TEQUILA SO
Jocsan Laguna

Umgang mit digitalen Beweisen

Bewahren, erfassen, dokumentieren, analysieren und präsentieren

PRAXISHANDBUCH · 2026



Vorstellung des Handbuchs

Dieses Handbuch erläutert, wie digitale Beweise mithilfe einer von anderen nachprüfbaren Methode entgegengenommen, gesichert, erfasst, übertragen, analysiert und vorgelegt werden. Es richtet sich an Polizeibeamte, Sachverständige, Rechtsanwälte und Verantwortliche in Organisationen. Ingenieurkenntnisse sind nicht erforderlich: Jeder Begriff wird anhand einer Handlung und eines Beispiels erklärt. Es ersetzt weder die zuständige Stelle noch die Rechtsvorschriften oder das fachliche Urteil, das jeder Fall erfordert.

Die zentrale Regel ist einfach: Öffnen Sie kein Gerät und suchen Sie nicht gezielt nach einer Bestätigung Ihres Verdachts. Legen Sie vielmehr fest, was nachgewiesen werden soll, wo sich mögliche Beweise befinden, welche geeignete Methode am wenigsten eingreift und welche Maßnahmen dokumentiert werden müssen. Eine brauchbare Schlussfolgerung ist nicht diejenige, die am überzeugtesten klingt, sondern diejenige, die Tatsachen, Ableitungen und offene Fragen klar voneinander trennt.

So verwenden Sie dieses Handbuch

Wenn Sie die erste Person sind, die den Fall entgegennimmt, lesen Sie die Kapitel 1, 3, 5 und 7. Dort erfahren Sie, wie Sie den Auftrag abgrenzen, Zuständigkeiten festlegen, einen Erfassungsweg auswählen und den Eingang ohne Improvisation dokumentieren. Wenn Sie Beweise erfassen oder analysieren, arbeiten Sie mit den Kapiteln 4, 6, 8, 9 und 10. Wenn Sie einen Antrag, einen Bericht oder eine Präsentation prüfen, verwenden Sie die Kapitel 2, 11 und 12 sowie die Anhänge A, K, L und M.

Die Beispiele sind fiktiv und vollständig ausgearbeitet, um die Argumentation zu veranschaulichen, nicht um ein starres Rezept vorzugeben. Die Vorlagen enthalten auszufüllende Felder und Anweisungen. Die Rechtsmatrix vergleicht Funktionen und behauptet nicht, dass zwei Artikel identisch seien. Daten und Versionen sind wichtig: Bevor Sie eine Vorschrift anwenden, prüfen Sie, ob sie gültig und auf den Sachverhalt, den Normadressaten, den Kanal und das Verfahren anwendbar ist.

Leitprinzipien

Grundsatz	Praxisbezug
Minimale Veränderung	Wählen Sie die Methode, die die geringsten Veränderungen verursacht, und dokumentieren Sie jede unvermeidliche Veränderung.
Befugnis vor Zugriff	Die Berechtigung zum Zugriff ist nicht dasselbe wie die technische Fähigkeit dazu. Beides ist erforderlich.
Kontext vor dem Fragment	Ein isoliertes Bildschirmfoto ersetzt weder die Datei noch die vollständige Nachricht oder Veröffentlichung.
Ockhams Rasiermesser	Beginnen Sie mit der Quelle, die Hypothesen am besten unterscheiden kann, statt Werkzeuge zu sammeln.
Entscheidungen ohne Ego	Widersprechen die Beweise der ersten Version, wird die Schlussfolgerung korrigiert, nicht das Original.
Reproduzierbarkeit	Eine andere qualifizierte Person muss das Verfahren nachvollziehen, prüfen und wiederholen können.
Ausdrückliche Einschränkung	Nicht Beobachtetes oder nicht Nachgewiesenes wird ausdrücklich ausgewiesen und nicht durch Vermutungen ergänzt.
Schutz von Personen	Die Sicherung von Beweisen berechtigt weder zur Verbreitung von Daten noch zu einer erneuten Viktimisierung einer Person.

