und des Kapitels mit 272 Bis und 272 Ter. Historischer Hintergrund, keine geltende Regel.Offizielle Online-Quelle

6.7 Die Quelle befindet sich nicht an einem Ort



Abbildung 14. Gerät, Anwendung, Konto und Anbieter: Ebenen moderner Beweismaterialien. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Begrenzte Schlussfolgerung
Die Benutzeransicht erschöpft die Quelle nicht. Der geeignete Export kann sich beim Anbieter, in einer Cloud, in einem Versionsverlauf oder in einer Übermittlungs-E-Mail befinden. Bestimmen Sie die Ebene und bewahren Sie ihren Kontext, bevor Sie den Inhalt analysieren.

Kapitel 7. Entgegennahme und anfängliche Sicherung

7.1 Nachvollziehbares Entgegennahmeprotokoll

Das Protokoll dokumentiert, was auf welchem Weg von wem übergeben wurde, wer es wann, wo und in welchem Zustand entgegengenommen hat. Es enthält verfügbare Kennungen, Zubehör, Siegel, Fotografien und Anmerkungen. Es genügt nicht, „ein Computer“ oder „ein USB-Stick“ zu vermerken: Marke, Modell, gegebenenfalls Seriennummer, Kapazität, physischer Zustand und vorhandene Kennzeichnungen werden dokumentiert. Bei einem Datenträger werden Trägertyp, Kapazität, Format und, sofern sichtbar, der Code des Zentralrings angegeben.

Die erste einschreitende Person benötigt keine forensischen Erfassungskenntnisse, um richtig zu handeln. Sie darf Geräte nicht ohne Autorisierung einschalten, durchsuchen oder verbinden; sie muss den Zustand fotografieren, Sichtbares notieren und Unterstützung anfordern. Wurden bereits Dateien geöffnet, wird auch dies dokumentiert und nicht verschwiegen, damit das Protokoll fehlerfrei erscheint. Ziel ist nicht, eine fehlerfreie Entgegennahme zu erfinden, sondern die Ausgangsbedingungen zu dokumentieren.

Feld	Was es enthalten muss	Fiktives Beispiel
Objekt und Kennung	Typ, Marke, Modell, Seriennummer, Kapazität und zugewiesener Code.	SSD, 2,5 Zoll, 512 GB, Serie demo-003.
Übergabe und Entgegennahme	Name, Funktion, Datum, Uhrzeit, Zeitzone und Ort.	Verwahrer A übergibt an Analyst B, 09. November, 14:32 −06.
Zustand	Betriebszustand, Sperrung, Netzwerk, Schäden und Zubehör.	Ausgeschaltet, kein sichtbarer Schaden, SATA-Kabel und Netzteil.
Siegel und Verpackung	Typ, Kennung, Zustand und Fotografien.	Siegel 01 intakt, starre Box und antistatische Tasche.
Frühere Handlungen	Öffnungen, Verbindungen, Kopien, Änderungen oder Unbekanntes.	Es ist unbekannt, ob das Gerät vor der Übergabe eingeschaltet wurde.
Erste Entscheidung	Sicherung, Weiterleitung, Erfassung oder Klärung sowie Verantwortlicher.	Zustand sichern und Spezialisten anfordern.



Abbildung 15. Fotografieren Sie den Ausgangszustand des Objekts und seines Zubehörs vor der Analyse. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

7.2 Verpackung und Versiegelung

Die Verpackung schützt vor physischen und elektrostatischen Schäden, Feuchtigkeit, unbefugtem Zugriff und Austausch. Sie wird nach Objekt und Zustand ausgewählt. Das Siegel enthält Kennung, Datum und Verantwortlichen und ist so beschaffen, dass eine Öffnung erkennbar wird. Muss es zur Bearbeitung geöffnet werden, wird dies dokumentiert und das Siegel nach Verfahren erneuert, ohne den Verlauf zu löschen. Öffnen und Erneuern sind Ereignisse der Verwahrung, keine Randnotiz.

Antistatik und Hochfrequenzabschirmung sind nicht gleichbedeutend. Erstere schützt Bauteile vor Entladungen; letztere soll drahtlose Kommunikation verhindern und muss validiert werden. Eine korrekte Verpackung korrigiert keine frühere Fehlentscheidung, verhindert jedoch weitere Veränderungen und ermöglicht zu rekonstruieren, wer auf das Objekt zugegriffen hat. Das Material wird nach der für das Beweismaterial erforderlichen Funktion ausgewählt, nicht nach dem professionellen Aussehen des Behälters.



Abbildung 16. Entgegennahme und Verpackung: physischer Schutz, Siegel, Kennzeichnung und Beziehung zwischen Objekten. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

7.3 Kennzeichnung und Beziehung zwischen Objekten

Jedes Objekt erhält eine stabile Kennung ohne Kundennamen. Abgeleitete Objekte werden über ein Herkunftsfeld mit dem Original verknüpft. Die Kennung wird nicht für einen anderen Export wiederverwendet: Es wird ein verknüpftes Objekt mit eigenem Datum, eigener Methode und eigenem Hashwert erstellt. Dadurch werden nicht Dateien verglichen, die lediglich denselben Namen tragen. Die physische Kennzeichnung und das Protokoll müssen mit dem digitalen Inventar und dem abschließenden Bericht übereinstimmen.

Eine mögliche Konvention ist ED-AAAAMMDD-CASO-FUENTE-SECUENCIA-VERSION. Wenn die Organisation bereits eine andere Konvention verwendet, wird diese beibehalten, sofern sie eindeutig und konsistent ist. Die Kennung ersetzt nicht das Originalobjekt: Ein anderer Export derselben Quelle erhält eine verwandte Kennung und einen Beziehungshinweis. Die Kennung muss das Auffinden ermöglichen, ohne Kunde, Inhaber oder sensible Informationen offenzulegen.

Fiktives Beispiel einer Kennung
ED-20261109-DEMO-MBL-003-A00

ED = digitale Beweise
20261109 = Entgegennahme

DEMO = fiktiver Fall
MBL = mobile Quelle
003 = drittes Objekt
A00 = anfängliche Erfassung



Abbildung 17. Objekt, Zustand, Datum, Verwahrer und Kennung kennzeichnen. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

7.4 Zubehör und Verbindungen als Teil der Entgegennahme

Ein Kabel, ein Adapter, eine SIM-Karte, eine SD-Karte oder ein Netzteil kann erklären, wie auf Informationen zugegriffen wurde oder welche Verbindungen möglich waren. Diese Elemente werden als verwandte Objekte erfasst, nicht als unsichtbares Zubehör. Fotografieren Sie nur das Telefon, kann Beweismaterial fehlen, das für die Erfassung oder Interpretation der Daten erforderlich ist. Das Inventar muss jedes empfangene Element und seine Beziehung zum Hauptgerät enthalten.



Abbildung 18. Zubehör und Verbindungen: Teil der Entgegennahme und der Erfassungsmöglichkeiten. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

7.5 Entgegennahme von Dateien und Nachrichten

Bei der digitalen Entgegennahme werden Herkunft, Kanal, Datum, mutmaßlicher Absender, Empfänger, Namen, Größen und Formate dokumentiert. Die Dateien werden unverändert gespeichert und ihre Hashwerte bei Eingang berechnet. Liefert der Anbieter Werte im Nachrichtentext, werden diese geprüft und die EML-Datei aufbewahrt. Bei einer Übermittlung per Link werden die Person, die ihn geöffnet hat, Berechtigungen, Download-Datum und Version dokumentiert. Der Download ist ein Entgegennahmeereignis, keine unsichtbare Handlung.

Der ursprüngliche Dateiname wird vor der Sicherung niemals zur „Sortierung“ geändert. Die Beziehung zwischen Original und Arbeitskopie wird im Manifest dokumentiert. Wurde die Datei zuvor von einer anderen Person umbenannt oder konvertiert, wird dieser Verlauf vermerkt und alle verfügbaren Versionen werden aufbewahrt. Ordnung wird durch das Inventar geschaffen, nicht durch Verändern des empfangenen Objekts.

Begrenzte Schlussfolgerung
Die Entgegennahme ist die erste Bewährungsprobe der Methode. Wenn Objekt, Zustand, Kennungen und frühere Handlungen nicht klar sind, beginnt jede spätere Behauptung mit einer vermeidbaren Unsicherheit.

Kapitel 8. Erfassung und technische Dokumentation

8.1 Physische, logische, flüchtige und dokumentarische Erfassung

Die physische Erfassung kopiert das gesamte Medium und kann nicht zugewiesenen Speicherplatz umfassen; die logische Erfassung erhält ausgewählte Dateien oder Quellen. Die flüchtige Erfassung sammelt Speicherinhalte und temporäre Zustände, sofern dies gerechtfertigt ist. Die dokumentarische Erfassung hält eine Darstellung fest, wenn die anderen Methoden nicht verfügbar sind, ohne ihr alle Eigenschaften des Originals zuzuschreiben. Jede Methode beantwortet eine andere Anforderung und erzeugt andere Einschränkungen.
Die Auswahl richtet sich nach der Fragestellung, nicht nach dem Ansehen des Werkzeugs. Zur Rekonstruktion gelöschter Aktivitäten kann ein Image geeignet sein; für Protokolle einer Plattform kann ein offizieller Export genügen. Die Methode wird mit Voraussetzungen, Befugnis, Werkzeug, Version, Parametern, Ausgabe und Fehlern beschrieben. Der Ausdruck „forensische Erfassung“ beschreibt für sich allein weder die durchgeführten Handlungen noch ihre Abdeckung.

Methode	Wann sie geeignet sein kann	Anzugebende Einschränkung
Physisches Image	Das gesamte Medium einschließlich nicht zugewiesenem Speicherplatz wird benötigt.	Keine Garantie für die Analyse jeder Datei oder Plattform.
Logische Erfassung	Ausgewählte Dateien oder Quellen werden benötigt.	Auswahl und Filter bestimmen die Abdeckung.
Flüchtige Speicherinhalte	Sitzungen, Schlüssel, Prozesse oder temporäre Zustände sind relevant.	Begründung, Befugnis und möglicher Verlust durch Zustandsänderung.
Offizieller Export	Die beste Quelle befindet sich beim Anbieter oder auf der Plattform.	Parameter, Format und Abdeckung des Anbieters.
Dokumentarisch	Keine andere Darstellung ist verfügbar und die Visualisierung muss dokumentiert werden.	Sie bewahrt nicht alle Eigenschaften des Originals.

8.2 Tatsächliche Verbindung: Quelle, Schreibblocker und Arbeitsstation

Schreibblocker und andere Schutzmaßnahmen werden bei Bedarf eingesetzt, gelten jedoch nicht als absolute Garantie. Dokumentiert wird der tatsächliche Ablauf: Gerät, Verbindung,

Zustand, Fehler und Überprüfung. Die Quelle wird mit dem Schreibblocker und die Arbeitsstation mit dem anderen Ende verbunden. Die Konfiguration muss dem tatsächlichen Vorgehen entsprechen, nicht dem idealen Bild eines Handbuchs.

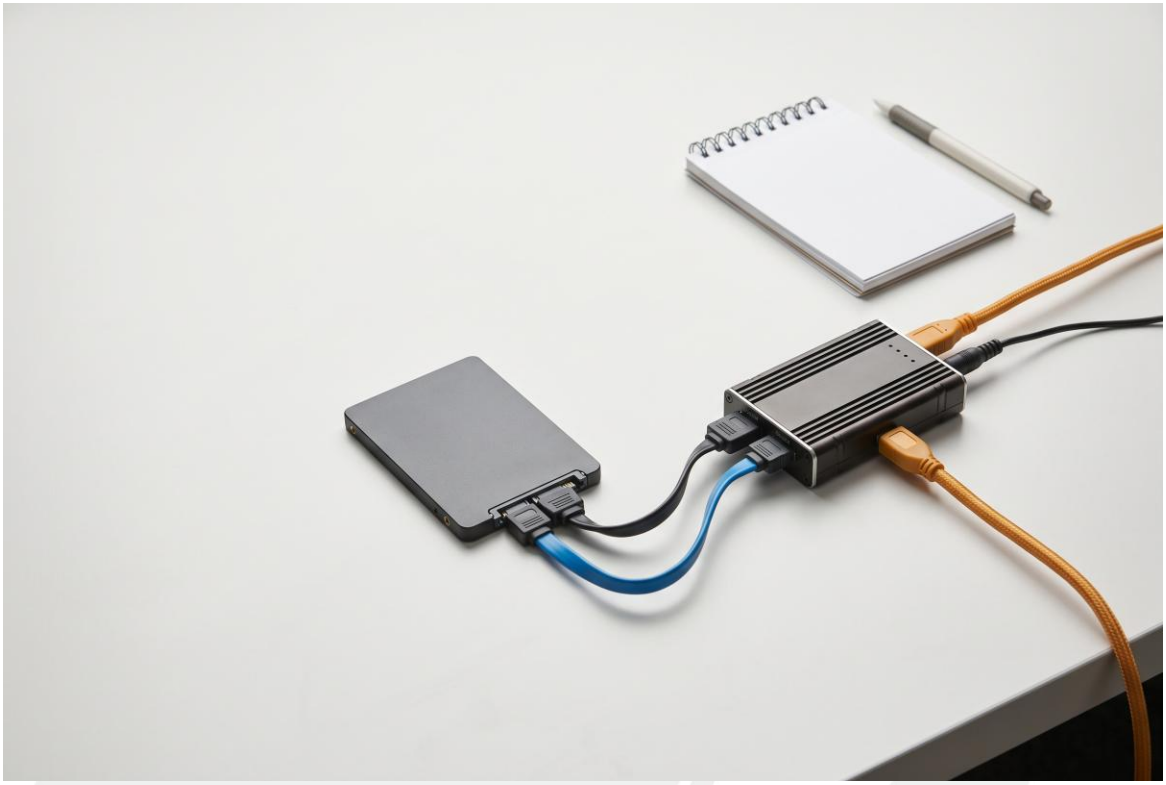


Abbildung 19. Quelle, Schreibblocker und Arbeitsstation: Auch die Verbindung ist Beweismaterial. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Dokumentieren Sie Modell und Seriennummer des Schreibblockers, sofern verfügbar, verwendete Anschlüsse, Kabel, Stromversorgung, Zustand der Anzeigen und alle Vorkommnisse. Erzeugt das Werkzeug einen Fehler, wird die Meldung aufbewahrt und ihre Auswirkung bewertet, statt sie zu verbergen. Der Schutz wird durch Konfiguration und Überprüfung nachgewiesen, nicht durch die bloße Behauptung, ein Gerät mit diesem Namen sei vorhanden gewesen.

8.3 Medien und Adapter: NVMe, SATA und optische Laufwerke

Die Bauform des Mediums verändert die Erfassung. Ein M.2-NVMe-Laufwerk wird nicht wie ein 2,5-Zoll-SATA-Laufwerk angeschlossen, und ein 3,5-Zoll-SATA-Laufwerk benötigt eine andere Stromversorgung. Der Adapter muss kompatibel sein und dokumentiert werden. Ein Foto des Adapters erläutert den Weg, doch das Protokoll muss Modell, Schnittstelle, Stromversorgung und die Überprüfung enthalten, ob das Medium von der Arbeitsstation korrekt erkannt wird.



Abbildung 20. Medien und Adapter: Bauform, Anschluss und Erfassungsverfahren. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Bei einem optischen Datenträger werden Lesegerät, Format, Kapazität, Lesemethode, unlesbare Sektoren und Beziehung zum empfangenen Träger dokumentiert. Es wird keine DVD-Erfassung behauptet, wenn die Bilder nur einen Ordner auf dem Computer und nicht den Datenträger zeigen. Schlägt das Lesen fehl, wird der Fehler aufbewahrt und ein zweites Laufwerk oder Verfahren geprüft, ohne das Problem durch eine allgemeine Behauptung zu ersetzen.

8.4 Logische Erfassung und Manifest

Eine logische Erfassung erhält ausgewählte Dateien oder Quellen. Vor ihrer Ausführung werden Ordner, Dateitypen, Datumsangaben, Filter und Ausschlüsse abgegrenzt. Die Ausgabe wird von einem Manifest begleitet, das Kennung, Name, Pfad, Objekttyp, Herkunft, Methode, Größe, Format, Hashwert und Anmerkungen verknüpft. Ohne Manifest kann ein Ordner voller Dateien Umfang haben, ist aber nicht unbedingt organisiertes Beweismaterial.

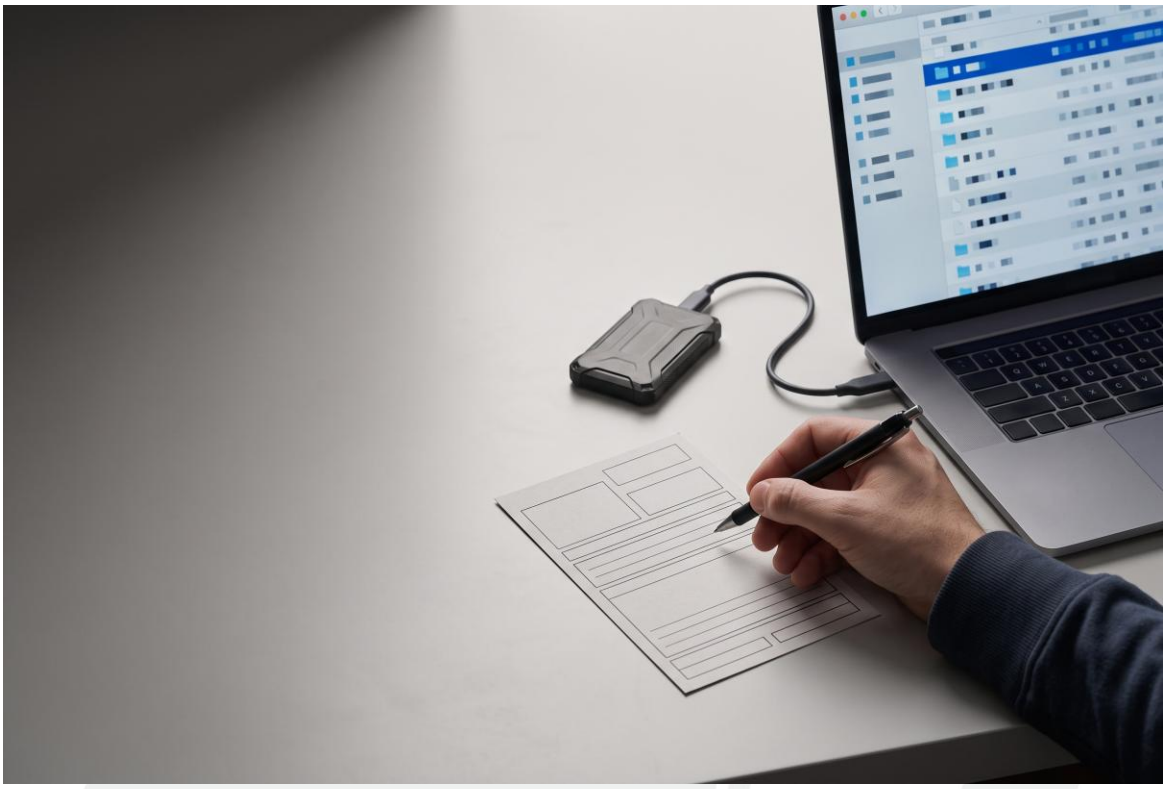


Abbildung 21. Dateimanifest: Herkunft, Derivate, Format und Integrität je Objekt. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Manifestregel
Das Manifest veröffentlicht keine Geheimnisse oder unnötigen sensiblen Daten. Der Pfad kann in der öffentlichen Version abgekürzt werden, wenn er geschützte Informationen offenlegt; er muss jedoch so viel Beziehung erhalten, dass das Objekt in der kontrollierten Akte gefunden werden kann.

8.5 Live-Erfassung und Werkzeugvalidierung

Eine Live-Erfassung ist gerechtfertigt, wenn Speicherinhalte, Sitzungen, Schlüssel oder Prozesse relevant sind und Befugnis sowie Fähigkeit zu ihrer Ausführung bestehen. Zustand, Werkzeug, Version, Parameter, unvermeidliche Veränderung und Ausgabe werden dokumentiert. Fehlen diese Voraussetzungen, wird der Fall weitergeleitet. Eine invasive Erfassung erfolgt nicht nur, weil ein Export schwieriger anzufordern wäre.

Ein Werkzeug muss für den vorgesehenen Einsatz bekannt und validiert sein. Name, Version, Umgebung, Konfiguration und Testergebnis werden dokumentiert. Eine Aktualisierung kann Format oder Verhalten ändern; ein alter Befehl darf nicht ungeprüft übernommen werden. Die Validierung verwendet fiktive Daten und zeigt, dass die Ausgabe geöffnet und dem erwarteten Objekt zugeordnet werden kann.



Abbildung 22. Werkzeug vor der Verwendung validieren: fiktive Daten, lesbare Ausgabe und erwartetes Objekt. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

8.6 Exporte und reproduzierbare Abfragen

Eine Abfrage muss mit denselben Parametern wiederholbar sein. Dokumentieren Sie System, Konto, Rolle, Filter, Zeitzone, Format, Felder, Datum, Bearbeiter und Ergebnis. Wenn die Plattform ihre Oberfläche ändert, bewahren Sie die Version oder einen Nachweis des verwendeten Wegs auf. Ein Bildschirmfoto kann die Konfiguration zeigen, ersetzt jedoch nicht die native Ausgabe. Wiederholbarkeit beruht auf dokumentierten Bedingungen, nicht auf Erinnerung.

Liefert eine Abfrage null Datensätze, darf nicht auf Nichtvorhandensein geschlossen werden, ohne Filter, Abdeckung, Zeitzone, Aufbewahrung und Fehler zu prüfen. Der Bericht beschreibt, was abgefragt wurde und welche Antwort erhalten wurde. Ein solcher dokumentierter Negativbefund ist belastbarer als eine absolute Behauptung. Ein Fehlen kann bedeutsam sein, jedoch nur innerhalb der nachgewiesenen Abdeckung.

8.7 Fehler und Vorkommnisse

Vorkommnisse werden nicht aus der Akte gelöscht: unlesbare Sektoren, beschädigte Dateien, fehlende Passwörter, Netzwerkunterbrechungen, Hashwertabweichungen und Anbieterwechsel werden dokumentiert. Es wird bewertet, ob sie Abdeckung, Authentizität oder Analyse beeinträchtigen; wenn möglich, wird eine zweite Übermittlung angefordert. Eine

Wiederholung beseitigt nicht den ersten Versuch, sondern erzeugt ein weiteres verknüpftes Objekt mit eigener Geschichte.
Muss eine Erfassung wiederholt werden, werden beide Objekte mit unterschiedlichen Kennungen aufbewahrt und der Grund erläutert. Die erste Datei wird nicht gelöscht, um eine unangenehme Erklärung zu vermeiden. Zur Nachverfolgbarkeit gehören auch fehlgeschlagene Entscheidungen und ihre Korrektur. Eine nur äußerlich fehlerfreie Akte ist weniger belastbar als eine, die das Vorkommnis und seine Behandlung ausweist.