Inhalt

Vorstellung des Handbuchs 2
So verwenden Sie dieses Handbuch 3
Leitprinzipien 4
Inhalt 5
Kapitel 1. Umfang, Fragen und Befugnis 8
1.1 Die Leitfrage für die gesamte Arbeit 8
1.2 Befugnis, Verhältnismäßigkeit und Vertraulichkeit 9
1.3 Erstinventar der Quellen 9
1.4 Vollständiges Beispiel: eine Forderung im Zusammenhang mit Verkäufen 9
Kapitel 2. Integrität, Original und Kontext 11
2.1 Das Original ist nicht immer das Gerät 11
2.2 Integrität, Authentizität, Zurechnung und Wahrheitsgehalt 11
2.3 Der Hashwert als Kontrolle, nicht als Dogma 12
2.4 Zugänglichkeit und Erhaltung des Kontexts 12
Kapitel 3. Rollen und Verantwortlichkeiten 14
3.1 Funktionen vor Positionsbezeichnungen 14
3.2 Operative Kommunikation 15
3.3 Unabhängigkeit und Überprüfung 15
Kapitel 4. Lebenszyklus und forensische Vorbereitung 16
4.1 Vorbereitung vor der Entgegennahme eines Falls 16
4.2 Unumkehrbare Entscheidungen 16
4.3 Dokumentierter Lebenszyklus 17
Kapitel 5. Entscheidungsbäume nach Szenario 18
5.1 Ein- oder ausgeschaltetes Gerät 18
5.2 Lokale, entfernte oder anbieterseitige Erfassung 18
5.3 Mobilgeräte und Isolation 18
5.4 Wann die Arbeit auszusetzen ist 19
Kapitel 6. Moderne Quellen und Gesprächsdatensätze 20
6.1 Cloud, SaaS und Exporte 20
6.2 E-Mail und EML 20
6.3 Anforderung und Entgegennahme von Gesprächsdatensätzen 21
6.4 Beispiel für den Text einer Anbieteranfrage 22
6.5 Virtualisierung, IoT und synthetische Inhalte 22
6.6 Regulierung und Gültigkeit ohne isolierte Beispiele 22
Kapitel 7. Entgegennahme und anfängliche Sicherung 24
7.1 Nachvollziehbares Entgegennahmeprotokoll 24
7.2 Verpackung und Versiegelung 24
7.3 Kennzeichnung und Beziehung zwischen Objekten 25
7.4 Entgegennahme von Dateien und Nachrichten 25
Kapitel 8. Erfassung und technische Dokumentation 26

8.1 Physische, logische, flüchtige und dokumentarische Erfassung 26
8.2 Werkzeuge und Validierung 26
8.3 Exporte und reproduzierbare Abfragen 27
8.4 Fehler und Vorkommnisse 27
Kapitel 9. Verwahrung, Transport und Aufbewahrung 28
9.1 Die Beweismittelkette als Antwort auf Fragen 28
9.2 Elektronische Übertragungen 28
9.3 Speicherung und späterer Zugriff 28
Kapitel 10. Untersuchung, Analyse und Hypothesen 30
10.1 Fragen vor Werkzeugen 30
10.2 Chronologie und Zeitzonen 31
10.3 Auswertung von Gesprächsdatenlisten und Protokollen 31
10.4 Wiederholbarkeit und Reproduzierbarkeit 31
Kapitel 11. Bericht, Präsentation und Widerlegung 32
11.1 Struktur des Berichts 32
11.2 Sprache für ein nichttechnisches Publikum 32
11.3 Zitate und Rechtsnormen 33
11.4 Prüfung auf Widersprüche 33
Kapitel 12. Häufige Fehler und kontinuierliche Verbesserung 34
12.1 Fehler, die Fälle verändern 34
12.2 Gewonnene Erkenntnisse 35
12.3 Mindestleitfaden für die gesamte Organisation 35
Anhang A. Zusammengefasste funktionale Rechtsmatrix 36
A.1 So lesen Sie den Vergleich 36
A.2 Aktualisierungsmethode 37
Anhang B. Formular für Umfang und Befugnisse 38
B.1 Format 38
Anhang C. Entgegennahmeprotokoll 39
C.1 Mindestdaten 39
Anhang D. Erfassungsprotokoll 40
D.1 Protokoll für jedes Objekt 40
Anhang E. Beweismittelkette und Übertragungen 41
E.1 Protokoll für jedes Ereignis 41
Anhang F. Anfrage an einen Anbieter und EML-Übermittlung 42
F.1 Felder der Anfrage 42
F.2 Überprüfung bei Empfang 42
Anhang G. Inventar und Dateimanifest 43
G.1 Spalten des Manifests 43
Anhang H. Chronologie und Zeitzonen 44
H.1 Korrelationstabelle 44
Anhang I. Hypothesen- und Analysematrix 45
I.1 Vorlage für die Argumentation 45

Anhang J. Prüfung synthetischer Inhalte 46
J.1 Mindestunterlagen 46
Anhang K. Vorlage für einen technischen Bericht 47
K.1 Aufbau des Berichts 47
Anhang L. Checklisten 48
L.1 Entgegennahme und Erfassung 48
L.2 Bericht und Veröffentlichung 48
Anhang M. Versionskontrolle für Rechtsnormen und das Handbuch 49
M.1 Änderungsprotokoll 49
M.2 Abschluss der Nutzung 49

Kapitel 1. Umfang, Fragen und Befugnis

Legen Sie fest, was nachgewiesen werden muss, bevor Sie Beweismaterial bearbeiten.



Abbildung 1. Legen Sie fest, was nachgewiesen werden muss, bevor Sie Beweismaterial bearbeiten.