Begrenzte Schlussfolgerung
Die Erfassung endet nicht mit einer Datei. Sie endet mit einer Ausgabe, die geöffnet, dem Objekt zugeordnet, überprüft und unter dokumentierten Bedingungen wiederholt werden kann. Fehler bleiben im Protokoll und werden nicht aus der Darstellung ausgeblendet.

Kapitel 9. Verwahrung, Transport und Aufbewahrung

9.1 Die Beweismittelkette als Antwort auf Fragen

Die Beweismittelkette ermöglicht zu rekonstruieren, welches Objekt vorhanden war, wo es sich befand, wer darauf zugreifen konnte, warum es bewegt und wie es überprüft wurde. Sie ist keine Liste von Unterschriften ohne Kennungen. Jede Übertragung umfasst Objekt, Übergabe, Entgegennahme, Datum, Zeitzone, Zweck, Zustand des Siegels und gegebenenfalls die Integritätsprüfung. Auch legitime Zugriffe ohne physische Übertragung werden erfasst: Öffnen des Behältnisses, Arbeitskopie, vorübergehende Ausleihe, Standortwechsel oder entfernter Download.

Wird nur die abschließende Übergabe dokumentiert, entstehen Lücken, die eine Rekonstruktion des Verlaufs verhindern. Ein Siegel kann bei Empfang intakt sein, obwohl unbekannt ist, wer es zuvor geöffnet hat. Die Kette dokumentiert Ereignisse: Entgegennahme, Öffnung, Kopie, Zugriff, Übertragung, Überprüfung und Rückgabe. Jedes Ereignis hat einen Verantwortlichen und einen Zweck, nicht nur Name und Datum.



Abbildung 23. Übertragung der Verwahrung: Objekt, Verantwortliche, Siegel und Überprüfung. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

9.2 Elektronische Übertragungen und Schlüssel

Bei einer Übertragung per Link müssen Empfänger, Berechtigungen, Kanal, Datum, Version und Download-Prüfung dokumentiert werden. Verschlüsselung schützt den Inhalt; die Schlüsselverwaltung erfolgt jedoch über einen separaten Kanal und ohne Geheimnisse im Protokoll. Der Empfänger bestätigt Objekt und Hashwert, bevor er fortfährt. Ein Link, ohne zu wissen, wer ihn öffnen kann, ist keine kontrollierte Verwahrung.
Enthält die Anbieter-E-Mail den Hashwert im Nachrichtentext, werden die vollständige EML-Datei und die Anhänge aufbewahrt. Der Nachrichtentext verbindet die Erklärung mit der Übermittlung; die empfangene Datei wird lokal überprüft. Ändert der Anbieter die Datei, sind eine neue Übermittlung und ein neuer Hashwert erforderlich, ohne die frühere Version stillschweigend zu ersetzen. Auch ein Wechsel des Schlüssels oder Empfängers wird dokumentiert.



Abbildung 24. Verschlüsselung und Schlüssel: Inhalte schützen, ohne die Kontrolle über den Empfang zu verlieren. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Schlüsselregel
Verschlüsselung allein genügt nicht: Dokumentieren Sie, wer den Schlüssel besitzt, über welchen separaten Kanal er übermittelt und wie der Empfang überprüft wurde. Schlüssel werden weder im Protokoll noch im Nachrichtentext aufgeführt.

9.3 Speicherung und späterer Zugriff

Das aufbewahrte Original und die Arbeitskopie werden entsprechend der Richtlinie getrennt. Sicherungskopien werden verschlüsselt und überprüft, ihre Wiederherstellung wird getestet. Eine Sicherungskopie, die niemand öffnen kann, ist keine brauchbare Aufbewahrung. Die Migration in ein anderes Format wird dokumentiert und beseitigt nicht das Original. Die Aufbewahrung umfasst künftige Lesbarkeit, Formatdokumentation und verfügbare Schlüssel. Gesetzliche Aufbewahrung, unternehmensinterne Richtlinien und Aufbewahrung zu Beweiszwecken verfolgen weder denselben Zweck noch dieselbe Frist. Es gibt keine allgemeingültige Zahl. Die Dauer wird nach Vorschrift, Fall und Bedarf festgelegt, mit eingeschränktem Zugriff und Protokollierung der Abfragen. Die Aufbewahrung umfasst künftige Lesbarkeit, Formatdokumentation und verfügbare Schlüssel. Die erste Arbeitskopie wird nicht mit der Originalverpackung verwechselt; jede Öffnung, Erneuerung des Siegels oder Übertragung wird dokumentiert.



Abbildung 25. Sicherungskopie und Migration: Original, Arbeitskopie und späteren Zugriff aufbewahren. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

9.4 Öffnen und Erneuern des Siegels

Das Öffnen eines Behältnisses zur Bearbeitung löscht weder das Siegel noch die Geschichte. Dokumentiert wird, wer mit welcher Befugnis warum geöffnet hat, welchen Zustand das Siegel

hatte und welches Objekt es enthielt. Nach Abschluss wird ein neues Siegel mit neuer Kennung angebracht; das frühere wird aufbewahrt, wenn das Verfahren dies verlangt. Die Kette wird durch überprüfbare Handlungen gestärkt, nicht durch die allgemeine Behauptung, das Paket sei geschlossen gewesen.



Abbildung 26. Öffnen und Erneuern des Siegels: eine Übertragung, die ebenfalls dokumentiert werden muss. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

9.5 Zugriffe, gemeinsame Verwahrung und Interessenkonflikte

Der spätere Zugriff erfordert Protokollierung von Abfragen, Zweck und Autorisierung. Prüft, exportiert oder teilt eine Person, muss die Handlung ihrer Funktion zugeordnet sein. Gemeinsame Verwahrung beseitigt keine Verantwortung: Sie legt fest, wer entscheidet, wer ausführt und wer überprüft. Interessenkonflikte werden erklärt und bei erforderlicher Unabhängigkeit getrennt.



Abbildung 27. Zugriffsprotokoll: Wer mit Autorisierung öffnen, einsehen und übertragen darf. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Begrenzte Schlussfolgerung
Die Verwahrung endet nicht, wenn das Objekt weggeschlossen wird. Sie endet, wenn jeder Zugriff, jede Übertragung und jede Überprüfung rekonstruiert werden kann, einschließlich der Art und Weise, wie die Möglichkeit des späteren Öffnens erhalten bleibt.

Kapitel 10. Untersuchung, Chronologie und alternative Hypothesen

10.1 Untersuchen heißt nicht, einen Schuldigen zu suchen

Die Untersuchung beginnt, wenn die Quelle identifiziert und erfasst wurde und dem Auftrag zugeordnet ist. Ihr Ziel ist nicht, die Datei zu finden, die den ersten Eindruck bestätigt, sondern eine Datenmenge in überprüfbare Beobachtungen zu verwandeln. Der Analyst öffnet die Arbeitskopie, dokumentiert die Werkzeuge und formuliert kleine Fragen: Welche Datei existiert, welches Datum zeigt sie, was bedeutet ein Feld, welche Änderung ist eingetreten, welches System hat den Eintrag erzeugt und welche andere Quelle könnte ihm widersprechen? Jede Antwort muss zu einem konkreten Objekt des Manifests zurückführen.

Der Unterschied zwischen Untersuchung und Analyse ähnelt dem Unterschied zwischen dem Betrachten der Teile einer Uhr und der Erklärung, warum sie stehen geblieben ist. Bei der Untersuchung werden Zahnräder, Verschleiß und Position beobachtet; bei der Analyse werden Erklärungen verglichen: Energiemangel, mechanischer Schaden, Manipulation oder eine falsche Ablesung. Werden die Beobachtungen zugunsten der bevorzugten Erklärung übersprungen, scheint jedes Teil sie zu bestätigen. Disziplin bedeutet, zuerst zu beschreiben und dann zu interpretieren, und auch die nicht passenden Befunde aufzubewahren.[19]

Arbeitsregel
Jede Aussage der Analyse muss rückverfolgbar sein: von der Schlussfolgerung zum Befund, zur Abfrage, zum analysierten Objekt, zur Erfassung und schließlich zur Quelle. Fehlt eine dieser Verbindungen, muss die Schlussfolgerung neu formuliert oder eine andere Quelle herangezogen werden.

10.2 Metadaten: der Datei zuhören, ohne alles zu glauben

Ein Metadatum ist eine Information über ein Objekt, kein freiwilliges Geständnis des Ereignisses. Das Erstellungsdatum in einem Dateisystem kann sich auf die Kopie auf diesem Medium beziehen; das interne Datum einer Fotografie kann von der Kamerauhr abhängen; ein Autorenfeld kann ein Kontoname sein, den eine beliebige Person konfiguriert hat. Jedes Feld hat einen Erzeuger, einen Mechanismus und eine Veränderungsmöglichkeit. Für seine richtige Lektüre muss bekannt sein, wer es wann unter welchen Bedingungen geschrieben hat und ob die Analyse es verändert hat.

Auch ein Dateiname kann Orientierung geben, ohne etwas zu beweisen. Eine Abfolge IMG_0041, IMG_0042 und IMG_0043 deutet auf eine Erzeugungsreihenfolge innerhalb einer Kamera oder Anwendung hin, schließt jedoch Kopien, Umbenennungen, Neunummerierungen oder importierte Dateien nicht aus. Die vorsichtige Analyse prüft, ob interne Kennungen,

[19]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodischer Leitfaden, weder Rechtsvorschrift noch Garantie für die Zulässigkeit.Offizielle Online-Quelle

Miniaturansichten, Datumsangaben, Anwendungsprotokolle und Sicherungskopien diese Abfolge bestätigen. Der Name ist ein Hinweis für die Untersuchung, kein chronologisches Siegel.

Angenommen, ein Bild zeigt 18:42 Uhr, während eine Anklage behauptet, es sei um 20:42 Uhr aufgenommen worden. Die erste Versuchung besteht darin, das Beweismaterial für gefälscht zu erklären. Die zweite, ebenso gefährliche, darin, 18:42 Uhr als absolute Zeit zu akzeptieren. Die richtige Methode bewahrt die native Datei, liest die Felder unverändert aus, prüft Zeitzone und Geräteuhr, vergleicht die vorherige und spätere Abfolge und sucht eine unabhängige Quelle: Versandnachricht, Cloud-Kopie, Kaufbeleg, Video einer anderen Kamera oder Aktivitätsprotokoll. Erst dann lässt sich erklären, ob eine Zonendifferenz, eine falsch eingestellte Uhr, eine Konvertierung oder eine größere Abweichung vorliegt.



Abbildung 28. Metadaten benötigen Erzeuger, Bedeutung, Kontext und Bestätigung; sie sind keine unfehlbaren Zeugen. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Beobachteter Wert	Technische Frage	Noch nicht zulässige Schlussfolgerung
Systemdatum	Welches Ereignis stellt es in diesem Dateisystem dar?	Es ist das ursprüngliche Datum des Ereignisses.
EXIF-Datum	Wie waren Uhr und Zeitzone konfiguriert?	Die Szene ereignete sich zwangsläufig zu dieser Zeit.

Beobachteter Wert	Technische Frage	Noch nicht zulässige Schlussfolgerung
Autor oder Konto	Wer konnte dieses Konto konfigurieren oder verwenden?	Die natürliche Person wurde identifiziert.
Aufeinanderfolgen der Name	Bleibt die Abfolge in anderen Quellen erhalten?	Es gab keine Kopien, Importe oder Umbenennungen.
Koordinaten	Welche Genauigkeit und Herkunft hat die Positionsangabe?	Die Person befand sich an einem exakten Punkt.

10.3 Chronologie: Uhren abgleichen, bevor Geschichten geordnet werden

Eine brauchbare Chronologie ist nicht nur eine Spalte geordneter Daten. Sie ist ein Abgleich von Uhren, die in unterschiedlichen Zonen liegen, mit verschiedenen Servern synchronisiert werden oder menschliche Fehler enthalten können. Zuerst wird der wörtliche Wert der Quelle dokumentiert, danach ihre angegebene oder abgeleitete Zone, die vorgenommene Umrechnung und die verfügbare Genauigkeit. Der ursprüngliche Wert wird niemals durch die Umrechnung ersetzt. Verwendet ein Anbieter UTC und ein Telefon lokale Zeit, muss der Bericht beide zeigen und erklären, wie sie verglichen wurden.

Die Genauigkeit ist ebenso wichtig wie das Datum. Ein Eintrag, der nur den Tag enthält, darf aus visueller Bequemlichkeit nicht auf 14:32 Uhr gesetzt werden. Eine Datei mit Sekunden hat nicht notwendigerweise Sekundengenauigkeit. Weist die Uhr eine bekannte Abweichung auf, werden ihre Messung und die betroffenen Quellen dokumentiert. Lässt sie sich nicht auflösen, wird ein Zeitfenster verwendet oder die Unsicherheit erklärt. Diese Ehrlichkeit verhindert, dass eine visuell perfekte Abfolge zwei unvereinbare Ereignisse in einen Kausalzusammenhang verwandelt.

Die Abfolge muss auch negative Ereignisse und Zeiträume ohne Daten enthalten. Eine Unterbrechung der Protokolle kann durch Inaktivität, Rotation, Verlust der Konnektivität, Konfiguration oder Löschung entstanden sein; die Zeitachse darf eine Erklärung nicht ohne Beweis wählen. Jedes Ereignis sollte als beobachtet, berechnet, von einer Person angegeben oder abgeleitet gekennzeichnet werden. Diese vier Kategorien als identisch zu behandeln, ist eine subtile Form, Gewissheit zu erzeugen.



Abbildung 29. Die Chronologie bewahrt ursprüngliche Zeit, Zeitzone, Umrechnung und Unsicherheit jeder Quelle. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Beispiel für eine chronologische Normalisierung
Objekt: ED-20261109-DEMO-SRV-001-A00
Wörtlicher Wert: 2026-11-03 20:14:07
Vom Anbieter angegebene Zeitzone: UTC
Arbeitsumrechnung: 2026-11-03 14:14:07 -06:00
Verfügbare Genauigkeit: Sekunden; Synchronisation des Servers nicht belegt
Beziehung: Ereignis vor der um 14:20:11 -06:00 empfangenen E-Mail
Einschränkung: Zeitliche Nähe beweist weder, wer die Handlung ausgeführt hat, noch, dass ein Ereignis das andere verursacht hat.

10.4 Antennen, Abdeckung und Azimut: Geografie ohne Abkürzungen

Eine Gesprächsdatenliste kann darauf hinweisen, dass eine Leitung über eine Funkzelle kommuniziert hat. Dies macht die Antenne nicht zu einer Person und beweist nicht, dass sich der Träger unter ihr befand. Die Funkzelle beschreibt eine funkgestützte Beziehung innerhalb der Bedingungen von Netz, Abdeckung, Auslastung, Technologie und Konfiguration. Die Analyse benötigt den Standort der Funkzelle, gegebenenfalls Ausrichtung oder Azimut, Technologietyp, Datum, verfügbare Leistungs- oder Messwerte und ein realistisches

Verständnis des Gebiets. Ein Punkt auf einer Karte stellt die Ausrüstung dar, nicht den Benutzer.
Der Azimut gibt den Sektor an, in den die Antenne gerichtet ist; er ist keine Laserlinie, die in einem Haus endet. Die Abdeckung hängt von Ausbreitung, Hindernissen, Frequenz, Gelände, Interferenz, Leistung und Netzentscheidungen ab. Ein Anruf kann von einer Funkzelle bedient werden, die nicht die nächstgelegene ist. Das Fehlen einer anderen Funkzelle in einem Export beweist ebenfalls nicht, dass keine alternative Abdeckung bestand: Sie kann nicht genutzt, nicht geliefert oder vom System nicht aufbewahrt worden sein.
In einer vom Autor geprüften anonymisierten Akte wurde ein Standort so behandelt, als beschreibe er den Weg einer Person, obwohl die Quelle nur eine Abdeckung aussagen konnte. Weitere Elemente erschwerten die Version: Ein Video lieferte eine Abfolge, die nicht mit der behaupteten Interpretation übereinstimmte, und Zeugen beschrieben die Ereignisse uneinheitlich. Der Wert der Analyse bestand nicht darin, eine Geschichte durch eine ebenso absolute andere zu ersetzen, sondern zu zeigen, dass die Schlussfolgerung nicht zwingend aus der Quelle folgte. Die Antenne blieb eine Antenne; die Identität des Trägers erforderte einen anderen Beweis.[20]



Abbildung 30. Eine Antenne liefert potenzielle Abdeckung, keine genaue Adresse und nicht die Identität des Trägers. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

[20]Jocsan Laguna. Sinaloa. Entwicklung und Schlussfolgerungen eines technischen Gutachtens zur Informatikforensik. Vom Autor bereitgestelltes Material; Fehler werden verallgemeinert, ohne personenbezogene Daten offenzulegen.

Vertretbare Form der Schlussfolgerung
„Der bereitgestellte Datensatz verknüpft das Ereignis mit der identifizierten Funkzelle. Ohne zusätzliche Messungen und Parameter erlaubt dieser Wert weder eine punktgenaue Standortbestimmung noch die Zuordnung der Terminalnutzung zu einer natürlichen Person.“

10.5 Bestätigung, die tatsächlich unterscheidet

Zwei Dateien mit demselben Inhalt sind nicht immer zwei unabhängige Quellen. Ein Bildschirmfoto und ein Ausdruck desselben Bildschirmfotos wiederholen nur eine Darstellung. Ein Serverprotokoll, eine von einem Dritten empfangene Nachricht und eine Abfolge von Sensordaten können dagegen unterschiedliche Ursprünge und Fehler haben. Eine Bestätigung gewinnt an Kraft, wenn die Quellen nicht dieselbe Abhängigkeit teilen und jede die Version hätte widerlegen können.

Konvergenz wird nicht nach Seitenzahl bewertet, sondern nach Unabhängigkeit, Nähe zum Ereignis, Fehlermöglichkeit und der Fähigkeit, Hypothesen zu unterscheiden. Hundert Bildschirmfotos ohne Herkunft können weniger wert sein als eine vollständige EML-Datei mit Kopfzeilen, überprüfbarem Anhang und Serverprotokollen. Ockhams Rasiermesser gebietet nicht, die bequemste Erklärung zu wählen: Es verlangt, keine weiteren Ursachen zu vervielfachen, wenn eine einfache Abfolge die Daten einschließlich ihrer Widersprüche erklärt.

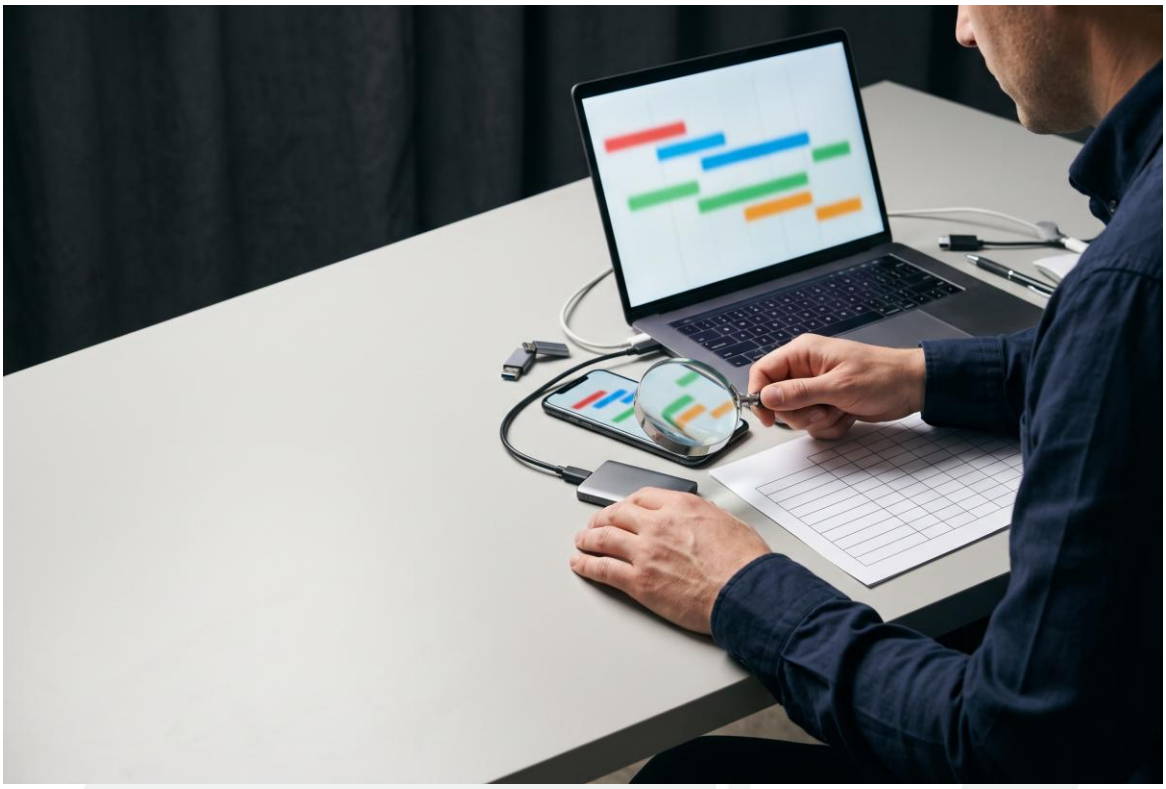


Abbildung 31. Bestätigung bedeutet, Quellen mit unterschiedlichen Ursprüngen und Fehlern zu vergleichen, nicht dasselbe Bildschirmfoto zu wiederholen. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

10.6 Hypothesenmatrix: Beweise widersprechen lassen

Vor der Analyse sollten mindestens zwei plausible Erklärungen und eine Bedingung zu ihrer Unterscheidung formuliert werden. Behauptet ein Unternehmen, eine Datei sei am Austrittstag von einem Mitarbeiter erstellt worden, könnten die Hypothesen lauten: Erstellung an diesem Datum durch das zugewiesene Konto; nachträgliche Kopie einer älteren Datei; Veränderung von Metadaten; oder Nutzung des Kontos durch eine andere Person. Nicht alle müssen gleich wahrscheinlich sein, aber alle müssen einer konkreten Prüfung standhalten.

Das Ergebnis kann positiv, negativ oder nicht eindeutig sein. Ein dokumentiertes negatives Ergebnis ist kein Misserfolg: Es kann eine Erklärung ausschließen und eine ungerechte Anschuldigung verhindern. Ein nicht eindeutiges Ergebnis darf ebenfalls nicht als Bestätigung dargestellt werden. Ermöglicht die Quelle keine Unterscheidung, muss eine andere Quelle angefordert, der Umfang geändert oder die Einschränkung erklärt werden. Der Analyst wird nicht dafür belohnt, eine falsche Hypothese beizubehalten, sondern dafür, sie aufzugeben, wenn die Daten dies erfordern.

Hypothese	Überprüfung	Fiktives Ergebnis	Eingeschränkte Interpretation
Das Dokument wurde am 3. November erstellt.	Interne Metadaten, Versionsverlauf und Cloud-Protokolle.	Der Verlauf zeigt eine frühere Version vom 28. Oktober.	Das sichtbare Datum belegt nicht die ursprüngliche Erstellung.
Das Konto wurde von seinem Inhaber verwendet.	Sitzungen, zweiter Faktor, Geräte und gleichzeitige Aktivität.	Es liegt eine Sitzung von einem nicht registrierten Gerät vor.	Die Zuordnung des Kontos identifiziert die Person noch nicht.
Das Image gehört zum selben Ereignis.	Abfolge, Miniaturansichten, Sicherungskopie und andere benachbarte Dateien.	Die Sicherungskopie enthält eine kohärente Abfolge.	Vereinbar mit dem Ereignis; seine Bedeutung erfordert Kontext.
Es gab keine weiteren Zugriffe.	Vollständige Abfrage, Aufbewahrung, Filter und Fehler.	Der Export umfasst nur sieben Tage.	Im abgefragten Zeitraum wurden keine Zugriffe festgestellt; ein vollständiges Nichtvorhandensein kann nicht behauptet werden.

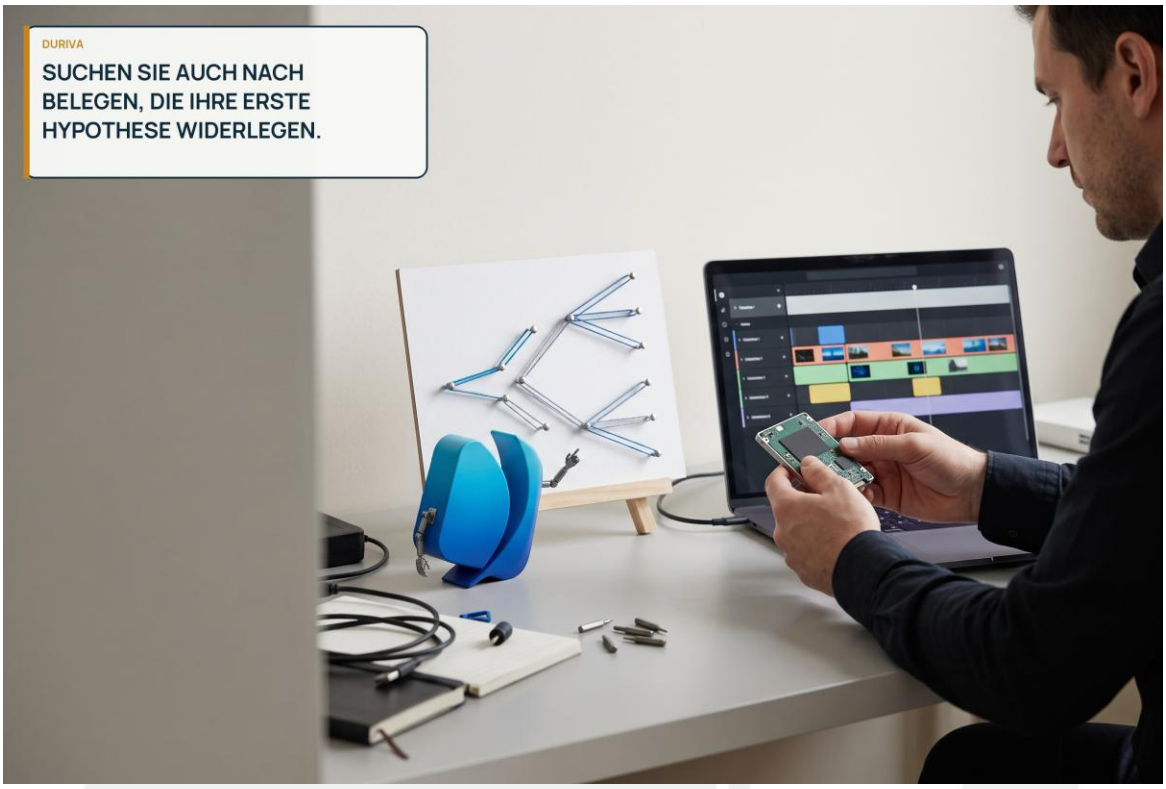


Abbildung 32. Auch nach Widersprüchen zur ersten Hypothese zu suchen verhindert, dass die Analyse zur Selbstbestätigung wird. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

10.7 Wiederholen, Reproduzieren und wissen, wann aufzuhören ist

Eine wiederholbare Abfrage kann unter dokumentierten Bedingungen erneut ausgeführt werden und am selben Objekt zu einem vereinbaren Ergebnis führen. Reproduzierbarkeit erfordert außerdem, dass eine andere qualifizierte Person das Verfahren ausreichend unabhängig verstehen und bewerten kann. Ein Bildschirmfoto des Ergebnisses genügt für beides nicht, wenn Datei, Werkzeugversion, Filter oder Abfrage unbekannt sind. Ziel ist, dass die Überprüfung anhand von Daten widersprechen kann und nicht auf das Gedächtnis des Analysten vertrauen muss.[21]

Die Analyse endet, wenn die Fragen des Auftrags innerhalb des Umfangs beantwortet wurden, wenn eine zusätzliche Quelle keine Unterscheidung mehr ermöglicht oder wenn Fortfahren einen unverhältnismäßigen Eingriff bedeutet. Sie wird auch ausgesetzt, um bei einer neuen Quelle eine Befugnis einzuholen. Vollständigkeit bedeutet nicht, jeden möglichen Ordner zu öffnen, sondern keine vernünftige Hypothese ungeprüft zu lassen, die mit den verfügbaren Beweisen beantwortet werden kann.

[21]ISO/IEC 27037:2012. Leitlinien für Identifizierung, Sammlung, Erfassung und Erhaltung digitaler Beweise. Die Ausgabe wurde von ISO als gültig bestätigt.Offizielle Online-Quelle

Ergebnis des Kapitels
Eine Analysematrix mit Aussage, Quelle, Abfrage, wörtlichem Befund, vereinbarer Hypothese, geschwächter Hypothese, Einschränkung und zusätzlicher Maßnahme. Die Schlussfolgerung entsteht aus dieser Matrix; sie wird nicht vorher formuliert, um sie nachträglich auszufüllen.

Kapitel 11. Bericht, Argumentation und Widerlegung

11.1 Der Bericht als Rückweg zur Quelle

Ein forensischer Bericht soll nicht durch Umfang oder die Zahl englischer Fachbegriffe beeindrucken. Er muss einer Person mit anderem Urteilsvermögen ermöglichen, das Objekt zu finden, die durchgeführten Handlungen zu verstehen und zu prüfen, ob sich die Schlussfolgerung aus den Befunden ableitet. Die Struktur ist ein Weg: Auftrag, Umfang, Befugnis, Quellen, Methode, Ergebnisse, Analyse, Schlussfolgerung, Einschränkungen und Anhänge. Kann eine Behauptung diesen Weg nicht rückwärts verfolgt werden, wird der Bericht zu Autoritätsliteratur.

Die Hauptleserschaft besteht nicht immer aus Ingenieuren. Eine Richterin, ein Rechtsanwalt, eine Führungskraft oder eine beschuldigte Person muss die Argumentation verstehen, ohne zuvor eine Geheimsprache zu erlernen. Klares Schreiben mindert die Wissenschaft nicht, sondern legt sie offen. Deshalb wird jeder Fachbegriff beim ersten Auftreten erklärt und jedes Bildschirmfoto durch das Originalobjekt oder eine Begründung für dessen Fehlen ergänzt. Die Einfachheit der Erklärung muss der Sorgfalt der Arbeit entsprechen, nicht deren Fehlen.



Abbildung 33. Der Bericht ermöglicht die Überprüfung von Quelle, Methode, Befund und Schlussfolgerung; er hängt nicht vom Ansehen des Unterzeichners ab. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

11.2 Tatsache, Ergebnis, Ableitung und Meinung

Der Text muss vier Ebenen unterscheiden. Eine dokumentierte Tatsache ist das, was bei der Entgegennahme festgehalten wurde: Die Datei ging mit einem bestimmten Namen und einer bestimmten Größe ein. Ein technisches Ergebnis ist das, was die Überprüfung erzeugt: Der berechnete Hashwert stimmt mit einem anderen Wert überein. Eine Ableitung ist die begründete Interpretation mehrerer Ergebnisse: Der empfangene Anhang stimmt mit der Datei überein, die der Anbieter angegeben hat. Eine Meinung ist die fachliche Schlussfolgerung innerhalb des Auftrags: Die Übermittlung bewahrt seit diesem Zeitpunkt einen überprüfbaren Integritätsmechanismus. Werden diese Ebenen vermischt, erscheint eine Meinung als beobachteter Wert.

Auch juristische und technische Fragen müssen getrennt werden. Der Sachverständige kann beschreiben, wie ein Datensatz erlangt wurde, welche Felder er enthält und welche Abweichungen er aufweist. Er muss nicht erklären, dass eine Person schuldig ist, dass eine Handlung eine Straftat darstellt oder dass eine Partei gewinnen soll. Diese Zurückhaltung mindert den Nutzen des Berichts nicht; sie verhindert, dass eine Schlussfolgerung aus einem anderen Zuständigkeitsbereich die Kraft der tatsächlichen Befunde beeinträchtigt.

Ebene	Korrektes Beispiel	Zu vermeidender Überschuss
Entgegennahme	„Die Datei adjunto.csv wurde in der als EV-04 identifizierten EML-Datei empfangen.“	„Die Bank lieferte die vollständige Wahrheit.“
Ergebnis	„Der berechnete SHA-256-Wert stimmt mit dem Wert im Nachrichtentext überein.“	„Der Inhalt wurde seit seiner Entstehung niemals verändert.“
Analyse	„Die Übereinstimmung verbindet den Anhang mit der Erklärung des Anbieters.“	„Der Anruf wurde vom Inhaber getätigt.“
Schlussfolgerung	„Die Integrität zwischen Übermittlung und Empfang wurde überprüft.“	„Der Beweis ist unwiderlegbar und schlüssig.“

11.3 Der Syllogismus und die falsche Konsequenz

Ein Syllogismus ordnet Prämissen und Schlussfolgerung. In der forensischen Arbeit hilft er, Sprünge zu erkennen, die Begeisterung häufig verdeckt. Obersatz: Eine Funkzelle registriert eine Beziehung zwischen dem Netz und einem Endgerät innerhalb der Abdeckungsbedingungen. Untersatz: Der analysierte Datensatz verknüpft eine Kommunikation mit Funkzelle A. Zulässige Schlussfolgerung: Es besteht eine dokumentierte Verbindung zwischen dieser Kommunikation und Funkzelle A. Nicht abgeleitet werden kann, dass sich eine

bestimmte Person an einer bestimmten Adresse befand. Dafür fehlen Prämissen über Standort, Endgerät und Nutzer.
Eine falsche Konsequenz entsteht, wenn eine wahre Aussage als Freibrief für eine andere verwendet wird, die nicht aus ihr folgt. Die Datei enthält eine IP-Adresse; also hat der Verdächtige die Nachricht geschrieben. Die Signatur wird verifiziert; also ist alles Gesagte geschehen. Das Video zeigt eine Uhr; also ist die gesamte Aufzeichnung authentisch. Der Datenträger ist versiegelt; also stammt die analysierte Kopie von ihm. Jede Schlussfolgerung erfordert eine zusätzliche Prämisse und eine andere Überprüfung. Die Argumentation wird nicht dadurch stärker, dass diese Schritte ausgelassen werden, sondern dadurch, dass sie sichtbar gemacht werden.
Bei physischen Datenträgern kann ein Widerspruch in der Identifizierung ausreichen, um eine Ableitung zu verhindern. Beschreibt das Protokoll einen Datenträgertyp, während Bilder oder Kapazitäten einem anderen entsprechen, darf dies nicht als geringfügiger Fehler abgetan werden. Zuerst muss geklärt werden, welches Objekt empfangen, welches erfasst und welches bei jeder Handlung verwendet wurde. Die Schlussfolgerung wird ausgesetzt, bis die Identität der Quelle geklärt ist. Eine ausgezeichnete Analyse des falschen Objekts ist nicht möglich.[22]

Die Prüfung des „daher“
Schreiben Sie nach jedem „daher“ die Prämisse auf, die die Schlussfolgerung zwingend macht. Beruht diese Prämisse nur auf Gewohnheit, Intuition oder Ansehen, ersetzen Sie die absolute Konsequenz durch eine begrenzte Beobachtung oder führen Sie die fehlende Überprüfung durch.

11.4 Widersprüche erklären, ohne sie zu verbergen

Ein Widerspruch bedeutet nicht immer Fälschung. Er kann eine Zeitzone, eine falsch gehende Uhr, Exporte mit unterschiedlichen Filtern, zwei gleichnamige Objekte, Feldinterpretationen oder eine tatsächlich inkompatible Quelle offenbaren. Der Bericht muss die Abweichung mit ihren wörtlichen Werten darstellen und mögliche Erklärungen analysieren. Sie zu verbergen, weil sie eine Version schwächt, bedeutet, die wissenschaftliche Funktion aufzugeben; sie ohne Untersuchung auszunutzen, ist der entgegengesetzte Fehler.
Angenommen, ein Video weist ein unmögliches Datum auf, eine Gesprächsdatenliste enthält eine Nummer im falschen Format und zwei Zeugen beschreiben unvereinbare Positionen. Keine dieser Abweichungen darf aus Bequemlichkeit ignoriert werden. Es wird geprüft, ob das Video einen Zähler oder ein nicht initialisiertes Systemdatum aufweist, ob die Nummer falsch transkribiert oder exportiert wurde und ob die Zeugen dasselbe Ereignis von verschiedenen Orten beobachtet haben. Lässt sich die Erklärung nicht halten, bleibt die Abweichung ungelöst. Ihre Auswirkung auf die Schlussfolgerung wird genau angegeben.
Der Fall der Fotografien und der Bank zeigt die konstruktive Seite: Alltägliche Quellen können eine Erklärung liefern, die mit der Version einer zunächst unwahrscheinlich erscheinenden

[22]Jocsan Laguna. Sinaloa. Entwicklung und Schlussfolgerungen eines technischen Gutachtens zur Informatikforensik. Vom Autor bereitgestelltes Material; Fehler werden verallgemeinert, ohne personenbezogene Daten offenzulegen.

Person vereinbar ist. Der Fall der Antenne zeigt die vorbeugende Seite: Eine technische Quelle kann zur Stützung von Aussagen verwendet werden, die sie nicht beweist. In beiden Fällen ist die Methode dieselbe: bewahren, verstehen, vergleichen und begrenzen. Beweise dienen nicht als Schmuck für Anklage oder Verteidigung, sondern dazu, eine überprüfbare Abfolge zu finden.[23][24]

11.5 Schlussfolgerungen formulieren, die die Beweise tragen

Eine starke Schlussfolgerung ist nicht unbedingt eine absolute Schlussfolgerung. „In dem Export zwischen diesen Daten wurden mit diesen Filtern und dieser Abdeckung keine Ereignisse festgestellt“ ist stärker als „sie fanden niemals statt“, weil es überprüfbar ist und einer kritischen Nachfrage standhält. Ebenso erklärt „die geprüften Daten sind mit Abfolge A vereinbar und weisen diese Abweichungen von B auf“ die Beweiskraft besser als „A wurde vollständig bewiesen“.
Der Grad der Behauptung muss der Unterscheidungskraft der Methode entsprechen. Liegt nur eine visuelle Darstellung vor, wird das Sichtbare beschrieben und die native Datei angefordert. Bestehen mehrere unabhängige Quellen, werden ihre Konvergenz und auch ihre Grenzen erläutert. Fehlt eine entscheidende Quelle, wird dies nicht durch Adjektive ausgeglichen. Der Leser muss wissen, was auf welcher Grundlage behauptet wurde, was ausgeschlossen blieb und welche neuen Informationen die Antwort verändern könnten.

Situation	Vertretbare Formulierung	Informationen, die sie ändern könnten
Übereinstimmender Hashwert	Das Objekt blieb zwischen den beiden dokumentierten Prüfungen unverändert.	Fehler bei der Identifizierung des Objekts oder des registrierten Algorithmus.
Zugewiesenes Konto	Die Ereignisse wurden dem Konto zugeordnet; die physische Person wird dadurch allein nicht identifiziert.	Aufzeichnungen über zweiten Faktor, Gerät, Kontrolle der Anmeldedaten und Bestätigung.
Metadaten zum Datum	Das interne Datum ist mit dem untersuchten Zeitraum vereinbar, abhängig von Uhr und Zeitzone.	Unabhängige Sicherungskopie, native Abfolge und Synchronisation.
Abfrage ohne Ergebnis	Innerhalb der angegebenen Abdeckung und Filter wurden keine Datensätze festgestellt.	Erweiterter Export, Korrektur der Filter oder Wiederherstellung der Aufbewahrungsdaten.

[23] Jocsan Laguna. Buch für Rechtsanwälte, Kapitel 1. Vom Autor bereitgestelltes narratives Recherchematerial. Namen im Handbuch zum Schutz von Identitäten geändert.
[24] Jocsan Laguna. Sinaloa. Entwicklung und Schlussfolgerungen eines technischen Gutachtens zur Informatikforensik. Vom Autor bereitgestelltes Material; Fehler werden verallgemeinert, ohne personenbezogene Daten offenzulegen.

11.6 Widerlegung und unabhängige Überprüfung

Vor der Übermittlung muss eine andere Person versuchen, die Argumentation zu widerlegen, ohne die Objekte zu verändern. Sie prüft, ob die Kennung mit dem Protokoll übereinstimmt, ob die Kopie von der Quelle stammt, ob die Abfrage dasselbe Ergebnis erzeugt und ob die Schlussfolgerung über die Daten hinausgeht. Dabei geht es nicht nur um Kommas. Eine Überprüfung, die den Bericht lediglich verschönert, lässt den Fehler bestehen, der den Fall verändern könnte.

Bei einer Anhörung besteht die professionelle Antwort nicht darin, jedes Wort wie persönliches Eigentum zu verteidigen. Wird ein falsches Datum genannt, wird es korrigiert; war eine Quelle nicht verfügbar, wird dies erklärt; erlaubt die Methode eine Behauptung nicht, wird sie zurückgezogen. Die Autorität des Sachverständigen beruht auf der Qualität der Methode und der Bereitschaft zur Überprüfung, nicht auf der Weigerung, eine Einschränkung anzuerkennen. Widerspruch ist eine Prüfung des Systems, keine Beleidigung.



Abbildung 34. Die unabhängige Überprüfung versucht, Fehler in Quelle, Methode und Ableitung vor der Übermittlung zu finden. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Fragen zur Widerlegung
Kann ich das genaue Objekt finden? Kann ich die Abfrage wiederholen? Ist die Quelle unabhängig von der bewerteten Version? Gibt es eine andere vereinbare Erklärung? Was wurde nicht geprüft? Welche Behauptung entfällt, wenn ich eine Prämisse zurückziehe?

11.7 Übermittlung, Anhänge und späterer Zugriff

Das Übermittlungspaket enthält Bericht, Manifest, referenzierte Anhänge und gegebenenfalls kontrollierte Kopien. Die Anhänge werden im Text und in den Dateien gleich benannt. Wird eine öffentliche Version übermittelt, werden personenbezogene und geheime Daten getrennt, ohne die vollständig aufbewahrte Version zu vernichten. Der Bericht veröffentlicht keine Passwörter, privaten Schlüssel oder Informationen, die einen neuen Schaden ermöglichen.
Es wird geprüft, ob die Datei geöffnet werden kann, ob die Bilder lesbar und die internen Links funktionsfähig sind und ob die zitierten Anhänge vorhanden sind. Die elektronische Übermittlung verwendet einen autorisierten Kanal, gegebenenfalls Verschlüsselung und eine Empfangsbestätigung. Der Hashwert des Berichts ermöglicht die Versionskontrolle, macht seinen Inhalt jedoch nicht wahr. Das übermittelte Objekt muss auch Jahre später mit verfügbarem Format und Kontext überprüft werden können.

Ergebnis des Kapitels
Ein Bericht, der jede Frage des Auftrags beantwortet, seine Quellen identifiziert, Beobachtung und Ableitung trennt, Widersprüche bewahrt, Einschränkungen ausweist und ausreichende Anhänge für eine unabhängige Überprüfung enthält.

Kapitel 12. Fehler, Lernen und öffentlicher Dienst

12.1 Fehler werden nicht durch Umschreiben der Vergangenheit korrigiert

Jedes reale Verfahren enthält unvollkommene Entscheidungen: Jemand hat vor dem Fotografieren angeschlossen, die Zeitzone vergessen, einen Ausdruck statt der Datei erhalten oder einen mehrdeutigen Namen verwendet. Die professionelle Antwort besteht nicht darin, das Ereignis zu löschen und ein ideales Protokoll zu erstellen. Das Vorgefallene wird aufbewahrt, sein Umfang dokumentiert und geprüft, ob die Informationen aus einer anderen Quelle wiederhergestellt werden können. Verbesserung beginnt mit der Wahrheit der Akte, nicht mit ihrem äußeren Erscheinungsbild.

Eine nachträgliche Korrektur kann Schaden begrenzen, erzeugt jedoch keine rückwirkende Verwahrung. Wird heute ein Hashwert einer vor einem Monat erhaltenen Datei berechnet, gilt der Wert ab heute; er belegt nicht, dass das Objekt den Vormonat über unverändert blieb. Wird ein zweiter Export angefordert, wird er als neues Objekt mit eigener Entgegennahme aufbewahrt und mit dem ersten verglichen. Diese Unterscheidung schützt Untersuchung und Personen.



Abbildung 35. Das Original wird aufbewahrt; die Analyse erfolgt mit einer kontrollierten Kopie. Ausnahmen werden begründet und dokumentiert. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

12.2 Fehler bei Entgegennahme und Sicherung

Ausschalten aus Gewohnheit kann Speicherinhalte und Sitzungen vernichten; unkontrolliertes Eingeschaltetlassen kann Daten weiter verändern. Die Arbeit am Original kann die Unterscheidung zwischen ursprünglichen und analysebedingten Änderungen verhindern. Ein Telefon in einer antistatischen Tasche als Faraday-Lösung zu bezeichnen verwechselt zwei Funktionen. Verpackung ohne Kennung verhindert zu erkennen, ob das zurückgegebene Objekt dasselbe ist. Diese Fehler werden nicht durch mehr Werkzeuge gelöst, sondern durch Zustand, Befugnis, Funktion und Dokumentation verhindert.
Auch die Behandlung von Zubehör als irrelevant ist ein Fehler. Ein Kabel oder Adapter erklärt die Verbindung; ein zusätzlicher Speicher kann die Quelle enthalten; ein Netzteil ermöglicht, den Zustand bis zur Entscheidung zu erhalten. Die Entgegennahme muss den Gesamtzusammenhang prüfen, ohne aus Neugier etwas zu verändern. Fotografieren, identifizieren, verknüpfen und Unterstützung anfordern sind einfache Handlungen, die unmögliche Erklärungen Jahre später vermeiden.