1.1 Die Leitfrage für die gesamte Arbeit

Ein brauchbarer Auftrag lautet nicht „prüfe alles“. Er beschreibt, was geschehen ist, was nachgewiesen werden soll, wofür das Ergebnis verwendet wird und welche Frist besteht. Die Antwort bestimmt, welche Quellen benötigt werden und welches Maß an Veränderung gerechtfertigt ist. Eine Dateiwiederherstellung zur Aufrechterhaltung des Betriebs ist nicht dasselbe wie ein forensisches Gutachten, das einer gerichtlichen Überprüfung standhalten muss, auch wenn beide dieselben Werkzeuge nutzen.

Notieren Sie die Sachverhalte in einfacher Sprache: Wer erhebt welche Behauptung, was bestreitet die andere Partei und welche Beweise liegen den ersten Aussagen zufolge vor? Trennen Sie Beobachtungen von Vermutungen. Diese Unterscheidung verhindert, dass eine Ausgangshypothese zu einer Anweisung wird, nur nach ihrer Bestätigung zu suchen.

Frage	Was dokumentiert werden muss	Entscheidung, die Improvisation vermeidet
Was behauptet jede Partei?	Getrennte Fassung pro Person 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.

Frage	Was dokumentiert werden muss	Entscheidung, die Improvisation vermeidet
Was kann aus dem Umfang ausgeschlossen werden?	Ausgeschlossene Daten, Geräte, Konten oder Zeiträume.	Unnötige Offenlegung verringern.

1.2 Befugnis, Verhältnismäßigkeit und Vertraulichkeit

Die Autorisierung muss Inhaber, Umfang, zulässige Handlungen, Systeme, Verantwortliche und Kommunikationskanal angeben. Wenn der Zugriff auf Daten Dritter, ein gemeinsam genutztes Konto oder einen Anbieter erforderlich ist, muss der rechtmäßige Beschaffungsweg dokumentiert werden. Ein Sachverständiger erhält keinen Zugriff allein deshalb, weil er weiß, wie er ihn technisch erlangen könnte.

Bei der Verhältnismäßigkeit ist zu prüfen, ob Quelle und Methode für das Ziel erforderlich sind. Beantwortet ein administrativer Export die Frage besser als eine vollständige Geräteprüfung, ist der Export zu wählen. Vertraulichkeit ist kein nachträglicher Zusatz: Bereits bei der Entgegennahme wird festgelegt, wer Informationen einsehen, kopieren, übertragen und veröffentlichen darf, insbesondere bei Daten Dritter oder von Opfern.

Handlungsregel

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

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 von Quellen verändert die Planung und die möglichen Schlussfolgerungen.

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 danach, welches Gerät wichtiger erscheint, sondern welche Informationen zuerst verschwinden können und welche Frage sie beantworten.

- Quellenkennung und derzeitiger Verwahrer.
- Datenart, Zeitraum und erwartetes Format.
- Bezug zu dem Sachverhalt, der nachgewiesen werden soll.
- Status: verfügbar, eingeschränkt, unsicher oder unzugänglich.
- Risiko von Veränderung, Verlust oder Offenlegung.
- Autorisierungsweg und nächster Ansprechpartner.

1.4 Vollständiges Beispiel: eine Forderung im Zusammenhang mit Verkäufen

Eine Handelskette behauptet, Verkäufe getätigt zu haben, für die keine Zahlung erfolgt sei. Ziel 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.

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. Der Plan vermeidet bereits eine invasive Prüfung persönlicher Geräte und erfordert den Vergleich unabhängiger Quellen.

1. Auftrag und Darstellungen der Parteien werden getrennt dokumentiert.
2. Autorisierung und Ausschlüsse sind festgelegt.
3. Quellen nach Fragestellung und Volatilität priorisiert.
4. Daten Dritter und Vertraulichkeitsmaßnahmen sind definiert.
5. Erwartetes Ergebnis und anfängliche Einschränkungen sind dokumentiert.

Kapitel 2. Integrität, Original und Kontext

Verstehen, welche Aussagen über eine Datei zulässig sind und welche nicht.



Abbildung 2. Verstehen, welche Aussagen über eine Datei zulässig sind und welche nicht.

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, sofern ihre Beziehung zum Ursprung sowie die erhaltenen oder verlorenen Informationen bekannt sind.

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.[1][2]

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

[1] Código de Comercio de México, Artikel 89–94 und 1205, amtliche Zusammenstellung. https://www.diputados.gob.mx/LeyesBiblio/pdf/CCom.pdf

[2] Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350, konsultierte Zusammenstellung mit Reform vom 15-01-2026. https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPCF.pdf

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.

Belastbare Aussage	Welche Beweise werden benötigt?	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.

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.“

2.4 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.

Die NOM-151-SCFI-2016 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.[3]

[3]NOM-151-SCFI-2016, Aufbewahrung und Digitalisierung von Datennachrichten. https://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017

Kapitel 3. Rollen und Verantwortlichkeiten

Festlegen, wer entscheidet, wer ausführt, wer dokumentiert und wer prüft.



Abbildung 3. Festlegen, wer entscheidet, wer ausführt, wer dokumentiert und wer prüft.

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.

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.

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.