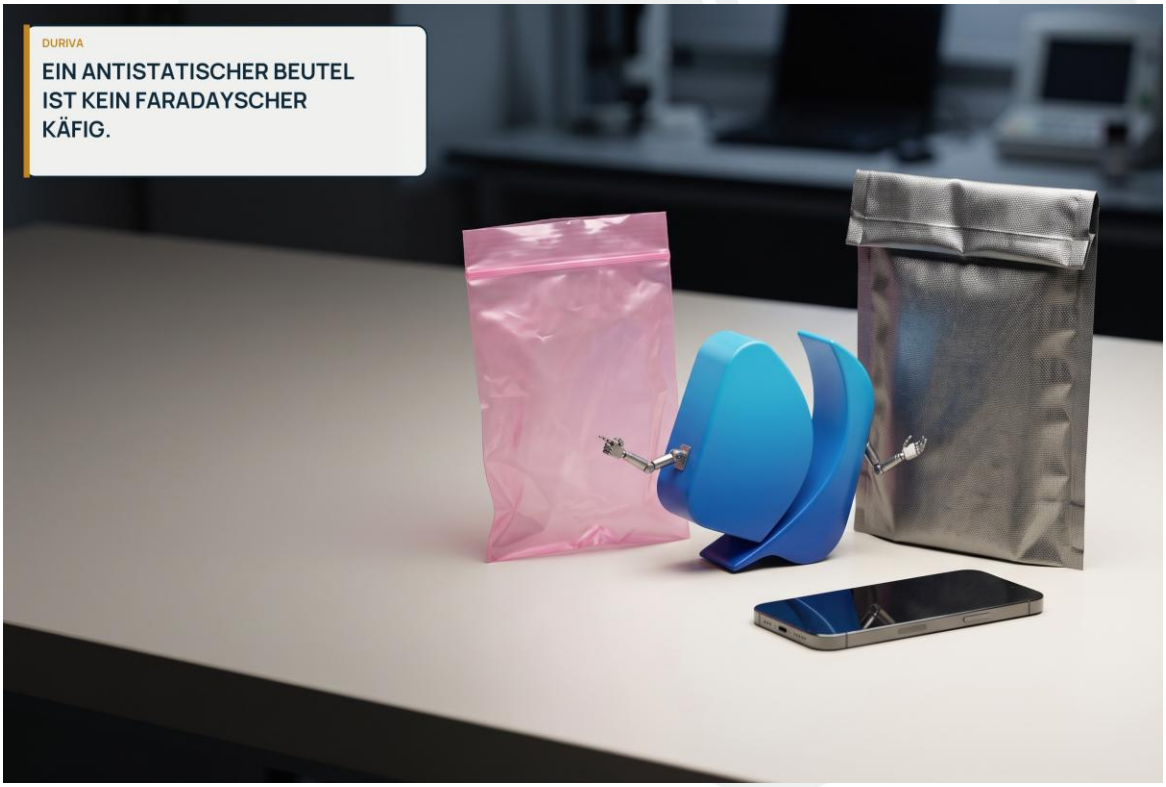


Abbildung 36. Elektrostatischer Schutz und Hochfrequenzabschirmung erfüllen unterschiedliche Funktionen. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

12.3 Fehler bei Quelle, Erfassung und Export

Ein Bildschirmfoto ohne URL, Datum, Konto und Kontext ist wie das Foto einer herausgerissenen Seite: Es ermöglicht, ein Fragment zu lesen, aber nicht, das Buch zu kennen. Die native Quelle ist aufzubewahren, sofern vorhanden; das Bildschirmfoto wird mit Pfad und

Zeitpunkt sowie der Person dokumentiert, die es erstellt hat. Ist nur die Visualisierung vorhanden, wird dies angegeben und nicht behauptet, der gesamte Verlauf sei geprüft worden. Das Bild kann nützlich sein, ohne als vollständiges Universum ausgegeben zu werden.
Ein Export ohne Filter, Zeitzone, Rolle und Feldverzeichnis kann eine korrekte und dennoch unverständliche Datei erzeugen. Dasselbe Problem entsteht, wenn nur eine PDF-Datei der Gesprächsdatenliste empfangen und die E-Mail mit der Integritätserklärung verworfen wird. Das robuste Verfahren fordert natives Format, Parameter, Prozess, Felder, Einschränkungen, Hashwert im Nachrichtentext und EML-Übermittlung an. Das ist keine Bürokratie, sondern die Information, die zum Verständnis des Vorhandenen erforderlich ist.



Abbildung 37. Ohne URL, Datum, Konto und Kontext bleibt ein Bildschirmfoto unvollständig, auch wenn das Bild scharf ist. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

12.4 Interpretationsfehler

Eine IP-Adresse einer Person zuzuordnen, ohne Zuweisung, Sitzung, Gerät, gemeinsame Nutzung und Kontext zu prüfen, macht aus einem Netzdatum eine physische Identität. Eine Antenne als Wohnadresse zu interpretieren, macht aus Abdeckung Anwesenheit. Ein Datum für unveränderlich oder für völlig nutzlos zu halten, sind zwei Versionen desselben Problems: nicht zu fragen, was das Feld erzeugt hat. Die seriöse Analyse schwankt nicht zwischen Leichtgläubigkeit und Geringschätzung; sie bewertet jede Quelle nach ihrem Mechanismus und ihrer Bestätigung.

Detektoren synthetischer Inhalte erfordern dieselbe Vorsicht. Ein Prozentsatz identifiziert für sich allein weder Urheberschaft noch Werkzeug oder Verhalten. Komprimierung, Zuschneiden, erneutes Aufnehmen und das Training des Detektors können das Ergebnis verändern. Datei, Version, Veröffentlichung, Verlauf und Kontext werden aufbewahrt; Methoden werden verglichen und falsch positive und falsch negative Ergebnisse erläutert. Ein Hinweis kann eine Quellenanfrage leiten, die Quelle jedoch nicht ersetzen.



Abbildung 38. Ein KI-Detektor liefert Hinweise mit Grenzen; er ersetzt weder Datei, Verlauf, Kontext noch Bestätigung. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

12.5 Juristische Fehler und Fehler bei der Gültigkeit

Eine Entsprechung aufgrund von Wortähnlichkeit kann gefährlicher sein als kein Zitat. Einfache, fortgeschrittene, digitale und qualifizierte Signaturen erzeugen nicht in allen Ländern dieselben Wirkungen. Eine Bankregel gilt nicht für jedes Unternehmen. Eine Archivnorm löst nicht jeden privaten Streit. Ein Gesetzesvorhaben ist kein Dekret. Die brauchbare Quellenangabe enthält Instrument, Artikel, Funktion, Geltungsbereich, Version und offizielle Quelle; jeder nicht überprüfte Teil wird erklärt.

Der Übergang des CNPCF zeigt, dass Erklärungen und Reformen vor der Wahl des Rechtsregimes geprüft werden müssen. Die Aufhebung besonderer KI-Bestimmungen in San Luis Potosí zeigt, dass auch eine viel diskutierte Reform ihre Gültigkeit verlieren kann. Das Handbuch versucht nicht, das Recht einzufrieren: Es vermittelt, es zu aktualisieren, ohne die

Methode zu verlieren. Die juristische Version wird zum Zeitpunkt des Falls geprüft und im Änderungsprotokoll registriert.[25][26]



Abbildung 39. Die Prüfung von Gültigkeit, Geltungsbereich und Reform verhindert, dass eine historische Quellenangabe zur aktuellen Grundlage wird. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

12.6 Gelernte Lektionen, die das Verfahren verändern

Eine gelernte Lektion muss zu einer sichtbaren Änderung führen. Trifft ein Export ohne Zeitzone ein, wird die Anfrage geändert, um sie anzufordern. Wurden zwei Objekte verwechselt, werden Kennung und Fotografie überprüft. Ändert ein Werkzeug das Format, werden Validierung und Beispiel aktualisiert. Nur einen weiteren Satz in einen Vorfallsordner zu schreiben, ohne das Verfahren zu ändern, erzeugt lediglich dokumentiertes Bedauern.
Die Überprüfung wird nach Risiko und Umgebungsänderungen geplant, nicht nach einem leeren Kalender. Offizielle Quellen, Werkzeugversionen, Anbieterformate und Speicherbedingungen werden geprüft. Bei der Aktualisierung des Handbuchs wird der anwendbare Inhalt ersetzt und der Verlauf aufbewahrt, statt widersprüchliche Anmerkungen

[25]Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350. Zusammenstellung mit Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von Erklärungen ab.Offizielle Online-Quelle
[26]San Luis Potosí. Gaceta Parlamentaria, 30-07-2026: Aufhebung von 187 Ter und des Kapitels mit 272 Bis und 272 Ter. Historischer Hintergrund, keine geltende Regel.Offizielle Online-Quelle

anzuhäufen. Historische Protokolle werden nicht verändert; das aktuelle Verfahren wird verbessert.

Fiktives Vorkommnis	Folge	Überprüfbare Änderung
Anhang ohne EML-Datei	Hashwert-Erklärung und Übermittlungskontext gehen verloren.	Die Empfangscheckliste verlangt EML-Datei, Anhänge und Vergleich.
Datum ohne Zeitzone	Die Chronologie kann Ereignisse verschieben.	Vorlage mit wörtlichem Wert, Zeitzone, Umrechnung und Unsicherheit.
Siegel ohne Protokoll gewechselt	Die Öffnung kann nicht rekonstruiert werden.	Obligatorisches Ereignis für Öffnen und Erneuern.
Schlussfolgerung über den Befund hinaus	Die Ableitung hält einer Widerlegung nicht stand.	Überprüfung der Prämissen und Tabelle der zulässigen Aussagen.
Veraltete Vorschrift	Eine nicht mehr zutreffende Wirkung wird angewendet.	Gültigkeitsprüfung mit Quelle und Konsultationsdatum.

12.7 Das letzte Ziel: den nächsten Übergriff verhindern

Dieses Handbuch soll nicht Personen ausbilden, die mehr technisches Papier erzeugen können. Es soll dazu beitragen, dass eine korrekte Entgegennahme eine Anklage auf Grundlage des falschen Objekts verhindert; dass eine ehrliche Chronologie eine Verurteilung auf Grundlage inkompatibler Uhren verhindert; dass ein Unternehmen die Aufzeichnungen bewahrt, die zeigen können, was geschehen ist; und dass eine Person versteht, warum ein Bildschirmfoto nicht genügt und was sie anfordern kann. Technik wird zum Dienst, wenn sie Willkür verringert.

Mit offenen Händen zu geben bedeutet nicht, Geheimnisse zu veröffentlichen oder eine Anleitung zum Schaden anzubieten. Es bedeutet, Grundlagen für würdiges Arbeiten zu teilen: identifizieren, schützen, fragen, überprüfen, Grenzen anerkennen und korrigieren. Wissen wird nicht wie in einer geschlossenen Faust zurückbehalten. Es wird mit einer Methode weitergegeben, damit andere es besser machen können und keine menschliche oder technische Autorität dort Glauben verlangen muss, wo sie Überprüfung anbieten sollte.

Abschluss des Handbuchs

Beweise zu bewahren bedeutet, die Möglichkeit der Wahrheit zu bewahren. Die Methode verspricht keinen Sieg: Sie verspricht, dass die Behauptung überprüft und der Fehler erkannt werden kann und dass die Schlussfolgerung nicht größer wird als die Tatsachen.

Anhang A. Funktionale juristische Entsprechungen

Untersuchte Gerichtsbarkeiten: Mexiko, Peru, Chile, Argentinien, Kolumbien, Ecuador und Spanien/Europäische Union. Stand der Dokumentenprüfung: 9. November 2026. Leitprinzip ist die funktionale Entsprechung, nicht die normative Identität.

Zusammenfassung

Diese Matrix beantwortet eine operative Frage: Welche Vorschrift erfüllt in jeder Gerichtsbarkeit die Funktion, die das Handbuch dokumentieren muss? Ausgangspunkt ist nicht die Suche nach einem Artikel mit derselben Nummer oder einem ähnlichen Wortlaut. Die funktionale Entsprechung ermöglicht den Vergleich der juristischen Anerkennung elektronischer Dokumente, der Schriftform, Zurechnung, Integrität, des Originalbegriffs, der Zugänglichkeit, Aufbewahrung, Zulässigkeit, Bewertung und Beweislast sowie sektoraler Pflichten für Aufzeichnungen und Vorfälle. Zwei Bestimmungen können denselben Zweck mit unterschiedlichen Vermutungen, Adressaten, Fristen und Folgen verfolgen; eine thematische Übereinstimmung darf daher niemals als Behauptung identischer prozessualer Wirkungen formuliert werden.
Das Ergebnis zeigt eine gemeinsame, aber nicht einheitliche Struktur. Mexiko, Kolumbien und Ecuador enthalten besonders klare Regeln für Datennachrichten, Schriftform, Original, Integrität und Aufbewahrung. Chile und Argentinien unterscheiden präzise die Wirkungen der verschiedenen Signaturklassen. Peru verteilt das Regime auf die Ley 27269, ihre Verordnung, das Zivilprozessgesetzbuch, Archivnormen und die SBS-Regulierung. Spanien kombiniert eIDAS, Prozessrecht und Vorschriften für Zahlungsdienste. In allen Fällen genügt die elektronische Form nicht, um Urheberschaft, Integrität oder Wahrheitsgehalt zu beweisen. Das Handbuch muss Quelle, Methode, Kontext, Kontinuität und Überprüfbarkeit verlangen; der Hashwert hilft beim Vergleichen von Objekten, beweist jedoch für sich allein weder, wer eine Datei erstellt hat, noch, ob sich das Geschilderte ereignet hat.

1. Methode und Grenzen des Vergleichs

Verwendet wurden amtliche Texte, gesetzliche Zusammenstellungen, Amtsblätter und Dokumente von Regulierungsstellen. Jeder Eintrag enthält das Rechtsinstrument und die tatsächlich aufgefundenen Artikel. „Direkt“ bedeutet, dass die Funktion ausdrücklich mit einer ähnlichen Struktur abgedeckt ist; „teilweise“ zeigt, dass nur ein Aspekt abgedeckt ist oder eine andere Vorschrift erforderlich wird; „sektoral“ begrenzt die Regel auf Archive, Signaturen, Zahlungen oder beaufsichtigte Stellen; „nicht belegt“ bedeutet, dass die Recherche keine ausreichend nachgewiesene allgemeine Regel gefunden hat. Die letzte Kategorie behauptet nicht, dass das Land keine Regulierung besitzt, sondern dass mit dem verfügbaren Material keine Entsprechung erfunden werden darf.
Die Recherche hat drei praktische Grenzen. Erstens kann eine Zusammenstellung Reformen zu unterschiedlichen Daten enthalten; in jedem Fall muss die für Sachverhalt und Verfahren geltende Version geprüft werden. Zweitens sind Zivil-, Handels-, Straf-, Verwaltungs-, Archiv- und Finanzvorschriften aufgrund von Wortähnlichkeit nicht austauschbar. Drittens sind

Zulässigkeit, Authentizität, Bewertung und Beweislast unterschiedliche Fragen: Eine Vorschrift kann die Vorlage eines Dokuments erlauben, ohne ihm volle Beweiskraft zu verleihen oder die Beweislast umzukehren. Folglich orientiert diese Matrix die technische Dokumentation und das Auffinden von Vorschriften, ersetzt jedoch weder die juristische Analyse der Akte noch eine gerichtliche Entscheidung.

Niveau	Operative Bedeutung	Regel für die Zitation im Handbuch
Direkt	Die Funktion ist ausdrücklich und mit einer vergleichbaren Struktur anerkannt.	Anforderungen, Ausnahmen und Wirkungen erläutern; nicht nur den Wortlaut kopieren.
Teilweise	Die Vorschrift deckt einen Teil der Funktion ab oder erfordert eine prozessuale Ergänzung.	Das ergänzende Rechtsinstrument zitieren und abgrenzen, was nicht abgedeckt ist.
Sektoral	Die Regel beschränkt sich auf Archive, Zertifizierung, Zahlungen oder beaufsichtigte Stellen.	Nicht auf alle digitalen Beweise oder alle Personen ausdehnen.
Nicht belegt	Eine ausreichend überprüfbare Entsprechung wurde nicht gefunden.	Schreiben Sie „in dieser Prüfung nicht belegt“, niemals „nicht vorhanden“.

2. Zentrale Matrix nach Rechtsfunktion

Die Tabelle konzentriert die Funktionen von Anerkennung und Form. Die Quellenangaben stehen in den Zellen, damit jede Aussage mit ihrer Quelle verbunden bleibt. Die Kategorien bewerten nicht die Qualität eines Rechtssystems: Sie beschreiben seinen Nutzen für das Handbuch und den Grad der nachgewiesenen Entsprechung. Insbesondere verlangt der Begriff des „Originals“ nicht immer die Aufbewahrung eines physischen Geräts; mehrere Rechtsordnungen behandeln ihn über Integrität ab der endgültigen Form und spätere Zugänglichkeit. Das Handbuch muss sowohl den Aberglauben an den Träger als auch die Annahme vermeiden, ein Bildschirmfoto bewahre alle Eigenschaften der Ausgangsdatei.
Kombiniert eine Zelle mehrere Vorschriften, ist die Funktion verteilt und darf nicht vollständig dem zuerst genannten Instrument zugeschrieben werden. Peru ist besonders lehrreich: Die Ley 27269 regelt digitale Signaturen und Zertifikate; sie enthält für sich allein kein allgemeines Regime für Original und Aufbewahrung von Datennachrichten. Die Zulassung digital signierter Dokumente ergibt sich aus ihrer Verordnung, und die Aufbewahrung von Mikroformen unterliegt einem besonderen archivischen Regime. Diese Trennung verhindert eine elegante, aber falsche Entsprechung.

Anerkennung des elektronischen Dokuments

Jurisdiktion	Regel, Umfang und Einschränkung
Mexiko	CCom 89 und 89 Bis: Neutralität und keine Zurückweisung aufgrund einer Datennachricht.
Peru	Ley 27269, Artikel 1–2, für elektronische Signatur; besonderer Geltungsbereich, kein vollständiges Dokumentenregime.
Chile	Ley 19.799, Artikel 1–3: Gleichwertigkeit des Trägers und Gültigkeit mit Ausnahmen.
Argentinien	Ley 25.506, Artikel 1, 3 und 6, für digitale Signatur und digitales Dokument.
Kolumbien	Ley 527, Artikel 5: Wirkungen werden nicht allein aufgrund einer Datennachricht verweigert.
Ecuador	Ley 67, Artikel 2: gleicher Rechtswert wie schriftliche Dokumente, vorbehaltlich von Gesetz und Verordnung.
Spanien / EU	eIDAS 46: Wirkungen und Zulässigkeit werden nicht allein aufgrund des elektronischen Formats verweigert.

Quellen der Tabelle:[27][28][29][30][31][32][33]

Schriftform und spätere Zugänglichkeit

Jurisdiktion	Regel, Umfang und Einschränkung
Mexiko	CCom 93 und 93 Bis; CNPCF 349 verlangt Zugänglichkeit.

[27]Código de Comercio de México, Artikel 89–94 und 1205: Neutralität, Zurechnung, Schriftform, Original, Integrität, Zugänglichkeit und Zulassung von Datennachrichten. Amtliche Zusammenstellung.Offizielle Online-Quelle
[28]Peru. Ley 27269 de Firmas y Certificados Digitales und Verordnung DS 052-2008-PCM. Besonderes Regime für Signatur und Zulassung digital signierter Dokumente.Offizielle Online-Quelle
[29]Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert.Offizielle Online-Quelle
[30]Argentinien. Ley 25.506 de Firma Digital, Artikel 1 und 5–9: digitales Dokument, Beweislast bei Berufung auf eine bestrittene elektronische Signatur und begrenzte Vermutungen.Offizielle Online-Quelle
[31]Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur.Offizielle Online-Quelle
[32]Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur.Offizielle Online-Quelle
[33]Reglamento (UE) 910/2014 eIDAS, Artikel 25–26 und 46: keine Diskriminierung elektronischer Signaturen und Dokumente aufgrund ihres Formats, fortgeschrittene elektronische Signatur und Rechtswirkungen qualifizierter elektronischer Signaturen.Offizielle Online-Quelle

Jurisdiktion	Regel, Umfang und Einschränkung
Peru	Verordnung 052-2008-PCM, Artikel 3, für Signaturanforderungen; archivische Zugänglichkeit wird gesondert geregelt.
Chile	Ley 19.799, Artikel 2.d verlangt geeignete Speicherung für spätere Nutzung; Artikel 3, Schriftform.
Argentinien	Ley 25.506, Artikel 6: Das digitale Dokument erfüllt die Schriftform; Decreto 182/2019, Aufbewahrung.
Kolumbien	Ley 527, Artikel 6: Nachricht für spätere Einsichtnahme zugänglich.
Ecuador	Ley 67, Artikel 6: Informationen für spätere Einsichtnahme zugänglich.
Spanien / EU	eIDAS enthält keine mit 93 Bis identische allgemeine Regel; LSSI und sektorale Vorschriften ergänzen. Teilweise, keine erzwungene Entsprechung.

Quellen der Tabelle:[343536373839]

Zurechnung und Signatur

Jurisdiktion	Regel, Umfang und Einschränkung
Mexiko	CCom 90–92; CNPCF 349; Vermutung nach zuverlässiger und zurechenbarer Methode.
Peru	Ley 27269, Artikel 3, und Verordnung 3–4; digitale Signatur in IOFE und Zulassung signierter Dokumente.

[34]Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350. Zusammenstellung mit Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von Erklärungen ab.Offizielle Online-Quelle
[35]Peru. Reglamento de la IOFE, DS 052-2008-PCM, Artikel 3 und 4: Anforderung an und Zulassung von digital signierten elektronischen Dokumenten.Offizielle Online-Quelle
[36]Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert.Offizielle Online-Quelle
[37]Argentinien. Decreto 182/2019: digitale Aufbewahrung und beglaubigte Kopien zu den vorgesehenen Fristen und Bedingungen.Offizielle Online-Quelle
[38]Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur.Offizielle Online-Quelle
[39]Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur.Offizielle Online-Quelle

Jurisdiktion	Regel, Umfang und Einschränkung
Chile	Ley 19.799, Artikel 2.f–g und 4–5: einfache und fortgeschrittene Signatur haben nicht dieselben Wirkungen.
Argentinien	Ley 25.506, Artikel 5, 7–9: Beweislast bei Berufung auf eine bestrittene elektronische Signatur; Vermutungen für eine gültige digitale Signatur.
Kolumbien	Ley 527, Artikel 7, 16–17 und 28: zuverlässige Methode, Zurechnung und Merkmale der digitalen Signatur.
Ecuador	Ley 67, Artikel 10, 13–16: Herkunft, Identität und Wirkungen der elektronischen Signatur.
Spanien / EU	eIDAS 25–26: keine Diskriminierung einfacher Signaturen; Gleichwertigkeit qualifizierter Signaturen mit handschriftlichen; Anforderungen an fortgeschrittene Signaturen.

Quellen der Tabelle:[40][41][42][43][44][45][46]

Original und Integrität ab der endgültigen Form

Jurisdiktion	Regel, Umfang und Einschränkung
Mexiko	CCom 93 Bis und CNPCF 350: Integrität ab endgültiger Erzeugung und Zugänglichkeit; Sonderregel für öffentliche Ketten in Artikel 350.
Peru	Als allgemeine Regel in der Ley 27269 nicht belegt. Mikroformen und archivische Integrität unterliegen einem besonderen Regime in DL 681 und DS 001-2000-JUS.

[40]Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350. Zusammenstellung mit Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von Erklärungen ab.Offizielle Online-Quelle
[41]Peru. Reglamento de la IOFE, DS 052-2008-PCM, Artikel 3 und 4: Anforderung an und Zulassung von digital signierten elektronischen Dokumenten.Offizielle Online-Quelle
[42]Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert.Offizielle Online-Quelle
[43]Argentinien. Ley 25.506 de Firma Digital, Artikel 1 und 5–9: digitales Dokument, Beweislast bei Berufung auf eine bestrittene elektronische Signatur und begrenzte Vermutungen.Offizielle Online-Quelle
[44]Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur.Offizielle Online-Quelle
[45]Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur.Offizielle Online-Quelle
[46]Reglamento (UE) 910/2014 eIDAS, Artikel 25–26 und 46: keine Diskriminierung elektronischer Signaturen und Dokumente aufgrund ihres Formats, fortgeschrittene elektronische Signatur und Rechtswirkungen qualifizierter elektronischer Signaturen.Offizielle Online-Quelle

Jurisdiktion	Regel, Umfang und Einschränkung
Chile	Ley 19.799, Artikel 2.g erkennt Änderungen bei fortgeschrittener Signatur; Artikel 5 bemisst den Wert nach Dokumentenart. Teilweise.
Argentinien	Ley 25.506, Artikel 8: Vermutung der Integrität bei wahrer digitaler Verifizierung. Direkt für digitale Signatur, nicht universell für jede Datei.
Kolumbien	Ley 527, Artikel 8–9: zuverlässige Gewährleistung der Integrität ab endgültiger Form und Vorlage.
Ecuador	Ley 67, Artikel 7: Nachweis der Integrität ab endgültiger Form; Verordnung, Artikel 6.
Spanien / EU	eIDAS 26.d verknüpft Daten zur Erkennung von Änderungen; LEC 326 regelt die Anfechtung von Authentizität und Integrität. Teilweise und prozessual.

Quellen der Tabelle:[47][48][49][50][51][52][53]

Aufbewahrung und Kontext von Herkunft, Ziel und Datum

Jurisdiktion	Regel, Umfang und Einschränkung
Mexiko	NOM-151 für Aufbewahrung und Digitalisierung; CCom 93 Bis für Zugänglichkeit.
Peru	DS 001-2000-JUS für Mikroformen; IOFE-Verordnung für Signatur und Zertifikate. Sektoral.

[47]Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350. Zusammenstellung mit Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von Erklärungen ab.Offizielle Online-Quelle
[48]Peru. DL 681 und DS 001-2000-JUS: fortschrittliche Technologien, Mikroformen, Authentizität, Integrität und archivische Aufbewahrung. Sektoraler Geltungsbereich.Offizielle Online-Quelle
[49]Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert.Offizielle Online-Quelle
[50]Argentinien. Ley 25.506 de Firma Digital, Artikel 1 und 5–9: digitales Dokument, Beweislast bei Berufung auf eine bestrittene elektronische Signatur und begrenzte Vermutungen.Offizielle Online-Quelle
[51]Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur.Offizielle Online-Quelle
[52]Ecuador. Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos: Einbeziehung von Anhängen, Dematerialisierung, Integrität und Verifizierung. Offizielle Veröffentlichung der Función Judicial.Offizielle Online-Quelle
[53]Spanien. Ley de Enjuiciamiento Civil, Artikel 326 und 384: private Dokumente, Anfechtung, Instrumente zur Archivierung, Kenntnisnahme oder Wiedergabe von Daten, Prüfung, Verwahrung und gesunde Kritik.Offizielle Online-Quelle

Jurisdiktion	Regel, Umfang und Einschränkung
Chile	Ley 19.799, Artikel 2.d und 5: spätere Nutzung und beglaubigte Datierung für das Datum eines privaten Instruments mit fortgeschrittener Signatur.
Argentinien	Decreto 182/2019, Artikel 5: digitale Aufbewahrung für bestimmte Fristen und beglaubigte Kopien.
Kolumbien	Ley 527, Artikel 12–13: Format, exakte Wiedergabe, Herkunft, Ziel, Datum und Uhrzeit; Dritte.
Ecuador	Ley 67, Artikel 8: Zugänglichkeit, Format, Herkunft, Ziel, Datumsangaben, Uhrzeiten und Integrität; Dritte.
Spanien / EU	Sektorale Vorschriften und Aufbewahrungsvorschriften; in dieser Prüfung ist keine einheitliche allgemeine Klausel äquivalent zu Ley 527.12 belegt.

Quellen der Tabelle:[54][55][56][57][58][59]

Zulässigkeit und Beweiswürdigung

Jurisdiktion	Regel, Umfang und Einschränkung
Mexiko	CCom 1205 lässt Datennachrichten zu; CFPC 210-A und CNPCF 348–350 legen Zuverlässigkeit, Zurechnung, Zugänglichkeit und Integrität fest.
Peru	CPC 188–197: Zweck, Rechtmäßigkeit, typische und atypische Mittel und Beweislast; Verordnung 4 für digital signierte Dokumente.

[54]NOM-151-SCFI-2016, Aufbewahrung und Digitalisierung von Datennachrichten, veröffentlicht am 30-03-2017. Anforderungen an Bescheinigung, Integrität, Zugänglichkeit und digitalen Fingerabdruck.Offizielle Online-Quelle
[55]Peru. DL 681 und DS 001-2000-JUS: fortschrittliche Technologien, Mikroformen, Authentizität, Integrität und archivische Aufbewahrung. Sektoraler Geltungsbereich.Offizielle Online-Quelle
[56]Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert.Offizielle Online-Quelle
[57]Argentinien. Decreto 182/2019: digitale Aufbewahrung und beglaubigte Kopien zu den vorgesehenen Fristen und Bedingungen.Offizielle Online-Quelle
[58]Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur.Offizielle Online-Quelle
[59]Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur.Offizielle Online-Quelle

Jurisdiktion	Regel, Umfang und Einschränkung
Chile	Ley 19.799, Artikel 5: voller Beweis in den vorgesehenen Fällen; sonstige Dokumente nach allgemeinen Regeln.
Argentinien	CCyC 318–319: Korrespondenz unabhängig vom Medium und Bewertung der Zuverlässigkeit von Trägern und Verfahren.
Kolumbien	Ley 527, Artikel 10–11: Zulässigkeit, gesunde Kritik, Erzeugung, Archivierung, Kommunikation, Integrität und Aussteller.
Ecuador	Ley 67, Artikel 14: elektronische Signatur als Beweis zugelassen; Artikel 2 und 7 setzen Wirksamkeit und Original voraus.
Spanien / EU	eIDAS 46 und LEC 326/384: Zulassung, Anfechtung, Vertrauensdienste und gesunde Kritik.

Quellen der Tabelle:[60][61][62][63][64][65][66]

Beweislast und Vermutungen

Jurisdiktion	Regel, Umfang und Einschränkung
Mexiko	Die Existenz einer Datei begründet keine allgemeine Urheberschaftsvermutung; die Methode und ihre Zurechnung müssen nachgewiesen werden.
Peru	CPC 196: Beweislast für die Person, die Tatsachen ihres Anspruchs behauptet oder durch neue Tatsachen widerspricht, sofern keine andere Regel gilt.

[60]Código Federal de Procedimientos Civiles, Artikel 210-A: Zuverlässigkeit der Methode, Zurechnung, Zugänglichkeit und Integrität elektronischer Informationen. Der Code wurde durch Dekret vom 07-06-2023 aufgehoben und unterliegt einem schrittweisen Übergangsregime.Offizielle Online-Quelle

[61]Peru. Código Procesal Civil, Artikel 188–197 und 245.5: Zweck, Rechtmäßigkeit, Mittel, Beweislast, Bewertung und Datumsbestimmung durch technische Mittel.Offizielle Online-Quelle

[62]Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert.Offizielle Online-Quelle

[63]Argentinien. Código Civil y Comercial, Artikel 318–319: Korrespondenz unabhängig vom Medium und Bewertung der Zuverlässigkeit von Trägern und technischen Verfahren.Offizielle Online-Quelle

[64]Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur.Offizielle Online-Quelle

[65]Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur.Offizielle Online-Quelle

[66]Spanien. Ley de Enjuiciamiento Civil, Artikel 326 und 384: private Dokumente, Anfechtung, Instrumente zur Archivierung, Kenntnisnahme oder Wiedergabe von Daten, Prüfung, Verwahrung und gesunde Kritik.Offizielle Online-Quelle

Jurisdiktion	Regel, Umfang und Einschränkung
Chile	Wert nach Art des Instruments und der Signatur; ein privates Datum erfordert besondere Aufmerksamkeit für die beglaubigte Datierung.
Argentinien	Ley 25.506, Artikel 5 und 7–8: Beweislast bei Berufung auf eine bestrittene elektronische Signatur; Vermutungen nur im jeweiligen Rechtsregime.
Kolumbien	Ley 527, Artikel 17, 21 und 28: begrenzte Vermutungen von Herkunft, Empfang und Signaturabsicht.
Ecuador	Ley 67, Artikel 10: Vermutung der Herkunft vorbehaltlich des Gegenbeweises und von Ausnahmen; keine automatische menschliche Urheberschaft.
Spanien / EU	LEC 326.4: Vermutung der bestrittenen Eigenschaft und der ordnungsgemäßen Leistung bei einem qualifizierten Dienst, entsprechend seinen Bedingungen.

Quellen der Tabelle:[67][68][69][70][71]

3. Mexiko: Rechtsgrundlage und Übergang

Mexiko bietet eine vollständige Abfolge für das Handbuch, verlangt jedoch die Unterscheidung zwischen geltendem Handelsregime, historischem CFPC und schrittweisem Inkrafttreten des CNPCF. Artikel 210-A des CFPC erkennt Informationen, die durch elektronische, optische oder andere Technologien erzeugt oder übermittelt werden, als Beweis an und verlangt die Bewertung von Zuverlässigkeit der Methode, Zurechnung und Zugänglichkeit; ihr Original stützt sich auf Integrität ab der endgültigen Form. Der Código de Comercio enthält die materielle Architektur des elektronischen Handels: 89 und 89 Bis, Neutralität und Nichtdiskriminierung; 90–92, Zurechnung, Versand, Empfang und Empfangsbestätigungen; 93 und 93 Bis, Schriftform, Original, Integrität und Zugänglichkeit; 94, Ort von Versand und Empfang. Artikel

[67]Peru. Código Procesal Civil, Artikel 188–197 und 245.5: Zweck, Rechtmäßigkeit, Mittel, Beweislast, Bewertung und Datumsbestimmung durch technische Mittel.Offizielle Online-Quelle
[68]Argentinien. Ley 25.506 de Firma Digital, Artikel 1 und 5–9: digitales Dokument, Beweislast bei Berufung auf eine bestrittene elektronische Signatur und begrenzte Vermutungen.Offizielle Online-Quelle
[69]Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur.Offizielle Online-Quelle
[70]Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur.Offizielle Online-Quelle
[71]Spanien. Ley de Enjuiciamiento Civil, Artikel 326 und 384: private Dokumente, Anfechtung, Instrumente zur Archivierung, Kenntnisnahme oder Wiedergabe von Daten, Prüfung, Verwahrung und gesunde Kritik.Offizielle Online-Quelle

1205 wurde direkt in der amtlichen Zusammenstellung überprüft und lässt unter anderem Fotografien, Videos, Ton und Datennachrichten zu.[72]
Der CNPCF, dessen konsultierte amtliche Zusammenstellung die letzte Reform vom 15. Januar 2026 ausweist, enthält in den Artikeln 348–350 eine ähnliche Struktur und ergänzt Technologien wie Blockchain. Artikel 350 enthält außerdem eine besondere Beweisregel für Register öffentlicher Ketten, sofern keine Verletzung oder fehlende Zuverlässigkeit nachgewiesen wird; daraus darf nicht die allgemeine Behauptung abgeleitet werden, jedes verteilte Register sei authentisch. Der Übergang erfolgt schrittweise und hängt von Erklärungen ab. Die konsultierte Zusammenstellung behält die allgemeine Grenze des 1. April 2027; eine am 29. April 2026 im Gaceta Parlamentaria veröffentlichte Initiative schlug den 31. Januar 2030 als Ersatz vor, doch eine Initiative ist kein veröffentlichtes Dekret. Bevor dieser Übergang auf einen realen Fall angewendet wird, muss geprüft werden, ob es eine spätere Reform im DOF gab und welche Erklärung für das zuständige Gericht gilt.[73][74]

Das Instrument	Überprüfte Funktion	Genauigkeit, die das Handbuch bewahren muss
CFPC 210-A	Elektronische Informationen als Beweis; Zuverlässigkeit, Zurechnung, Zugänglichkeit und Integrität.	Sie ist die historische Grundlage des Übergangs, kein Artikel, der einfach seine Nummer ändert.
CNPCF 348–350	Anerkennung, Zuverlässigkeit, Original, Zugänglichkeit und Regel für öffentliche Ketten.	Schrittweises Inkrafttreten; Erklärung und Reformen zum Zeitpunkt des Falls prüfen.
CCom 89–94	Neutralität, Wirkungen, Zurechnung, Versand/Empfang, Schriftform, Original und Ort.	Eine Empfangsbestätigung nicht mit Wahrheitsgehalt des Inhalts oder gültiger Einwilligung in jedem Kontext verwechseln.
CCom 1205	Ausdrückliche Zulässigkeit von Datennachrichten und anderen Medien.	Zulässigkeit ist keine vollständige Beweiskraft und beseitigt weder Widerspruch noch Begutachtung.

[72]Código de Comercio de México, Artikel 89–94 und 1205: Neutralität, Zurechnung, Schriftform, Original, Integrität, Zugänglichkeit und Zulassung von Datennachrichten. Amtliche Zusammenstellung.Offizielle Online-Quelle
[73]Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350. Zusammenstellung mit Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von Erklärungen ab.Offizielle Online-Quelle
[74]Cámara de Diputados. Gaceta Parlamentaria, 29-04-2026. Initiative zur Änderung des Inkrafttretens des CNPCF auf den 31-01-2030. Es handelt sich um eine Initiative, nicht um ein veröffentlichtes Dekret.Offizielle Online-Quelle

Das Instrument	Überprüfte Funktion	Genauigkeit, die das Handbuch bewahren muss
NOM-151-SCFI-2016	Aufbewahrung, Digitalisierung, akkreditierter PSC, Hashwert, RFC 3161, Bescheinigungen und Zugänglichkeit.	Technische Anforderung für Aufbewahrung und Digitalisierung in ihrem Bereich, kein magisches Zertifikat für Urheberschaft oder Wahrheitsgehalt.
CNBV 316 Bis und Serie	Nachweise, Benachrichtigungen, Verschlüsselung, Zugriffe, Vorfälle, Vorkommnisse, Protokolle und Überprüfungen.	Jeder Artikel hat eigene Adressaten, Gegenstände und Fristen; „316 Bis“ darf nicht als eine einzige Verpflichtung zitiert werden.

Quellen der Tabelle:[7576777879]

Die NOM-151 erfordert eine technische Behandlung getrennt von den Verfahrensregeln. Ihr Nutzen liegt in der Aufbewahrung und Feststellung von Datennachrichten und in den Bedingungen der Digitalisierung, nicht in der Erklärung, dass alles Gespeicherte wahr ist. Die Normalisierungsseite des Wirtschaftssekretariats weist sie als gültig aus, während der DOF-Text die Anforderungen an Bescheinigung, Integrität und Zugänglichkeit konkretisiert. Das Handbuch muss Werkzeug, Version, Algorithmus, Datum und Zeitzone, Identität des Bearbeiters und die Beziehung zwischen Original, Kopie und Bescheinigung dokumentieren. Ein Zeitstempel oder eine Bescheinigung allein beweist weder menschliche Urheberschaft noch rechtmäßige Beschaffung oder Vollständigkeit eines Gesprächs.[8081]

Die CNBV-Regulierung gliedert sich wie folgt: 316 Bis, Nachweise; 316 Bis 1, Benachrichtigungen; 316 Bis 10, Verschlüsselung und Schutz; 316 Bis 11, Zugriffskontrolle; 316 Bis 12, Untersuchung und Meldung von Vorfällen mit Information an die Kommission innerhalb von fünf Kalendertagen; 316 Bis 14, Vorkommnisse und nicht anerkannte Vorgänge mit fünfjähriger Aufbewahrung; 316 Bis 15, Protokolle mit sicherer Aufbewahrung für 180 Tage

[75]Código Federal de Procedimientos Civiles, Artikel 210-A: Zuverlässigkeit der Methode, Zurechnung, Zugänglichkeit und Integrität elektronischer Informationen. Der Code wurde durch Dekret vom 07-06-2023 aufgehoben und unterliegt einem schrittweisen Übergangsregime.Offizielle Online-Quelle

[76]Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350. Zusammenstellung mit Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von Erklärungen ab.Offizielle Online-Quelle

[77]Código de Comercio de México, Artikel 89–94 und 1205: Neutralität, Zurechnung, Schriftform, Original, Integrität, Zugänglichkeit und Zulassung von Datennachrichten. Amtliche Zusammenstellung.Offizielle Online-Quelle

[78]NOM-151-SCFI-2016, Aufbewahrung und Digitalisierung von Datennachrichten, veröffentlicht am 30-03-2017. Anforderungen an Bescheinigung, Integrität, Zugänglichkeit und digitalen Fingerabdruck.Offizielle Online-Quelle

[79]Disposiciones de carácter general aplicables a las instituciones de crédito, Artikel 316 Bis, 316 Bis 1, 316 Bis 10 bis 17: Nachweise, Verschlüsselung, Zugriff, Vorfälle, Vorkommnisse, Protokolle und Überprüfungen.Offizielle Online-Quelle

[80]NOM-151-SCFI-2016, Aufbewahrung und Digitalisierung von Datennachrichten, veröffentlicht am 30-03-2017. Anforderungen an Bescheinigung, Integrität, Zugänglichkeit und digitalen Fingerabdruck.Offizielle Online-Quelle

[81]Secretaría de Economía. PLATIICA. Datenblatt der NOM-151-SCFI-2016 zur Aufbewahrung und Digitalisierung von Datennachrichten. Gültigkeitsprüfung und ergänzende Referenz zum DOF-Text.Offizielle Online-Quelle

und Bearbeitung von Nutzeranfragen innerhalb von zehn Werktagen; 316 Bis 17, Sicherheitsüberprüfungen mindestens jährlich. Diese Fristen werden weder auf andere Länder noch auf alle Unternehmensarten übertragen. Für ein Gutachten werden die mit Vorgang und Zeitraum verbundenen Aufzeichnungen angefordert, nicht undifferenziert „alle Server“.[82]

4. Peru: verteiltes Regime und finanzielle Aktualisierung

Peru erfordert, die Vorstellung eines einzigen Gesetzes für Datennachrichten aufzugeben. Die Ley 27269, geändert durch die Ley 27310, regelt digitale Signaturen und Zertifikate und umfasst im überprüften amtlichen Text 16 Artikel. Artikel 1 erkennt die elektronische Signatur an; Artikel 2 begrenzt ihren Geltungsbereich; Artikel 3 definiert die digitale Signatur mit asymmetrischer Kryptografie. Die durch DS 052-2008-PCM verabschiedete Verordnung entwickelt die IOFE und regelt in den Artikeln 3 und 4 die Gleichwertigkeit der in dieser Infrastruktur erzeugten digitalen Signatur sowie die Zulassung digital signierter elektronischer Dokumente als Beweis. Die Vorschrift selbst erkennt die Vielfalt elektronischer Signaturen an und erlaubt nicht, jedes eingefügte Symbol oder Bild als akkreditierte digitale Signatur zu behandeln.[8384]

Im Verfahrensrecht enthält das Zivilprozessgesetzbuch in den Artikeln 188–197 die allgemeinen Regeln: Zweck, Gelegenheit, Relevanz, Rechtmäßigkeit, typische und atypische Mittel, Beweis von Amts wegen, Beweislast und Bewertung. Artikel 192 nennt Parteierklärung, Zeugen, Dokumente, Sachverständigenuntersuchung und gerichtliche Inspektion; Artikel 193 lässt technische oder wissenschaftliche Hilfsmittel als atypische Mittel zu; Artikel 196 verteilt die Beweislast, sofern keine andere Bestimmung gilt. Artikel 245.5 erlaubt dem Richter, ein durch technische Mittel bestimmtes Datum als gewiss anzusehen, sofern diese ihn überzeugen. Für Archive umfassen DL 681 und DS 001-2000-JUS Technologien und Mikroformen, Authentizität, Integrität und Aufbewahrung; ihr Geltungsbereich darf nicht mit einer allgemeinen Originalregel für jede private Datei verwechselt werden.[8586]

Peruanisches Thema	Nützliche Regel	Operative Warnung
SBS 504-2021, Art. 12.6.g	Beweise für forensische Untersuchungen nach Vorfällen aufbewahren.	In ein dokumentiertes Verfahren überführen, nicht in eine undifferenzierte Sammlung.

[82]Disposiciones de carácter general aplicables a las instituciones de crédito, Artikel 316 Bis, 316 Bis 1, 316 Bis 10 bis 17: Nachweise, Verschlüsselung, Zugriff, Vorfälle, Vorkommnisse, Protokolle und Überprüfungen.Offizielle Online-Quelle

[83]Peru. Ley 27269 de Firmas y Certificados Digitales und Verordnung DS 052-2008-PCM. Besonderes Regime für Signatur und Zulassung digital signierter Dokumente.Offizielle Online-Quelle

[84]Peru. Reglamento de la IOFE, DS 052-2008-PCM, Artikel 3 und 4: Anforderung an und Zulassung von digital signierten elektronischen Dokumenten.Offizielle Online-Quelle

[85]Peru. Código Procesal Civil, Artikel 188–197 und 245.5: Zweck, Rechtmäßigkeit, Mittel, Beweislast, Bewertung und Datumsbestimmung durch technische Mittel.Offizielle Online-Quelle

[86]Peru. DL 681 und DS 001-2000-JUS: fortschrittliche Technologien, Mikroformen, Authentizität, Integrität und archivische Aufbewahrung. Sektoraler Geltungsbereich.Offizielle Online-Quelle

Peruanisches Thema	Nützliche Regel	Operative Warnung
SBS 504-2021, Art. 15	Der Superintendencia stehen Bericht über erhebliche Vorfälle und forensische Analyse zur Verfügung.	Der Bericht muss eine Managementzusammenfassung und technische Details enthalten.
SBS 504-2021, Artikel 17.3–17.4	Aufzeichnungen von Registrierung, Authentifizierungsversuchen und Vorgängen aufbewahren und schützen; Transaktionen überwachen.	Diese Aufzeichnungen sind besonders relevant für die Rekonstruktion von Abfolge und Authentifizierung, aber kein automatischer Beweis der physischen Identität.
SBS 2286-2024, neuer 20.3	Unternehmenshaftung für bestimmte nicht anerkannte Vorgänge, sofern nicht die Verantwortung des Nutzers nachgewiesen wird.	Dies ist die korrekte Änderung der 504-2021; keine falsche Nummerierung oder den früheren Text als unverändert zitieren.