Funktion	Hauptverantwortung	Erwartete Dokumentation
Verwahrer	Kontrolliert Zugriff, Standort und Übertragungen.	Beweismittelkette.
Prüfer	Prüft Methode, Ergebnisse und Grenzen.	Anmerkungen und Entscheidung.

3.2 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.

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.

3.3 Unabhängigkeit und Überprüfung

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.

Bestätigungstendenzen werden kontrolliert, indem Hypothesen und abweichende Ergebnisse dokumentiert werden. Eine Prüfung, die nur bestätigen soll, was der Analyst bereits geschrieben hat, ist nicht unabhängig. Der Bericht muss nachvollziehbar machen, was gefunden, was ausgeschlossen und was weiterhin offen ist, auch wenn die Antwort nicht zugunsten des Auftraggebers ausfällt.

Kapitel 4. Lebenszyklus und forensische Vorbereitung

Verluste verhindern, bevor ein Vorfall eintritt.

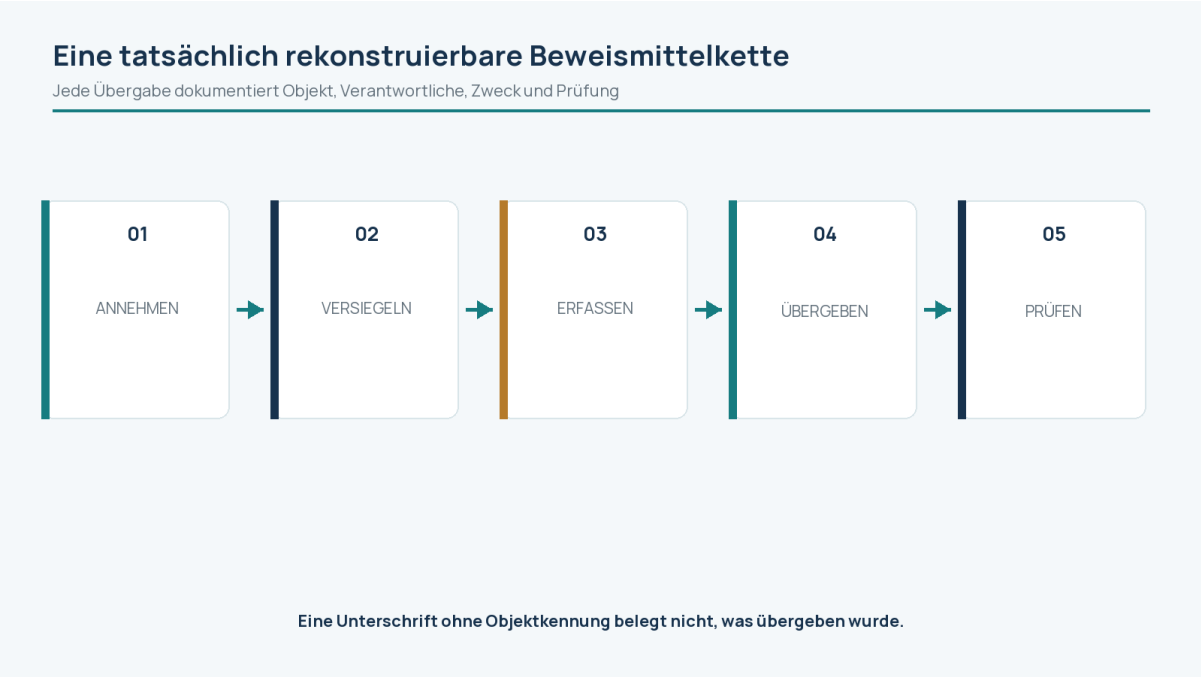


Abbildung 4. Verluste verhindern, bevor ein Vorfall eintritt.

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.

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.

- Aktuelles Inventar der IT-Assets und ihrer Eigentümer.
- Protokollquellen, Format und Aufbewahrungszeitraum.
- Technische, juristische und anbieterseitige Kontakte einschließlich Vertretungen.
- Dokumentierte Zeitzone und Zeitsynchronisation.
- Verfügbare Verfahren zur Erfassung, Versiegelung und Übertragung.
- Regelmäßige Übungen mit fiktivem Beweismaterial.

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.

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.

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.

4.3 Dokumentierter Lebenszyklus

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.

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.[4][5]

[4] ISO/IEC 27037:2012. Leitlinien für Identifizierung, Sammlung, Erfassung und Erhaltung digitaler Beweise. https://www.iso.org/standard/44381.html

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

Kapitel 5. Entscheidungsbäume nach Szenario

Wählen Sie den Weg nach Zustand, Ziel und Risiko, nicht nach Gewohnheit.