Quellen der Tabelle:[8788]

Der Finanzvergleich muss diese Aktualisierung von 2024 widerspiegeln. Der geänderte Absatz 20.3 umfasst nicht anerkannte Vorgänge über digitale Kanäle ohne die Anforderung verstärkter Authentifizierung, in bestimmten Ausnahmefällen oder nachdem der Nutzer den Diebstahl oder Verlust von Anmeldedaten gemeldet hat, sofern nicht die Verantwortung des Nutzers nachgewiesen wird. Dies unterscheidet sich von der Behauptung, die Bank hafte immer oder die Verwendung von Anmeldedaten beweise stets eine Autorisierung. Das Gutachten muss Faktoren, Registrierung, Aufzeichnungen, Warnmeldungen, Gerätekontext und Abfolge untersuchen und die technischen Tatsachen mit der zum Zeitpunkt des Vorgangs geltenden Regel verbinden.[89]

5. Chile: Signatur, Datum und Sicherheitsregulierung

Die in der Zusammenstellung der Biblioteca del Congreso Nacional geltende Ley 19.799 regelt elektronische Dokumente und ihre Wirkungen. Artikel 1 verankert die Gleichwertigkeit des Trägers, Artikel 2 definiert Dokument und Signaturen, Artikel 3 erkennt Form und Wirkungen mit Ausnahmen, Artikel 4 verlangt eine fortgeschrittene elektronische Signatur für ein öffentliches Instrument und Artikel 5 unterscheidet den Beweiswert. Private Instrumente mit

[87]Peru. SBS 504-2021, Artikel 12.6.g, 15 und 17.3–17.4: Aufbewahrung, Berichterstattung und forensische Analyse, Aufzeichnungen von Registrierung, Authentifizierung und Vorgängen.Offizielle Online-Quelle
[88]Peru. SBS 2286-2024: Änderung von Artikel 20.3 über bestimmte nicht anerkannte Vorgänge und Haftung, sofern nicht die Verantwortung des Nutzers nachgewiesen wird.Offizielle Online-Quelle
[89]Peru. SBS 2286-2024: Änderung von Artikel 20.3 über bestimmte nicht anerkannte Vorgänge und Haftung, sofern nicht die Verantwortung des Nutzers nachgewiesen wird.Offizielle Online-Quelle

fortgeschrittener Signatur unterliegen dem gesetzlichen Regime des vollen Beweises, beweisen ihr Datum jedoch nur mit einer elektronischen Datierung durch einen akkreditierten Anbieter. Dokumente mit nicht fortgeschrittener elektronischer Signatur werden nach allgemeinen Regeln bewertet. Diese Unterscheidung verhindert zwei Fehler: einer einfachen Signatur jeden Wert abzusprechen und ihr automatisch den Wert einer fortgeschrittenen Signatur zu verleihen.[90]

Im Bankbereich unterscheidet die Recopilación Actualizada de Normas das Kapitel 20-10 über Management von Informationssicherheit und Cybersicherheit vom Kapitel 20-9 über Kontinuität. Kapitel 20-7 regelt Auslagerung und verlangt Vertraulichkeit, Integrität, Nachverfolgbarkeit und Verfügbarkeit sowie zeitnahen Zugriff auf Aufzeichnungen und Informationen, die von Behörden verlangt werden. Kapitel 20-8 betrifft Informationen über operative Vorfälle. Für das Handbuch wird die funktionale Entsprechung anhand von Kontrollen und verfügbaren Beweisen formuliert, nicht durch die Behauptung, ein Kapitel reproduziere 316 Bis. Die geltende Vorschrift und der Geltungsbereich der Stelle müssen angefordert werden, bevor Fristen oder Mindestinhalte festgelegt werden.[91]

Bedarf des Falls	Chilenische funktionale Quelle	Vorsicht
Dokument und Signatur zurechnen	Ley 19.799, Artikel 2–5.	Formale Identifizierung, fortgeschrittene Signatur und Beweiskraft trennen.
Datum eines privaten Instruments nachweisen	Ley 19.799, Artikel 5.2.	Die fortgeschrittene Signatur allein genügt nicht, um das Datum zu beweisen.
Anbieter/Cloud und Aufzeichnungen prüfen	RAN 20-7 und 20-10; Vorfälle, 20-8.	Kontinuität, Auslagerung und Cybersicherheit nicht verwechseln.

Quellen der Tabelle:[9293]

6. Argentinien: begrenzte Vermutungen und Zuverlässigkeit des Trägers

Die Ley 25.506 erkennt elektronische und digitale Signaturen mit unterschiedlichen Wirkungen an. Artikel 5 definiert die elektronische Signatur, die eine Anforderung der digitalen Signatur

[90]Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert.Offizielle Online-Quelle
[91]Chile. Recopilación Actualizada de Normas, Kapitel 20-7, 20-8 und 20-10: Auslagerung, operative Vorfälle, Informationssicherheit und Cybersicherheit.Offizielle Online-Quelle
[92]Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert.Offizielle Online-Quelle
[93]Chile. Recopilación Actualizada de Normas, Kapitel 20-7, 20-8 und 20-10: Auslagerung, operative Vorfälle, Informationssicherheit und Cybersicherheit.Offizielle Online-Quelle

nicht erfüllt; wird sie bestritten, muss die Person, die sie geltend macht, ihre Gültigkeit nachweisen. Die Artikel 7 und 8 vermuten Urheberschaft und Integrität der digitalen Signatur unter den gesetzlichen Bedingungen; Artikel 9 bestimmt die Gültigkeit und Artikel 6 erkennt die Schriftform an. Decreto 182/2019 regelt Aufbewahrung und beglaubigte Kopien. Die Ley 27.446 hob den früheren Artikel 4 der Ley 25.506 auf und ersetzte andere Bestimmungen; der Anhang darf historische Ausschlüsse daher nicht als geltenden Text wiedergeben.[949596]
Der Zivil- und Handelsgesetzbuch enthält die übergreifenden Beweisregeln. Artikel 318 erlaubt die Vorlage von Korrespondenz unabhängig vom Erzeugungs- oder Übermittlungsmedium, mit Einschränkungen für vertrauliche Korrespondenz. Artikel 319 verlangt die Bewertung privater Instrumente unter anderem nach Kongruenz, technischer Klarheit, Verwendungen, früheren Beziehungen und Zuverlässigkeit von Trägern und technischen Verfahren. Das Handbuch kann diese Leitlinien in konkrete Fragen übertragen: Welches System erzeugte den Eintrag, wer verwaltete die Schlüssel, welche Änderungen waren möglich, wie wurde exportiert, ist die Abfolge kongruent und liegt eine unabhängige Bestätigung vor? Die Vermutung kryptografischer Integrität beantwortet diese Kontextfragen nicht von selbst.[97]

BCRA-Regulierung	Funktion	Unterschied zu Mexiko
Comunicación A 7783	Transaktionsaufzeichnungen mindestens 90 Tage in digitalem Format verfügbar; Echtzeitaufzeichnung für bestimmte Nachrichtendienste; Überwachung.	Eigene Frist und Reichweite; nicht durch 180 mexikanische Tage ersetzen.
Comunicación A 8280	Reaktion und Wiederherstellung nach Cyber-Vorfällen; Abschlussbericht innerhalb von fünf aufeinanderfolgenden Tagen nach Eindämmung, Wiederherstellung und Lösung.	Die Berechnung hängt vom in der Vorschrift beschriebenen Ereignis ab; sie ist nicht identisch mit der CNBV-Meldung.

Quellen der Tabelle:[9899]

[94]Argentinien. Ley 25.506 de Firma Digital, Artikel 1 und 5–9: digitales Dokument, Beweislast bei Berufung auf eine bestrittene elektronische Signatur und begrenzte Vermutungen.Offizielle Online-Quelle
[95]Argentinien. Ley 27.446: Aufhebung des früheren Artikels 4 der Ley 25.506 und Ersetzung anderer Bestimmungen. Dies verhindert, den historischen Text als gültig zu zitieren.Offizielle Online-Quelle
[96]Argentinien. Decreto 182/2019: digitale Aufbewahrung und beglaubigte Kopien zu den vorgesehenen Fristen und Bedingungen.Offizielle Online-Quelle
[97]Argentinien. Código Civil y Comercial, Artikel 318–319: Korrespondenz unabhängig vom Medium und Bewertung der Zuverlässigkeit von Trägern und technischen Verfahren.Offizielle Online-Quelle
[98]Argentinien. BCRA Comunicación A 7783: digitale Transaktionsaufzeichnungen mindestens 90 Tage verfügbar und Überwachung von Sicherheitsereignissen.Offizielle Online-Quelle
[99]Argentinien. BCRA Comunicación A 8280: Reaktion und Wiederherstellung nach Cyber-Vorfällen; Abschlussbericht innerhalb von fünf aufeinanderfolgenden Tagen nach Eindämmung, Wiederherstellung und Lösung.Offizielle Online-Quelle

7. Kolumbien: Datennachrichten, Aufbewahrung und Empfangsbestätigungen

Die Ley 527 de 1999 bietet eine sehr klare funktionale Entsprechung zum mexikanischen Modell. Artikel 5 verhindert, Wirkungen aufgrund der elektronischen Form zu verweigern; Artikel 6 deckt Schriftform und Zugänglichkeit ab; Artikel 7 behandelt die Signatur mit einer zuverlässigen und geeigneten Methode; die Artikel 8–9 behandeln Original und Integrität; 10–11 Zulässigkeit und Bewertung; 12–13 Aufbewahrung direkt oder durch Dritte; 16–25 Zurechnung, Versand, Empfang, Empfangsbestätigungen, Duplikate, Zeit und Ort. Artikel 28 legt Merkmale der digitalen Signatur fest. Artikel 12 verlangt die Aufbewahrung von Informationen, mit denen Herkunft, Ziel, Datum und Uhrzeit bestimmt werden können; dies muss in die Formate für Export und Verwahrung aufgenommen werden.[100]

Das CPACA enthält Regeln für Verwaltungshandlungen. Die Artikel 57–58 verlangen Authentizität, Integrität und Verfügbarkeit von Handlungen und elektronischen Archiven; Artikel 61 verlangt Kontrolle empfangener Dokumente, Datum und Uhrzeit, Sicherheit und Empfangsbestätigung; Artikel 62 regelt den Nachweis von Versand/Empfang und von Dienstausfällen. Diese Bestimmungen ersetzen nicht die Ley 527: Sie betreffen das Verwaltungsverfahren. Für den Finanzsektor wurde die Circular Externa 033 de 2020 als Instrument mit Anweisungen zu Sicherheit und Cybersicherheit gefunden, doch die abgerufenen Quellen erlaubten nicht die sichere Bestimmung aller operativen Nummern. Die Matrix weist ihr daher aus Gründen der Sorgfalt keine ungelesenen Fristen oder wörtlichen Anforderungen zu.[101][102]

Anwendung	Dokumentarische Regel	Empfohlene Mindestaufzeichnung
Ursprüngliche Nachricht	Ley 527, Artikel 8–9.	Objekt in nativem Format, Integrität, Erzeugungsprozess und Form der Vorlage.
Aufbewahrung	Ley 527, Artikel 12–13.	Format, Herkunft, Ziel, Datum, Uhrzeit, Verwahrer und beteiligter Dritter.
Administrativer Empfang	CPACA 61–62.	Eingangsregistrierung, Empfangsbestätigung, Datum/Uhrzeit und überprüfbarer Nachweis jeder Störung.

[100]Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur.Offizielle Online-Quelle
[101]Kolumbien. CPACA, Artikel 57–58, 61 und 62: Authentizität und Integrität von Handlungen und elektronischen Archiven, Empfangsbestätigung und Nachweis von Dienstausfällen.Offizielle Online-Quelle
[102]Kolumbien. Superintendencia Financiera. Circular Externa 033 de 2020, als Anweisung zu Sicherheit und Cybersicherheit identifiziert; ihre Nummern müssen vor der Auferlegung besonderer Verpflichtungen bestätigt werden.Offizielle Online-Quelle

Anwendung	Dokumentarische Regel	Empfohlene Mindestaufzeichnung
Cybersicherheit im Finanzbereich	CE 033 de 2020 durch SFC identifiziert.	Nummern und offizielle Version bestätigen, bevor besondere Verpflichtungen auferlegt werden.

8. Ecuador: dokumentarische Entsprechung und Zahlungssystem

Die Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos —Ley 67— regelt die zentralen Funktionen ausdrücklich. Artikel 2 erkennt Datennachrichten nach Gesetz und Verordnung den gleichen Rechtswert zu; Artikel 6 umfasst zugängliche schriftliche Informationen; Artikel 7 Original und Integrität; Artikel 8 Aufbewahrung mit Format, Zugänglichkeit, Herkunft, Ziel, Datumsangaben, Uhrzeiten und Integrität; Artikel 10 Herkunft und Identität mit Vermutung und Ausnahmen; Artikel 11 Versand und Empfang; die Artikel 13–14 Definition und Wirkungen elektronischer Signaturen. Die Verordnung konkretisiert die Einbeziehung von Anhängen, Dematerialisierung, Integrität und Verifizierung. Die Vermutung in Artikel 10 erlaubt nicht, die natürliche Person, die ein Gerät betätigt hat, automatisch zu identifizieren: Verifizierung, Mitteilungen und Sorgfalt des Empfängers müssen analysiert werden.[103][104]

Im Finanzbereich regelt die Resolución JPRM-2025-006-M, veröffentlicht im Registro Oficial Suplemento 104 vom 18. August 2025, Zahlungssysteme. Ihre Artikel 77–79 behandeln Betrieb, Gültigkeit, Clearing und Abrechnung; Artikel 82 verlangt die Einzelzuordnung von Geldern und Wallet-Bewegungen sowie kontinuierliche Verfügbarkeit; spätere Bestimmungen regeln Teilnehmer und Aufsicht. Diese Quelle hilft, Aufzeichnungen und Bestätigungen des Zahlungssystems zu verstehen, belegt jedoch nicht dieselben Pflichten für Protokolle, Aufbewahrung und Vorfälle wie die CNBV. Das Handbuch muss diese Entsprechung als sektoral und teilweise kennzeichnen und das Regime der Stelle und des Kanals anfordern, bevor Verantwortlichkeiten abgeleitet werden.[105]

[103]Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur.Offizielle Online-Quelle

[104]Ecuador. Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos: Einbeziehung von Anhängen, Dematerialisierung, Integrität und Verifizierung. Offizielle Veröffentlichung der Función Judicial.Offizielle Online-Quelle

[105]Ecuador. Resolución JPRM-2025-006-M, Registro Oficial Suplemento 104, 18-08-2025: Betrieb, Gültigkeit, Clearing, Abrechnung und Verfügbarkeit von Geldern in Zahlungssystemen.Offizielle Online-Quelle

Bedarf	Ecuadorianische Quelle	Einschränkung
Nachricht und Metadaten aufbewahren	Ley 67, Artikel 8.	Eine PDF-Visualisierung genügt nicht, wenn Format und Herkunftsdaten verloren gehen.
Nachricht zurechnen	Ley 67, Artikel 10 und 13–14.	Signatur und Herkunft identifizieren für sich allein weder die natürliche Person noch beweisen sie alle Tatsachen.
Elektronische Zahlung rekonstruieren	Resolución JPRM-2025-006-M.	Regime für Zahlungssysteme, keine allgemeine Entsprechung aller CNBV-Verpflichtungen.

9. Spanien und Europäische Union: Nichtdiskriminierung, Vertrauensdienste und Verfahren

Spanien erfordert die Verbindung europäischen und prozessualen Rechts. eIDAS, Artikel 25, verbietet, einer Signatur Wirkungen oder Zulässigkeit allein deshalb zu verweigern, weil sie elektronisch oder nicht qualifiziert ist; die qualifizierte Signatur hat dieselbe Wirkung wie eine handschriftliche; Artikel 26 definiert Anforderungen an die fortgeschrittene Signatur; Artikel 46 verbietet, einem Dokument Wirkungen und Zulässigkeit aufgrund seines Formats zu verweigern. Das Gesetz 6/2020 regelt bestimmte elektronische Vertrauensdienste und hob das Gesetz 59/2003 und Artikel 25 der LSSI auf. Daher wäre es ein Aktualisierungsfehler, das frühere Gesetz über elektronische Signaturen als gültig zu zitieren. Die funktionale Entsprechung konzentriert sich auf Nichtdiskriminierung, Signaturniveaus und Vertrauensdienste, nicht auf das Kopieren der mexikanischen Struktur.[106][107]

Die am 7. Oktober 2026 aktualisierte konsolidierte LEC unterscheidet Authentizität und Bewertung. Artikel 326 regelt private Dokumente und ihre Anfechtung; seine Absätze 3 und 4 behandeln elektronische Dokumente und nicht qualifizierte und qualifizierte Vertrauensdienste, mit Vermutungen im vorgesehenen Fall. Artikel 384 regelt Instrumente zur Archivierung, Kenntnisnahme oder Wiedergabe von Daten: Prüfung unter Beteiligung der Parteien, Dokumentation und Verwahrung sowie Bewertung nach gesunder Kritik. Das Gesetz selbst erlaubt, Authentizität, Integrität, Genauigkeit von Datum und Uhrzeit oder andere Merkmale in

[106]Reglamento (UE) 910/2014 eIDAS, Artikel 25–26 und 46: keine Diskriminierung elektronischer Signaturen und Dokumente aufgrund ihres Formats, fortgeschrittene elektronische Signatur und Rechtswirkungen qualifizierter elektronischer Signaturen.Offizielle Online-Quelle

[107]Spanien. Ley 6/2020 über elektronische Vertrauensdienste: Aufhebung des Gesetzes 59/2003 und von Artikel 25 der LSSI; das frühere Regime wird nicht als gültig zitiert.Offizielle Online-Quelle

Frage zu stellen. Die Vorlage eines elektronischen Dokuments beendet daher die technische Debatte nicht; sie eröffnet sie mit einem überprüfbaren und widerspruchsfähigen Objekt.[108]

Zahlungsdienste	Spanische Regel	Technische Anwendung
RD-ley 19/2018, Artikel 45	Rückerstattung für nicht autorisierte Vorgänge unter den vorgesehenen Bedingungen und Ausnahmen, einschließlich begründetem Betrugsverdacht, der schriftlich mitgeteilt wird.	Fehlende juristische Autorisierung von einer bloßen Abweichung bei Gerät oder Anmeldedaten unterscheiden.
Art. 66	Rahmen für Risikomanagement, Kontrollen und Verfahren zur Verwaltung/Klassifizierung von Vorfällen; mindestens jährliche Bewertung.	Einschlägige Bewertungen und Kontrollen anfordern, ohne anzunehmen, dass sie einen konkreten Vorgang belegen.
Art. 67	Unverzügliche Meldung schwerer Vorfälle an die Banco de España; Information der Nutzer ohne ungerechtfertigte Verzögerung, wenn ihre Interessen beeinträchtigt sind oder beeinträchtigt werden könnten.	Chronologie von Erkennung, Klassifizierung, Meldung und Minderungsmaßnahmen aufbewahren.

Quellen der Tabelle:[109]

10. Funktionaler Vergleich von Aufzeichnungen und Finanzvorfällen

Die folgende Tabelle vermeidet eine häufige Vereinfachung: jede Cybersicherheitsnorm als „das Äquivalent“ der Artikel 316 Bis und Folgende darzustellen. Tatsächlich gibt es verschiedene Funktionen: Nachweise ausstellen, den Nutzer benachrichtigen, Zugriff kontrollieren, Authentifizierung registrieren, Protokolle aufbewahren, Vorfälle untersuchen, die Regulierungsstelle informieren und Verantwortung für nicht anerkannte Vorgänge zuweisen. Eine Gerichtsbarkeit kann diese Funktionen in getrennten Instrumenten abdecken. Das Gutachten muss zuerst eine Liste der erforderlichen Daten erstellen und erst danach ihre Grundlage suchen, nicht mit einer allgemeinen Anfrage nach „allen vorhandenen Aufzeichnungen“ beginnen.

[108]Spanien. Ley de Enjuiciamiento Civil, Artikel 326 und 384: private Dokumente, Anfechtung, Instrumente zur Archivierung, Kenntnisnahme oder Wiedergabe von Daten, Prüfung, Verwahrung und gesunde Kritik.Offizielle Online-Quelle
[109]Spanien. Real Decreto-ley 19/2018, Artikel 45, 66 und 67: Rückerstattung für nicht autorisierte Vorgänge, Risikomanagement und unverzügliche Meldung schwerer Vorfälle.Offizielle Online-Quelle

Die genannten Fristen sind bewusst wenige und an den gelesenen Text gebunden. Die mexikanische Frist von 180 Tagen wird nicht auf Argentinien und die Frist von fünf Kalendertagen der CNBV nicht auf Peru oder Spanien übertragen. Ist eine Frist nicht überprüft, wird sie in der Zelle nicht erfunden. Für die Beweissicherung kann das Handbuch empfehlen, sofort eine Kopie zu erstellen und die Daten beim Verwahrer anzufordern, ohne auf den Ablauf der Mindestaufbewahrungsfrist zu warten, da die gesetzliche Aufbewahrung weder unbegrenzte Verfügbarkeit noch Abdeckung aller relevanten Ereignisse garantiert.

Mexiko

Jurisdiktion	Regel, Umfang und Einschränkung
Aufzeichnungen/Authentifizierung	CNBV 316 Bis 11 und 15: Zugriff und Protokolle.
Vorfälle	316 Bis 12: Untersuchung und Meldung.
Nicht anerkannte Vorgänge	316 Bis 14: Vorkommnisse und nicht anerkannte Vorgänge.
Überprüfte Frist und Reichweite	180 Tage für Protokolle nach 316 Bis 15; fünf Jahre für 316 Bis 14; Meldung innerhalb von fünf Kalendertagen nach 316 Bis 12, jeweils in ihrem Geltungsbereich.

Quellen der Tabelle:[110]

Peru

Jurisdiktion	Regel, Umfang und Einschränkung
Aufzeichnungen/Authentifizierung	SBS 504-2021, 17.3–17.4: Registrierung, Versuche und Vorgänge; Überwachung.
Vorfälle	12.6.g und 15: Aufbewahrung, Berichterstattung und forensische Analyse.
Nicht anerkannte Vorgänge	SBS 2286-2024 ändert 20.3 und die Haftung, sofern nicht die Verantwortung des Nutzers nachgewiesen wird.
Überprüfte Frist und Reichweite	Keine einheitliche Frist übertragen; geltende Regel und Änderungen lesen.

Quellen der Tabelle:[111]

[110]Disposiciones de carácter general aplicables a las instituciones de crédito, Artikel 316 Bis, 316 Bis 1, 316 Bis 10 bis 17: Nachweise, Verschlüsselung, Zugriff, Vorfälle, Vorkommnisse, Protokolle und Überprüfungen.Offizielle Online-Quelle
[111]Peru. SBS 2286-2024: Änderung von Artikel 20.3 über bestimmte nicht anerkannte Vorgänge und Haftung, sofern nicht die Verantwortung des Nutzers nachgewiesen wird.Offizielle Online-Quelle

Chile

Jurisdiktion	Regel, Umfang und Einschränkung
Aufzeichnungen/Authentifizierung	RAN 20-10; Auslagerung und Aufzeichnungen in 20-7.
Vorfälle	RAN 20-8.
Nicht anerkannte Vorgänge	Erfordert eine besondere Vorschrift für Produkt und Kanal.
Überprüfte Frist und Reichweite	Keine ungeprüften Fristen zuweisen.

Quellen der Tabelle:[112]

Argentinien

Jurisdiktion	Regel, Umfang und Einschränkung
Aufzeichnungen/Authentifizierung	BCRA A 7783: Transaktionen und Sicherheitsereignisse.
Vorfälle	BCRA A 8280: Reaktion, Wiederherstellung und Abschlussbericht.
Nicht anerkannte Vorgänge	Regeln nach Kanal und Nutzervorschriften; nicht allein aus der Authentifizierung ableiten.
Überprüfte Frist und Reichweite	Digitale Aufzeichnungen mindestens 90 Tage in A 7783; Abschlussbericht innerhalb von fünf aufeinanderfolgenden Tagen im Fall von A 8280.

Quellen der Tabelle:[113]

Kolumbien

Jurisdiktion	Regel, Umfang und Einschränkung
Aufzeichnungen/Authentifizierung	Ley 527 für allgemeine Aufbewahrung; SFC für Aufsicht.

[112]Chile. Recopilación Actualizada de Normas, Kapitel 20-7, 20-8 und 20-10: Auslagerung, operative Vorfälle, Informationssicherheit und Cybersicherheit.Offizielle Online-Quelle
[113]Argentinien. BCRA Comunicación A 7783: digitale Transaktionsaufzeichnungen mindestens 90 Tage verfügbar und Überwachung von Sicherheitsereignissen.Offizielle Online-Quelle

Jurisdiktion	Regel, Umfang und Einschränkung
Vorfälle	CE 033 de 2020 als Anweisung in diesem Bereich identifiziert.
Nicht anerkannte Vorgänge	Eine ausreichende textliche Regel wurde in dieser Prüfung nicht belegt.
Überprüfte Frist und Reichweite	Nummern und amtlichen Text bestätigen, bevor Fristen oder Pflichtfelder verwendet werden.

Quellen der Tabelle:[114]

Ecuador

Jurisdiktion	Regel, Umfang und Einschränkung
Aufzeichnungen/Authentifizierung	Ley 67.8 für Nachrichten; JPRM-2025-006-M für Zahlungssysteme.
Vorfälle	Keine vollständige Entsprechung mit der CNBV belegt.
Nicht anerkannte Vorgänge	Erfordert ein besonderes Regime für Stelle und Kanal.
Überprüfte Frist und Reichweite	Keine Frist für Protokolle oder Vorfälle erfinden.

Quellen der Tabelle:[115]

Spanien

Jurisdiktion	Regel, Umfang und Einschränkung
Aufzeichnungen/Authentifizierung	RD-ley 19/2018, 66: Risiken und Kontrollen.
Vorfälle	Art. 67: schwere Vorfälle und Benachrichtigung der Nutzer.
Nicht anerkannte Vorgänge	Art. 45: Rückerstattung unter Bedingungen und Ausnahmen.
Überprüfte Frist und Reichweite	Schwerer Vorfall: unmittelbar; Risikobewertung mindestens jährlich; statistische Daten mindestens jährlich.

[114]Kolumbien. Superintendencia Financiera. Circular Externa 033 de 2020, als Anweisung zu Sicherheit und Cybersicherheit identifiziert; ihre Nummern müssen vor der Auferlegung besonderer Verpflichtungen bestätigt werden.Offizielle Online-Quelle
[115]Ecuador. Resolución JPRM-2025-006-M, Registro Oficial Suplemento 104, 18-08-2025: Betrieb, Gültigkeit, Clearing, Abrechnung und Verfügbarkeit von Geldern in Zahlungssystemen.Offizielle Online-Quelle

Quellen der Tabelle:[116]

11. Internationale methodische Standards

ISO/IEC 27037:2012 bietet Leitlinien für Identifizierung, Sammlung, Erfassung und Erhaltung potenzieller digitaler Beweise. Die offizielle ISO-Seite zeigt, dass die Ausgabe 2018 überprüft und bestätigt wurde und weiterhin gültig ist. Ihre Definitionen ermöglichen Präzision bei Identifizierung, Sicherung, bitweisem Image, Wiederholbarkeit und Reproduzierbarkeit. Der Standard dient zum Aufbau von Verfahren und Kontrollen, nicht zur Erklärung, dass ein Dokument aufgrund eines bestimmten Werkzeugs authentisch oder zulässig ist. Er ersetzt weder die Regeln der einzelnen Gerichtsbarkeiten noch die gerichtliche Bewertung.[117]
NIST SP 800-86 strukturiert den Prozess in Sammlung, Untersuchung, Analyse und Bericht und verbindet Dateien, Betriebssysteme, Datenverkehr und Anwendungen mit der Reaktion auf Vorfälle. Der Leitfaden weist darauf hin, dass er weder ein universelles Verfahren noch eine Rechtsberatung ist. Für das Handbuch strukturiert er Quellen und Dokumentation; für die juridischen Anhänge ist er ein technischer Leitfaden. Eine gute Praxis bildet jede Phase mit Arbeitsnachweisen ab: Identifizierung von Quelle und Befugnis, dokumentierte Erfassung, Überprüfung, Befunde, alternative Hypothesen und begrenzte Schlussfolgerungen. Ziel ist nicht, Gewissheit zu erzeugen, sondern sichtbar zu machen, was getan wurde, was wiederholt werden kann und was weiterhin unbewiesen bleibt.[118]

Handbuchphase	Methodischer Bezug	Erforderliche Qualitätsnachweise
Identifizierung	ISO/IEC 27037	Quelle, Verwahrer, Zustand, Befugnis, Veränderungsrisiko und Priorität.
Erfassung	ISO/IEC 27037 und NIST SP 800-86	Methode, Werkzeug/Version, Datum und Zeitzone, gegebenenfalls Hashwert, Vorkommnisse und Beziehung zwischen Original und Kopie.
Untersuchung und Analyse	NIST SP 800-86	Arbeitskopie, Hypothesen, Tests, negative Ergebnisse und Reproduzierbarkeit.

[116]Spanien. Real Decreto-ley 19/2018, Artikel 45, 66 und 67: Rückerstattung für nicht autorisierte Vorgänge, Risikomanagement und unverzügliche Meldung schwerer Vorfälle.Offizielle Online-Quelle
[117]ISO/IEC 27037:2012. Leitlinien für Identifizierung, Sammlung, Erfassung und Erhaltung digitaler Beweise. Die Ausgabe wurde von ISO als gültig bestätigt.Offizielle Online-Quelle
[118]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodischer Leitfaden, weder Rechtsvorschrift noch Garantie für die Zulässigkeit.Offizielle Online-Quelle

Handbuchphase	Methodischer Bezug	Erforderliche Qualitätsnachweise
Bericht	NIST SP 800-86 und lokale Verfahrensnorm	Tatsachen, Methode, Befunde, Einschränkungen, Anhänge und mögliche Widerlegung.

12. Regeln für die Verwendung der Matrix ohne falsche Entsprechungen

Die erste Regel lautet: Funktion + Instrument + Artikel + Geltungsbereich + Version zitieren, nicht „das äquivalente Gesetz“. Die zweite verlangt, Unterschiede zu bewahren: einfache, fortgeschrittene, digitale oder qualifizierte Signatur; elektronisches Original und gedruckte Kopie; Integritätsvermutung und Urheberschaftsnachweis; archivische Aufbewahrung und forensische Verwahrung; Authentifizierungsregistrierung und Einwilligung; Zulässigkeit und Beweiskraft. Die dritte verlangt, das Konsultationsdatum zu dokumentieren und spätere Reformen zu prüfen, wenn die Akte dies erfordert. Die vierte verbietet, eine Bankregel zur Rechtfertigung beliebiger privater Untersuchungen außerhalb ihres persönlichen Geltungsbereichs oder eine Verwaltungsregel zur Entscheidung jedes Zivil- oder Strafverfahrens zu verwenden.

Die zweite Prüfung ist materiell. Vor dem Abschluss des Anhangs muss geprüft werden, ob jeder Link die Quelle öffnet und der Artikel im heruntergeladenen Text vorhanden ist, ob Peru kein nicht vorhandenes allgemeines Regime in der Ley 27269 zugeschrieben wurde, ob die peruanische Änderung SBS 2286-2024 ist, ob Argentinien den durch Ley 27.446 aufgehobenen Artikel nicht als gültig wiedergibt und ob Spanien das Gesetz 59/2003 nicht als gültig zitiert. Der mexikanische Übergang muss die CNPCF-Zusammenstellung, die Initiative zur Verlängerung bis 2030 und jedes tatsächlich veröffentlichte Dekret getrennt halten. Die KI-Regulierung von San Luis Potosí wird in einer separaten Akte dokumentiert, weil sie Reform und spätere Aufhebung enthält, nicht eine Regel der Verwahrung.

Redaktionelle Kontrolle	Abnahmefrage	Maßnahme bei Nichterfüllung
Identität	Erscheinen Instrument und Artikel wörtlich in der Quelle?	Die Quellenangabe entfernen oder als nicht verifiziert kennzeichnen.
Funktion	Regelt die Vorschrift die beschriebene Funktion tatsächlich?	Als teilweise/sektoral neu einordnen und die Einschränkung erläutern.
Gültigkeit	Sind Version und Reformen auf den Sachverhalt anwendbar?	Datum dokumentieren und gezielte Prüfung im Amtsblatt durchführen.

Redaktionelle Kontrolle	Abnahmefrage	Maßnahme bei Nichterfüllung
Geltungsbereich	Sind Normadressat, Kanal und Verfahren umfasst?	Die Regel nicht ausdehnen; das besondere Regime anfordern.
Wirkung	Werden Zulassung, Authentizität, Wert und Beweislast unterschieden?	Die Schlussfolgerung ohne automatische Vermutungen neu formulieren.
Technische Prüfung	Ermöglicht das Format die Überprüfung der normativen Anforderungen?	Native Datei, Kontext, Metadaten und Exportprozess aufbewahren.

Operative Schlussfolgerung: Das Handbuch benötigt keine Tabelle ähnlicher Formulierungen, sondern eine Anleitung, dasselbe Problem mit unterschiedlichen Regeln nachzuweisen. Nützliche funktionale Entsprechung ermöglicht zu entscheiden, was aufzubewahren, anzufordern und zu überprüfen ist und welche Einschränkung zu erklären ist. Alles, was nicht durch geprüfte Quelle und Umfang gestützt wird, bleibt außen vor oder wird ausdrücklich als nicht belegt gekennzeichnet.

Umfang der Studie
Juristischer Hinweis: Dieses Dokument ist allgemeines Recherche- und Gestaltungsmaterial. Es stellt weder Rechtsberatung noch forensisches Gutachten oder Stellungnahme zu einem konkreten Fall dar. Die Anwendung auf eine Akte erfordert die Prüfung der zum Zeitpunkt der Tatsachen geltenden Vorschrift, Gerichtsbarkeit, Materie, Kanal und der entsprechenden Verfahrensregeln.

A.13 Praktische Anwendung: Rechtsregime vor der Schlussfolgerung auswählen

Eine Akte kann mehrere Länder betreffen, ohne dass alle ihre Vorschriften auf alle Tatsachen anwendbar sind. Ein in Mexiko verwaltetes Konto, ein Anbieter in Chile und ein in Spanien bestrittener Vorgang erfordern die Trennung von Ort des Geschehens, regulierter Stelle, Kanal, Vertrag, Verfahren und zeitlicher Version. Der erste Schritt ist nicht, Artikel 210-A zu übersetzen, sondern zu bestimmen, welche Funktion benötigt wird: Nachricht aufbewahren, Zurechnung nachweisen, Protokolle erlangen, Authentifizierung rekonstruieren oder eine Vorfallspflicht prüfen. Anschließend wird die Vorschrift gesucht, die diese Funktion für diese Stelle und dieses Verfahren erfüllt.

Schritt	Angewandte Frage	Dokumentiertes Ergebnis
Abgrenzen	Welcher Sachverhalt, Normadressat, Kanal und Prozess wird analysiert?	Übersicht über Gerichtsbarkeit und Geltungsbereich.
Lokalisieren	Welche Vorschrift deckt die Funktion in diesem Bereich ab?	Rechtsinstrument, Artikel, Version und offizielle Quelle.
Einordnen	Ist die Entsprechung direkt, teilweise oder sektoral?	Ausdrückliche Einschränkung und ergänzende Vorschriften.
Aufbewahren	Welches Objekt ermöglicht die Überprüfung der Anforderung?	Native Datei, Kontext, Metadaten, Export und Verwahrung.
Schlussfolgern	Welche Wirkung ist nachgewiesen und welche nicht?	Begrenzte Aussage ohne Übernahme fremder Vermutungen.

A.14 Datenschutz während der Untersuchung in Mexiko

Die forensische Verwahrung ist keine allgemeine Ausnahme vom Datenschutz. Die Verarbeitung muss Zweckbindung, Verhältnismäßigkeit, Sicherheit und Vertraulichkeit wahren; die vollständige Akte wird nicht allein aus Bequemlichkeit geteilt. Arbeits- und Verbreitungsfassungen werden getrennt, Zugriffe eingeschränkt und die Aufbewahrung nicht relevanter Dritter Daten vermieden. Erhebliche Verletzungen müssen mit der gesetzlich vorgesehenen Sorgfalt behandelt werden, einschließlich Information der Betroffenen, damit sie ihre Rechte wahren können. Derzeitige Bundesbehörde ist die Secretaría Anticorrupción y Buen Gobierno, entsprechend dem im März 2025 begonnenen Übergang.[119][120]

Vergleichsregel
Nützliche juristische Entsprechung führt zu einer überprüfbaren Entscheidung: was aufzubewahren, anzufordern und zu überprüfen ist und was nicht behauptet werden darf. Ändert die Analyse keine dieser Antworten, ist die Quellenangabe dekorativ.

[119]Ley Federal de Protección de Datos Personales en Posesión de los Particulares, neues Gesetz vom 20-03-2025, geändert am 14-11-2025. Artikel 5–9, 18–20 und 31: Grundsätze, Sicherheit, Vertraulichkeit, Verletzungen und Fristen.Offizielle Online-Quelle
[120]Secretaría Anticorrupción y Buen Gobierno. Comunicado 011, 21-03-2025: Übergang der Aufgaben des INAI zum Schutz personenbezogener Daten an das Sekretariat.Offizielle Online-Quelle

Anhang B. Formular für Umfang und Befugnisse

Dieses Formular wird vor dem Zugriff auf die Quelle ausgefüllt. Es verhindert, dass der Auftrag impulsiv erweitert wird oder technische Fähigkeit mit Erlaubnis verwechselt wird. Ändern sich Objekt, Zeitraum oder Zweck, wird eine neue Version erstellt und die frühere aufbewahrt. Für jedes nicht verfügbare Feld werden Grund und Person angegeben, die die Angabe klären kann.

B.1 Inhalt des Formats

Feld	Erforderlicher Inhalt	Vollständiges fiktives Beispiel
Kennung	Fallcode ohne Kundennamen oder sensible Daten.	EXP-DEMO-2026-001.
Verwendungszweck	Vorgesehene Verwendung: Betriebskontinuität, interne Untersuchung, forensisches Gutachten oder Verfahren.	Feststellen, ob die geltend gemachten Verkäufe erfasst, übermittelt und abgerechnet wurden.
Getrennte Fassungen	Was jede Partei behauptet, ohne es als erwiesene Tatsache darzustellen.	Handel: nicht bezahlte Verkäufe. Zahlungsabwickler: Vorgänge nicht erhalten.
Zeitraum	Beginn, Ende, Zeitzone und erforderliche Genauigkeit.	1.–3. November 2026, Ortszeit −06:00.
Einbezogene Quellen	Autorisierte Systeme, Dateien, Konten und Geräte.	Abrechnungsdateien, Berichte des Zahlungsabwicklers und Bankgutschriften zu drei Referenzen.
Ausschlüsse	Was nicht geprüft wird und warum.	Persönliche Geräte und E-Mails außerhalb der Fallreferenzen.
Befugnis	Autorisierender Inhaber, Instrument, zulässige Handlungen und Gültigkeit.	Autorisierter Vertreter; dokumentierte administrative Abfrage und Export.
Risiken	Volatilität, Datenschutz, Kontinuität, Dritte und unumkehrbare Entscheidungen.	Rotation von Protokollen und personenbezogene Daten nicht relevanter Käufer.

Feld	Erforderlicher Inhalt	Vollständiges fiktives Beispiel
Ergebnisdokument	Produkt, Format, Empfänger, Kanal und Überprüfung.	Technischer Bericht, Manifest und Exporte; verschlüsselte Übermittlung an den Verantwortlichen.
Änderungskontrolle	Version, Datum, Antragsteller, Autorisierender und Auswirkungen auf Quellen.	A01: Feldverzeichnis des Zahlungsabwicklers ergänzt, ohne Geräte zu erweitern.

Ausgangsbedingung
Die Erfassung wird nicht ausgeführt, bevor Umfang, Befugnis und Ausschlüsse beantwortet werden können. Erzwingt eine Dringlichkeit eine Maßnahme, werden die Ausnahmeentscheidung, ihre Begründung und die Grenze des Durchgeführten dokumentiert.

Anhang C. Protokoll der Entgegennahme und anfänglichen Sicherung

Das Protokoll wird bei Eingang des Objekts ausgefüllt, nicht nach Abschluss der Analyse. Beobachtungen und Angaben der übergebenden Person werden getrennt dokumentiert. Die Fotografie wird mit der Kennung verknüpft, ersetzt jedoch nicht die Beschreibung. Ist eine frühere Handlung unbekannt, wird „unbekannt“ mit einer Erklärung vermerkt und nicht durch eine beruhigende Annahme ersetzt.

C.1 Beispiel eines physischen Protokolls

Feld	Fiktiver Eintrag
Fall und Beweismaterial	EXP-DEMO-2026-001 · ED-20261109-DEMO-SSD-003-R00.
Objekt	SATA-SSD-Laufwerk, 2,5 Zoll, angegebene Kapazität 512 GB; sichtbare Seriennummer DEMO-003.
Übergabe	Verwahrer A, autorisierter Verwaltungsverantwortlicher; 9. November 2026, 14:32 −06:00.
Entgegennahme	Analyst B, zugewiesener Spezialist; Entgegennahmelabor.
Beobachteter Zustand	Ausgeschaltet und getrennt; Gehäuse ohne sichtbare Verformung; Anschluss ohne sichtbare Rückstände.
Zubehör	SATA-Kabel und Netzteil als verwandte Objekte ACC-003-01 und ACC-003-02 erfasst.
Angegebener Verlauf	Die Einheit wurde vom Systempersonal entfernt; es ist unbekannt, ob sie nach dem Vorfall angeschlossen wurde.
Fotografien	FOT-003-01 Übersicht; FOT-003-02 Serie; FOT-003-03 Anschlüsse und Zubehör.
Verpackung und Siegel	Antistatische Tasche in starrem Behälter; Siegel SL-DEMO-003 intakt.
Erste Entscheidung	Sichern, Schreibblocker validieren und autorisierte physische Erfassung vorbereiten.

Feld	Fiktiver Eintrag
Anmerkungen	Während der Entgegennahme wurde nicht eingeschaltet oder durchsucht. Keine Passwörter im Protokoll aufgeführt.

C.2 Entgegennahme von Dateien oder Nachrichten

Bei elektronischer Entgegennahme werden die Felder für den physischen Zustand durch Kanal, Konto, mutmaßlichen Absender, URL oder Nachricht, Berechtigungen, Originalnamen, Größen und Download-Datum ersetzt. Die Datei wird vor Umbenennung oder Konvertierung aufbewahrt. Stammt sie aus einer E-Mail, werden die EML-Datei aufbewahrt und getrennte Hashwerte für Nachricht und Anhänge berechnet. Stammt sie aus einem Link, werden die zugreifende Person und die verfügbare Version dokumentiert.

Kontrolle	Fiktives Beispiel
Kanal und Nachricht	E-Mail des Anbieters, empfangen am 9. November 2026, 15:02 −06:00.
Vollständiges Objekt	entrega_001.eml mit Nachrichtentext, Kopfzeilen und zwei Anhängen aufbewahrt.
Anhänge	registros.csv und diccionario.pdf; Originalnamen im Manifest beibehalten.
Erklärung des Anbieters	Der Nachrichtentext gibt den Algorithmus SHA-256 und einen Wert für jeden Anhang an.
Überprüfung	Dokumentierte lokale Berechnung: registros.csv stimmt überein; diccionario.pdf stimmt nicht überein.
Behandlung	Kein Anhang wird bearbeitet; Klärung und zweite Übermittlung der PDF-Datei werden angefordert.
Einschränkung	Die Übereinstimmung der CSV-Datei belegt Gleichheit mit der Übermittlung, nicht Wahrheitsgehalt oder vollständige Abdeckung.

Anhang D. Erfassungsprotokoll

Das Protokoll muss nachvollziehbar machen, was mit welcher Abdeckung und unter welchen Bedingungen kopiert wurde. Das Werkzeug wird nicht als Vertrauensmarke genannt: Version, Konfiguration, Validierung und Ergebnis werden ergänzt. Fehler werden zusammen mit der Ausgabe aufbewahrt. Wird die Erfassung wiederholt, wird eine neue Kennung erstellt und die Beziehung erläutert.

D.1 Vollständiges Beispiel

Feld	Fiktiver Eintrag
Fall und Erfassung	EXP-DEMO-2026-001 · ED-20261109-DEMO-SSD-003-A01.
Verwandte Quelle	ED-20261109-DEMO-SSD-003-R00, im Entgegennahmeprotokoll identifiziert.
Ziel und Abdeckung	Physisches Image des gesamten Mediums einschließlich nicht zugewiesenem Speicherplatz für die spätere Untersuchung.
Befugnis	Formular A01; Umfang auf die empfangene SSD und den abgegrenzten Vorfall beschränkt.
Verbindung	Quelle mit dem Schreibblocker und dieser mit der Arbeitsstation verbunden; Modell und Anschlüsse im Protokoll vermerkt.
Werkzeug	Für Testimage validiertes Werkzeug; Name, Version und Konfiguration im technischen Protokoll.
Datum und Zeitzone	Beginn 2026-11-09T15:21:08−06:00; Ende 2026-11-09T16:47:52−06:00.
Ausgabe	ssd003_A01.e01 und Protokolldatei; Arbeitskopie getrennt vom aufbewahrten Original.
Integrität	Algorithmus SHA-256; Wert mit der Imagedatei im kontrollierten Manifest verknüpft.
Vorkommnisse	Zwölf unlesbare Sektoren dokumentiert; die Meldung wird nicht verborgen und keine fehlerfreie Erfassung behauptet.
Überprüfung	Die Ausgabe lässt sich öffnen, die Größe stimmt mit dem Medium überein und der Prüfwert stimmt überein.

Feld	Fiktiver Eintrag
Abschluss	Original mit neuer Kennung erneut versiegelt; früheres Siegel und Öffnung in der Verwahrung dokumentiert.