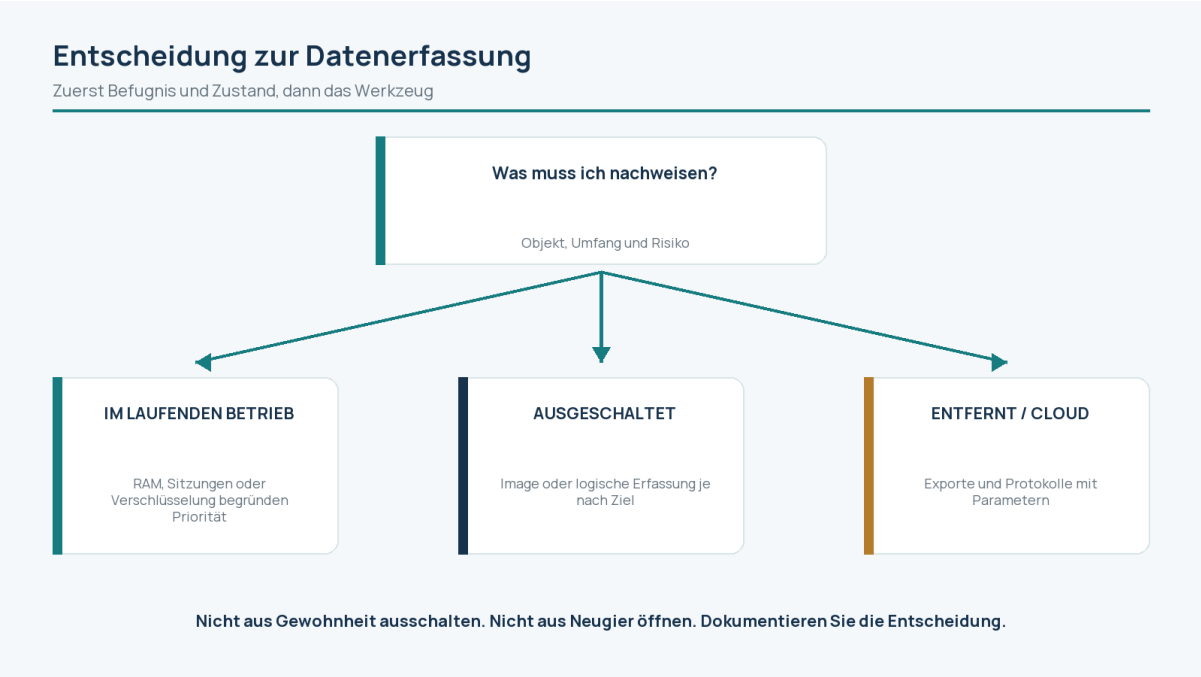


Abbildung 5. Wählen Sie den Weg nach Zustand, Ziel und Risiko, nicht nach Gewohnheit.

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.

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.

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.

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.

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.

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.

5.4 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.

Das Protokoll des Abbruchs enthält den Grund, den verbleibenden Zustand des Objekts, frühere Handlungen, erkannte Risiken und die nächste verantwortliche Person. Es ist kein Misserfolg, sondern dient dazu, Analysemöglichkeiten zu erhalten und nicht vertretbare Handlungen zu vermeiden.

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.

Kapitel 6. Moderne Quellen und Gesprächsdatensätze

Cloud, E-Mail, Anbieter, Protokolle und synthetische Inhalte mit Kontext bearbeiten.



Abbildung 6. Cloud, E-Mail, Anbieter, Protokolle und synthetische Inhalte mit Kontext bearbeiten.

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.

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.

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.

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, aber weder die Wahrheit aller Angaben des Absenders noch die nachgewiesene physische Identität des Absenders.

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.

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.[6]

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.

[6] Mexiko. Disposiciones de carácter general aplicables a las instituciones de crédito, Artikel 316 Bis und Serie. https://www.cnbv.gob.mx/Prensa/Presentaciones%20Seminario%20Corresponsales/i.%20Circular%20%C3%9Anica%20de%20Bancos.pdf