Abnahmekriterium
Die Existenz der Datei genügt nicht. Sie muss geöffnet, der Quelle zugeordnet, ihre Abdeckung beschrieben und Vorkommnisse aufbewahrt werden. Kann ein Schritt nicht überprüft werden, wird dies vor dem Fortfahren vermerkt.

Anhang E. Beweismittelkette und Übertragungen

Das Protokoll erfasst Ereignisse, nicht nur Transporte. Das Öffnen eines Siegels, Erstellen einer Kopie, Herunterladen einer Datei oder Einsehen eines Behältnisses kann ebenfalls ändern, wer verantwortlich ist und was überprüft werden muss. Jede Zeile verknüpft Objekt, Verantwortliche, Zweck, Standort, Siegel und Integrität. Schlüssel werden in diesem Format niemals aufgeführt.

E.1 Beispiel einer Abfolge

Ereignis	Verantwortliche und Zweck	Überprüfung und Ergebnis
Empfang 09-11 14:32 −06	Verwahrer A übergibt SSD-003 an Analyst B zur Sicherung.	Serie und Fotografien stimmen überein; Siegel SL-003 intakt.
Öffnung 09-11 15:18 −06	Analyst B öffnet das Behältnis für die autorisierte Erfassung.	Früheres Siegel und Grund bleiben erhalten; das Objekt bleibt unverändert.
Erfassung 09-11 15:21 −06	Analyst B erstellt A01 auf einer validierten Arbeitsstation.	Ausgabe, Vorkommnisse und Hashwert werden in Protokoll D dokumentiert.
Erneutes Versiegeln 09-11 16:55 −06	Analyst B legt die Quelle in das Behältnis zurück.	Neues Siegel SL-003-B; Original getrennt von der Arbeitskopie.
Übertragung 10-11 09:10 −06	Verwahrer C übergibt Kopie A01 an Prüfer D über einen verschlüsselten Kanal.	Empfänger, Berechtigungen, Download und Hashwert-Überprüfung bestätigt.
Abfrage 10-11 11:42 −06	Prüfer D öffnet die Kopie, um die Hypothesenmatrix zu überprüfen.	Dokumentierter Zugriff; keine Änderung am Original.

E.2 Elektronische Übertragung

Eine Übertragung per Link umfasst Absender, Empfänger, Berechtigungen, Ablaufdatum, Version, Übermittlungskanal für den Schlüssel und Download-Prüfung. Der Empfang wird nicht aufgrund einer Systemanzeige „gesendet“ angenommen. Der Empfänger bestätigt Identität, Größe und gegebenenfalls Hashwert des Objekts. Wird der Link ersetzt, bleibt der Verlauf beider Übermittlungen erhalten.

Anhang F. Anfrage und Erfassung über einen Anbieter

Dieses Format verhindert, „alle Informationen“ anzufordern und eine kontextlose Tabelle zu erhalten. Die Anfrage bestimmt Fragestellung, Felder und Übermittlungsform. Die Autorisierung wird über einen sicheren Kanal gesendet; das Beispiel enthält keine realen Daten. Kann der Anbieter einen Punkt nicht erfüllen, muss er dies in der Antwort erklären, damit die Einschränkung mit dem Beweismaterial übermittelt wird.

F.1 Musteranfrage

Fiktive Anforderung von Aufzeichnungen und überprüfbarer Übermittlung
Betreff: EXP-DEMO-2026-001 · Aufzeichnungen vom 1. bis 3. November 2026

Über den autorisierten sicheren Kanal bitte ich um die mit den in der Akte enthaltenen Referenzen verbundenen Ereignisse von 2026-11-01T00:00:00−06:00 bis 2026-11-03T23:59:59−06:00. Bitte geben Sie die vom System verwendete Zeitzone, die Sommerzeit und die Umrechnungsregel an.

Bitte liefern Sie, sofern verfügbar: Datum/Uhrzeit, Ereignistyp, Richtung, Dauer, Kennungen, Funkzelle, Technologie, Ergebnis und eine Erklärung leerer Felder. Einschließlich nativem CSV-/XLSX-Format, PDF-Lesekopie, Feldverzeichnis, Prozess und Extraktionsdatum, Filtern, Abdeckung und Einschränkungen der Aufbewahrung.

Geben Sie im Nachrichtentext der Antwort für jede Datei den Algorithmus und den Hashwert an. Bewahren Sie die Übermittlung im EML-Format mit Nachrichtentext, Kopfzeilen und Anhängen auf. Übermitteln Sie in dieser E-Mail keine Schlüssel oder Anmeldedaten.

Autorisierter technischer Verantwortlicher · EXP-DEMO-2026-001

F.2 Protokoll des Exports oder der API

Feld	Fiktives Beispiel
Konto und Rolle	Verwaltungskonto DEMO; Rolle nur Lesen und Export.
System und Version	Anbieterportal; dokumentierte Version oder Datum der Oberfläche.

Feld	Fiktives Beispiel
Abfrage	Zeitraum, Referenzen und Ereignistypen; im Protokoll gespeicherte Filter.
Zeitzone und Format	Angegebenes UTC; native CSV-Datei und Feldverzeichnis.
API, falls zutreffend	Endpunkt, Version, Parameter, Paginierung und Grenzen; keine Geheimnisse im Bericht.
Ergebnis	Zwei Dateien, Zeilenzahl und dokumentierte Exportfehler.
Übermittlung	Vollständige EML-Datei, URL oder kontrollierter Kanal und Download-Datum.
Überprüfung	Hashwert jedes Objekts und Beziehung zur Erklärung des Anbieters.
Abdeckung und Einschränkung	Verfügbare Aufbewahrung, fehlende Daten und nicht abgedeckter Zeitraum.

Anhang G. Inventar und Manifest der Objekte

Das Manifest verknüpft Objekte und verhindert, dass ein Ordner zu einer Sammlung ohne Herkunft wird. Jede Zeile entspricht einer Datei, einem Image, einem Export, einer Visualisierung oder einem Bericht. Pfad und Größe helfen bei der Identifizierung; der Hashwert kontrolliert dieses bestimmte Objekt. Sensible Daten werden in öffentlichen Versionen ausgelassen, ohne die vollständige Arbeitsversion zu vernichten.

G.1 Beispiel eines Manifests

Kennung	Beziehung und Objekt	Kontrolle
DEMO-EML-001-R00	Empfangene Original-E-Mail; Nachrichtentext, Kopfzeilen und Anhänge.	Name, Größe, Empfangsdatum und SHA-256 im kontrollierten Protokoll.
DEMO-CSV-001-R00	Anhang registros.csv, unverändert aus der EML-Datei extrahiert.	Stimmt mit dem im Nachrichtentext angegebenen Hashwert überein; 18.420 Zeilen.
DEMO-PDF-001-R00	Anhang diccionario.pdf aus der ersten Übermittlung.	Hashwert stimmt nicht überein; für Vergleich und Klärung aufbewahrt.
DEMO-PDF-001-R01	Zweite Übermittlung des Feldverzeichnisses; verknüpftes, aber eigenständiges Objekt.	Neues Datum und neuer Hashwert; R00 wird nicht stillschweigend ersetzt.
DEMO-CSV-001-W01	Arbeitskopie der CSV-Datei zur Abfrage.	Abgeleitet von R00; Analyseänderungen werden separat gespeichert.
DEMO-INF-001-V10	Bericht Version 1.0 und referenzierte Anhänge.	Verschlüsselte Übermittlung; Hashwert der Verteilung und Empfänger dokumentiert.

Namensregel
Der operative Name löscht nicht das Original. Das Manifest bewahrt den empfangenen Namen und ergänzt die interne Kennung, sodass Sortieren niemals eine Veränderung der Quelle bedeutet.

Anhang H. Chronologie und Zeitzonen

Die Chronologie trennt die Angabe der Quelle von der Umrechnung durch den Analysten. Der ursprüngliche Wert wird niemals durch ein „korrigiertes“ Datum ersetzt. Die Genauigkeit wird mit der verfügbaren Granularität angegeben: Tag, Minute, Sekunde oder Zeitfenster. Ist die Synchronisation nicht belegt, wird dies als Einschränkung vermerkt, statt die Uhrzeit in eine fiktive Gewissheit zu verwandeln.

H.1 Beispiel einer Zeitachse

Quelle und wörtlicher Wert	Normalisierung	Zulässige Interpretation
Server: 2026-11-03 20:14:07 UTC	2026-11-03 14:14:07 −06:00; Genauigkeit in Sekunden.	Auf dem Server beobachtetes Ereignis; physische Urheberschaft nicht bewiesen.
E-Mail: 03. November 2026 14:20:11 −06:00	Keine Umrechnung; Kopfzeile in der EML-Datei aufbewahrt.	Empfang sechs Minuten später; Nähe beweist keine Kausalität.
Fotografie: 2026:11:03 14:16:00	Zeitzone nicht angegeben; Geräteuhr ausstehend.	Nur vereinbar, wenn Zeitzone und Uhr bestätigt werden; nicht als Gewissheit eingeordnet.
Zeugenaussage: „nach dem Essen“	Ungefähres Zeitfenster; keine genaue Uhrzeit zugewiesen.	Von einer Person angegebener Kontext, kein technischer Datensatz.
Export: vom 1. bis 3. November	Begrenzte Abdeckung; außerhalb dieses Zeitraums wurde nicht abgefragt.	Das Fehlen von Ereignissen außerhalb des Umfangs kann nicht behauptet werden.

H.2 Regel für widersprüchliche Datumsangaben

Zuerst wird geprüft, ob Ereignisse zum selben Objekt und zur selben Bedeutung gehören; danach Zeitzone, Uhr, Umrechnung, Format und Exportprozess. Erst anschließend wird eine Manipulation bewertet. Die Abweichung wird mit beiden Werten und ihrer möglichen Erklärung aufbewahrt. Eine brauchbare Zeitachse zeigt die Unsicherheit, statt sie unter einer geordneten Zelle zu verbergen.

Anhang I. Hypothesen- und Bestätigungsmatrix

Die Matrix wird vor den Schlussfolgerungen formuliert. Sie muss eine Prüfung enthalten, die jede Hypothese schwächen kann, nicht nur Daten, die sie stützen. Stammen zwei Quellen aus derselben Datei, wird ihre Abhängigkeit gekennzeichnet; sie als unabhängige Bestätigung zu zählen, würde die Beweiskraft künstlich erhöhen.

I.1 Ausgearbeitetes Beispiel

Element	Fiktive Ausarbeitung
Behauptung	Die Datei wurde erstmals am 3. November auf dem Konto des ehemaligen Mitarbeiters erstellt.
Hypothese A	Neue Erstellung an diesem Datum durch das zugewiesene Konto.
Hypothese B	Nachträgliche Kopie oder Änderung eines früheren Dokuments.
Hypothese C	Nutzung des Kontos durch eine andere Person oder eine unkontrollierte Sitzung.
Quellen	Native Datei, Cloud-Verlauf, Sitzungen, zweiter Faktor, frühere Sicherungskopie.
Überprüfung	Version, Anwendungsautor, Sitzung und Gerät vergleichen; frühere Abfolge prüfen.
Befund	Frühere Version vom 28. Oktober und Sitzung von einem nicht registrierten Gerät.
Wirkung	Schwächt die neue Erstellung und die automatische Zurechnung zum Inhaber.
Einschränkung	Noch nicht identifiziert, wer das Gerät kontrollierte oder welche Absicht bestand.
Zusätzliche Maßnahme	Aufzeichnungen über Registrierung und Geräteaktivität innerhalb des autorisierten Umfangs anfordern.
Vorläufige Schlussfolgerung	Das sichtbare Datum belegt nicht die erstmalige Erstellung; das Konto identifiziert die Person nicht allein.

Entscheidung ohne Ego
Widerspricht der Befund der Ausgangshypothese, wird die Hypothese oder die Schlussfolgerung geändert. Das Objekt wird nicht verändert und der Befund wird nicht ausgelassen, um eine bequeme Version zu bewahren.

Anhang J. Prüfung synthetischer Inhalte

Ziel ist nicht, einen Prozentsatz für „KI“ zu erhalten, sondern Herkunft, Umwandlungen und Veröffentlichung zu dokumentieren. Erstellung, Bearbeitung, Transcodierung und erneutes Aufnehmen sind unterschiedliche Ereignisse. Der Detektor wird, falls verwendet, mit Name, Version, Konfiguration und Einschränkungen dokumentiert. Ein positives oder negatives Ergebnis ersetzt weder die Datei noch den Kontext.

J.1 Angewandtes Format

Feld	Fiktives Beispiel
Empfangenes Objekt	video_publicado.mp4; Link, Konto, Datum und aufbewahrte Kopie.
Frühere Quelle	Die Generierungsdatei ist unbekannt; sie wird vom Inhaber und der Plattform angefordert.
Verlauf	Veröffentlichung, Download und Konvertierung als getrennte Ereignisse dokumentiert.
Angegebenes Werkzeug	Keine Erklärung des Herausgebers; kein konkretes Werkzeug wird angenommen.
Technische Analyse	Codec, Bilder, Audio, Kontinuität und verfügbare Metadaten.
Detektor	Orientierendes Ergebnis; Version und Einschränkungen dokumentiert, kein automatisches Urteil.
Bestätigung	Kameraoriginal, Bearbeitungsverlauf und frühe Veröffentlichung angefordert.
Juristischer Kontext	Einwilligung, Identität, Nutzung, Verhalten, Datum und geltende Vorschrift getrennt geprüft.
Zulässige Schlussfolgerung	Die Datei weist mit einer Bearbeitung vereinbare Umwandlungen auf; Herkunft und Autor sind nicht belegt.
Quelle, die das Ergebnis ändern würde	Originaldatei mit überprüfbarem Verlauf oder Aufzeichnungen des Generierungsdienstes.

Anhang K. Berichtsstruktur und Schlussfolgerung

Die Vorlage ordnet den Inhalt, ersetzt jedoch nicht die Argumentation. Jedes Kapitel des Berichts beantwortet eine Leserfrage und verweist auf konkrete Anhänge. Personenbezogene Daten werden auf das Erforderliche beschränkt. Die Management- und die technische Fassung können getrennt werden, um die Lektüre durch Geschäftsleitung und Fachprüfer zu ermöglichen, ohne ihre Beziehung zu verlieren.

K.1 Empfohlene Abfolge

Abschnitt	Beantwortete Frage	Mindestinhalt
Auftrag und Umfang	Was wurde angefordert und was blieb ausgeschlossen?	Fragen, Zweck, Gerichtsbarkeit, Zeitraum und Ausschlüsse.
Befugnis und Rollen	Wer hat autorisiert und wer hat ausgeführt?	Autorisierungen, Funktionen, Kommunikationen und erklärte Interessenkonflikte.
Quellen	Welche Objekte wurden empfangen oder erfasst?	Manifest, Kennungen, Zustände, Darstellungen und Fehlstellen.
Methode	Wie und mit welcher Abdeckung wurde untersucht?	Werkzeuge, Versionen, Parameter, Daten, Abfragen und Vorkommnisse.
Befunde	Was wurde beobachtet?	Positive, negative und nicht eindeutige Ergebnisse mit Objektbezug.
Analyse	Welche Erklärungen wurden verglichen?	Hypothesen, Bestätigungen, Widersprüche und vermiedene falsche Konsequenzen.
Schlussfolgerungen	Was kann innerhalb des Umfangs behauptet werden?	Antwort je Frage, Grad der Behauptung und Grundlage.
Einschränkungen	Was wurde nicht nachgewiesen?	Fehlende Quellen, Abdeckung, Uhr, Formate, Fehler und Zugriff.

Abschnitt	Beantwortete Frage	Mindestinhalt
Anhänge und Übermittlung	Wie wird geprüft?	Protokolle, Erfassungen, Manifest, Chronologie, Abfragen und Versionskontrolle.

K.2 Beispiel einer vollständigen Schlussfolgerung

Fiktive Schlussfolgerung
Die Datei registros.csv, empfangen als Anhang der Nachricht DEMO-EML-001-R00, wies mit dem im Nachrichtentext des Anbieters angegebenen Wert eine SHA-256-Übereinstimmung auf. Dies belegt die Gleichheit zwischen dem empfangenen Anhang und der Datei, auf die sich diese Erklärung bezieht. Der Export enthält 18.420 Zeilen vom 1. bis 3. November 2026, ausgedrückt in UTC gemäß dem gelieferten Feldverzeichnis. Innerhalb dieser Abdeckung wurden keine Ereignisse mit den drei abgefragten Referenzen festgestellt. Dieses Ergebnis beweist weder das Nichtvorhandensein von Vorgängen außerhalb des Zeitraums, in anderen Kanälen oder in nicht gelieferten Aufzeichnungen noch identifiziert es die Person, die sie durchgeführt haben könnte.

Die vorstehende Schlussfolgerung benötigt weder das Wort „fehacientemente“ noch ein Versprechen des gerichtlichen Erfolgs. Ihre Stärke liegt darin, dass jede Komponente aufgefunden werden kann: Nachricht, Datei, Hashwert, Zeilen, Zeitraum, Referenzen und Einschränkung. Findet die Gegenseite eine andere Quelle, kann die Analyse erweitert werden, ohne die frühere Arbeit zu vernichten.

Anhang L. Operative Checklisten

Die Listen dienen als Abschlusskontrolle, nicht als Ersatz für fachliches Urteil. Jede positive Antwort benötigt auffindbare Beweise. „Nicht zutreffend“ erfordert eine Begründung. Schlägt eine Kontrolle fehl, wird dokumentiert, wer mit welcher Begründung und Einschränkung fortfährt. Die Fragen können gedruckt und dem Verfahren angepasst werden, ohne zu einer rückwirkenden Erklärung nicht durchgeführter Handlungen zu werden.

L.1 Entgegennahme und Erfassung

Kontrolle	Erwarteter Nachweis	Bei Nichterfüllung
Sind Umfang und Befugnis dokumentiert?	Unterzeichnetes Formular oder überprüfbare Autorisierung.	Aussetzen und klären; gegebenenfalls die Ausnahme dokumentieren.
Hat das Objekt eine Kennung und einen Zustand?	Protokoll, Serie, Fotografien und Zubehör.	Nicht analysieren, bis die Identität geklärt oder die Einschränkung erklärt wurde.
Sind Quelle und Kopie getrennt?	Beziehung zwischen Original und Derivat sowie Standort.	Kontrollierte Kopie erstellen, ohne die Entgegennahme umzuschreiben.
Sind Methode und Abdeckung klar?	Erfassungsprotokoll, Filter und Format.	Protokoll mit dem tatsächlich Ausgeführten vervollständigen.
Wird die Ausgabe geöffnet und überprüft?	Öffnungstest, Manifest und relevanter Hashwert.	Als neues Objekt wiederholen und Vorkommnisse aufbewahren.
Wurden Fehler und Ausschlüsse dokumentiert?	Vorkommnisse, Filter, fehlende Felder und Grund.	Keine Vollständigkeit behaupten; Schlussfolgerung begrenzen.

L.2 Analyse, Bericht und Übermittlung

Kontrolle	Überprüfungsfrage	Erforderliches Ergebnis
Nachverfolgbarkeit	Führt jede Schlussfolgerung zu Befund und Quelle zurück?	Vollständiger Weg und übereinstimmende Anhänge.

Kontrolle	Überprüfungsfrage	Erforderliches Ergebnis
Chronologie	Bleiben wörtliche Werte, Zeitzonen und Genauigkeiten erhalten?	Erklärte Umrechnung und sichtbare Unsicherheit.
Hypothese	Wurde nach Umständen gesucht, die der Ausgangsversion widersprechen?	Alternativen, negative und nicht eindeutige Ergebnisse.
Sprache	Sind Integrität, Urheberschaft und Wahrheitsgehalt getrennt?	Keine absoluten Aussagen oder falschen Konsequenzen.
Widerlegung	Hat eine andere Person versucht, Fehler zu finden?	Anmerkungen, Antworten und dokumentierte Änderungen.
Gültigkeit	Entsprechen die Vorschriften Normadressat, Materie und Datum?	Offizielle Quelle, Version, Funktion und Geltungsbereich.
Übermittlung	Öffnen, lesen und enthält die Datei die zitierten Anhänge?	Überprüftes Paket, Kanal und bestätigter Empfang.
Datenschutz	Vermeidet die verbreitete Version unnötige Offenlegung?	Zugriff, Minimierung und kontrollierte Versionen.

Anhang M. Kontrolle von Versionen, Quellen und Erkenntnissen

Die Versionskontrolle unterscheidet die historische Akte vom aktuellen Verfahren. Ein früheres Protokoll wird nicht verändert, um aktuell zu erscheinen; ein Leitfaden wird dagegen korrigiert, wenn sich Vorschrift oder Werkzeug ändert. Jede Änderung gibt Grund, Quelle, Verantwortlichen, Datum und Wirkung an. Nicht verifizierte Quellen werden nicht als verifiziert dargestellt.

M.1 Normatives und technisches Protokoll

Element	Was dokumentiert wird	Beispiel
Instrument oder Werkzeug	Vollständiger Name, Thema, Gerichtsbarkeit oder Version.	CNPCF, Artikel 348–350; Werkzeug und Validierungsversion.
Quelle und Abfrage	Offizielle URL, Datum, Zusammenstellung und Verantwortlicher.	Portal der Abgeordnetenkammer, dokumentierte Abfrage.
Festgestellte Änderung	Reform, Aufhebung, Erklärung oder Verhaltensänderung.	Initiative von Dekret getrennt; neue Exportversion.
Funktionale Wirkung	Welche Anforderung oder Entscheidung ändert sich und für wen.	Übergangsregime oder Feldverzeichnis aktualisieren.
Redaktionelle Maßnahme	Geändertes Kapitel, Tabelle oder Format.	Geltenden Text ersetzen und Verlauf aufbewahren.
Überprüfung	Person, Datum, Test und nächste risikobasierte Überprüfung.	Artikel in der Quelle prüfen und fiktives Beispiel testen.

M.2 Lektion in Verbesserung umsetzen

Feld	Fiktives Beispiel
Vorkommnis	Ein Export ohne Zeitzone und Feldverzeichnis wurde empfangen.

Feld	Fiktives Beispiel
Auswirkung	Es konnte keine zuverlässige Chronologie erstellt und leere Felder konnten nicht interpretiert werden.
Ursache	Die frühere Anfrage verlangte einen „vollständigen Bericht“ ohne Format oder Kontext.
Korrektur des Falls	Eine neue Übermittlung wurde angefordert; die erste und ihre Einschränkung bleiben erhalten.
Vorbeugende Änderung	Anhang F verlangt Zeitzone, Feldverzeichnis, Filter, natives Format, Hashwert und EML-Datei.
Überprüfung	Übung mit fiktivem Anbieter: Alle Felder treffen ein und können geöffnet werden.
Verantwortlicher und Version	Methodischer Prüfer; Format F wird mit Datum und Grund von 1.0 auf 1.1 geändert.

Kontinuitätsregel
Eine neue Version verbirgt die frühere nicht. Sie zeigt, was geglaubt wurde, was sich mit welcher Quelle geändert hat und wie sich dies auf künftige Fälle auswirkt, ohne bereits abgeschlossene Akten zu verändern.