Element der Anfrage	Was vom Anbieter angefordert wird	Was bei Empfang geprüft wird
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.

```
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.

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.[7]

6.6 Regulierung und Gültigkeit ohne isolierte Beispiele

[7] Reglamento (UE) 2024/1689 de inteligencia artificial, Artikel 50, konsolidierter Text vom 27-07-2026. https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/spa/pdf

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.

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.[8][9][10]

[8] Código Penal Federal, Artikel 199 Octies und 199 Nonies, Zusammenstellung mit Reform vom 13-03-2026. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

[9] Kongress von San Luis Potosí. Verabschiedung der Reform zur Ahndung der missbräuchlichen Nutzung von KI, 14-11-2025. https://congresosanluis.gob.mx/content/aprobada-reforma-para-sancionar-uso-indebido-de-inteligencia-artificial

[10] Gaceta Parlamentaria de San Luis Potosí. Aufhebung von 187 Ter und des Kapitels mit 272 Bis und 272 Ter, veröffentlicht am 30-07-2026. http://congresosanluis.gob.mx/sites/default/files/unpload/tl/gpar/2026/07/%C3%9ANICO.pdf

Kapitel 7. Entgegennahme und anfängliche Sicherung

Dokumentieren Sie das Objekt und seinen Zustand vor jeder Analyse.

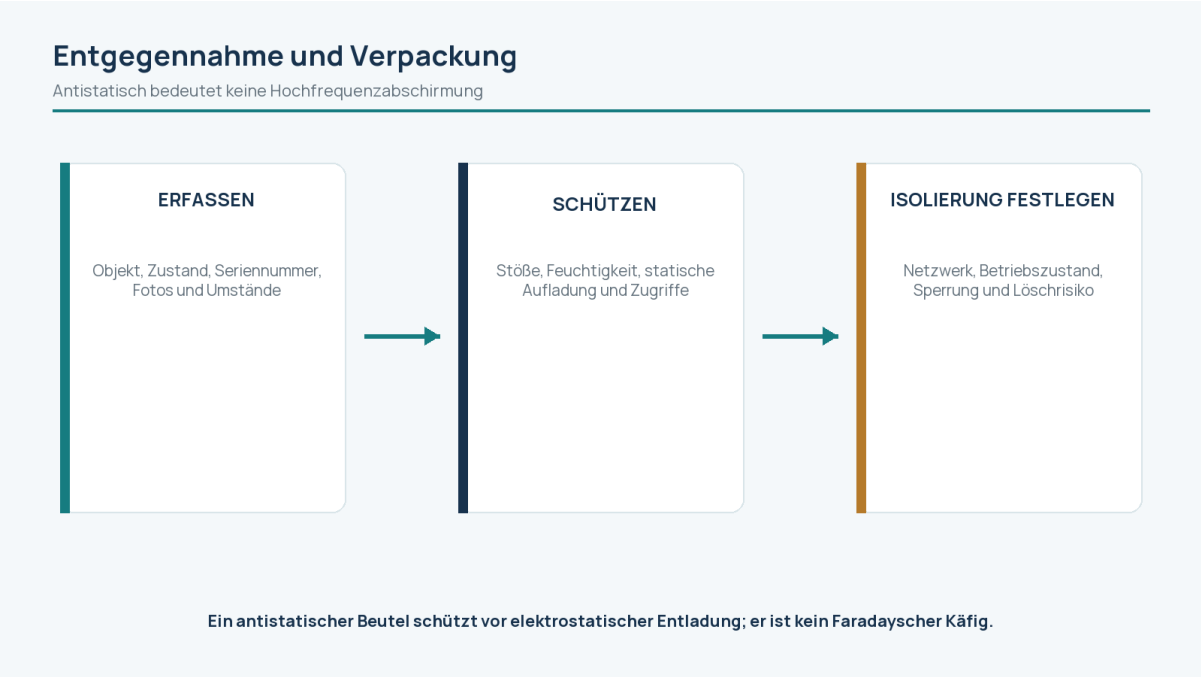


Abbildung 7. Dokumentieren Sie das Objekt und seinen Zustand vor jeder Analyse.

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.

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.

- Eindeutige Kennung des Falls und des Objekts.
- Datum, Uhrzeit, Zeitzone, Ort, Übergabe und Entgegennahme.
- Physische Beschreibung, Seriennummer, Kapazität und Zubehör.
- Betriebszustand, Sperrung, Netzwerk und sichtbare Schäden.
- Übersichtsfotografien und Fotografien der Kennungen.
- Bekannte frühere Handlungen und unmittelbare Risiken.

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.

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.

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.

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 physische Kennzeichnung und das Protokoll müssen mit dem digitalen Inventar und dem abschließenden Bericht übereinstimmen.

```
Ein fiktives Beispiel:
ED-20261109-DEMO-MBL-003-A00

ED = digitale Beweise
20261109 = Entgegennahme
DEMO = fiktiver Fall
MBL = mobile Quelle
003 = drittes Objekt
A00 = anfängliche Erfassung
```

7.4 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 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.

Kapitel 8. Erfassung und technische Dokumentation

Daten mit Methode, Validierung und Nachverfolgbarkeit erlangen.

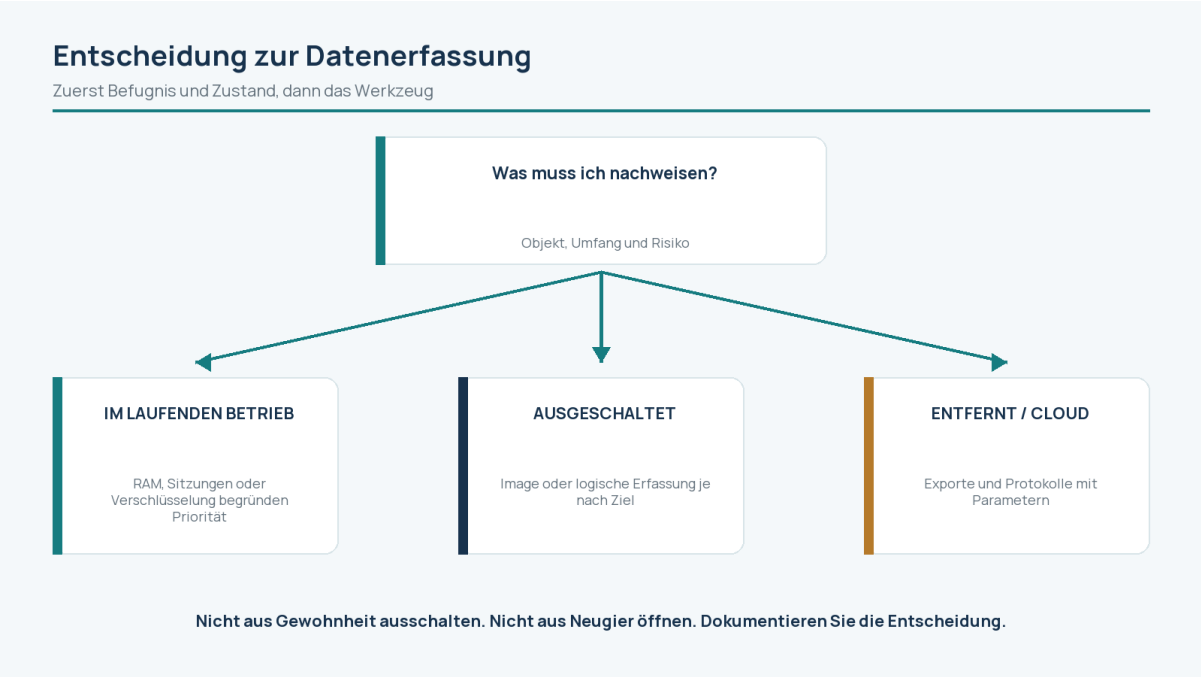


Abbildung 8. Daten mit Methode, Validierung und Nachverfolgbarkeit erlangen.

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.

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.

8.2 Werkzeuge und Validierung

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.

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. Erzeugt ein Werkzeug eine Störung, wird die Meldung aufbewahrt und ihre Auswirkung bewertet, statt sie zu verbergen.

Erfassungsfeld	Fiktives Beispiel	Was es nachweist
Quelle	Datenträger DEMO-SSD-003	Genaue Objektbezeichnung und Verwahrer.
Methode	Bit-für-Bit-Image auf kontrollierter Kopie	Art der Abdeckung.
Werkzeug	Im Labor validierte Bezeichnung und Version	Ausführungsbedingungen.
Datum und Zeitzone	2026-11-09T14:32:07-06:00	Zeitliche Abfolge.
Integrität	SHA-256 des erfassten Objekts	Objekt, auf das sich der Wert bezieht.
Vorkommnisse	Dokumenterter unlesbarer Sektor	Umfang und Grenze des Ergebnisses.

8.3 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.

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.

8.4 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.

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.

Kapitel 9. Verwahrung, Transport und Aufbewahrung

Die Beziehung zwischen Objekt, Verantwortlichem, Standort und Überprüfung aufrechterhalten.

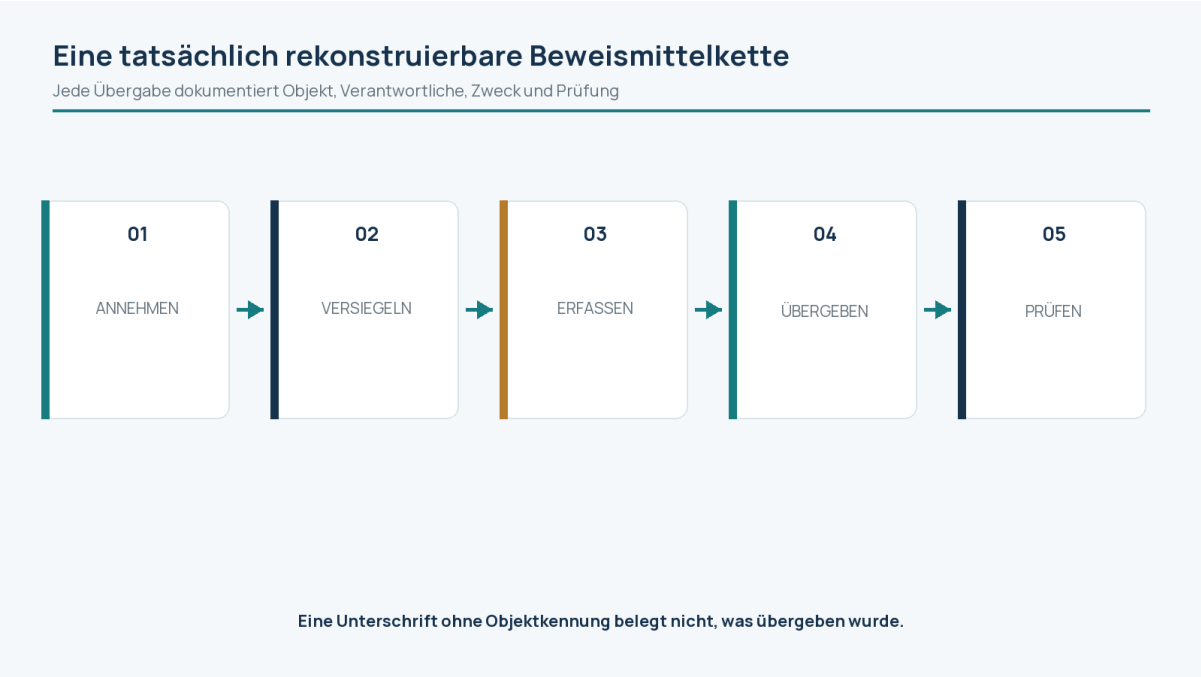


Abbildung 9. Die Beziehung zwischen Objekt, Verantwortlichem, Standort und Überprüfung aufrechterhalten.

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.

Die Kette erfasst auch legitime Zugriffe ohne physische Übertragung: Öffnen des Behältnisses, Erstellen einer Arbeitskopie, vorübergehende Ausleihe, Standortwechsel oder entfernter Download. Wird nur die abschließende Übergabe dokumentiert, entstehen Lücken, die eine Rekonstruktion des Verlaufs verhindern.

9.2 Elektronische Übertragungen

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.

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.

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.

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.

Kapitel 10. Untersuchung, Analyse und Hypothesen

Artefakte in Erklärungen überführen, ohne unbelegte Sprünge in der Beweisführung.

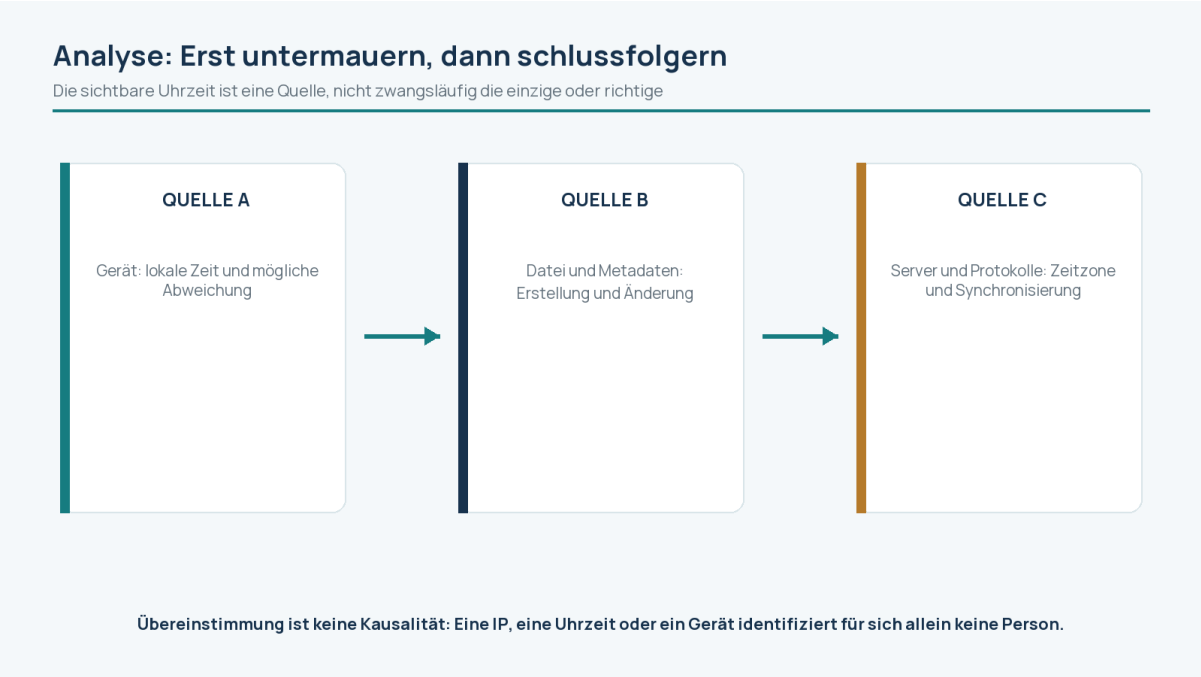


Abbildung 10. Artefakte in Erklärungen überführen, ohne unbelegte Sprünge in der Beweisführung.

10.1 Fragen vor Werkzeugen

Die Analyse beginnt mit Aussagen, die bestätigt oder geschwächt werden können. Jede wird mit Quellen und Prüfungen verknüpft. Ziel ist nicht, bei einem ersten Treffer aufzuhören, sondern auch alternative Erklärungen und Ergebnisse zu suchen, die der ersten Version widersprechen können.

Eine Hypothesenmatrix dokumentiert Aussage, Quelle, Methode, Befund, Alternative und Einschränkung. Dies verringert das Risiko, Artefakte intuitiv auszuwählen, und macht nachvollziehbar, warum sich eine Schlussfolgerung geändert hat. Das Fehlen von Beweisen in einer Quelle kann wichtig sein, muss jedoch im Rahmen ihrer Abdeckung interpretiert werden.

Behauptung	**Quelle und Prüfung**	**Alternative**	**Eingeschränktes Ergebnis**
Das Video ist eine einzige durchgehende Aufzeichnung.	Namen, Datumsangaben, Kapitel und Kontinuität.	Nachträgliche Auswahl oder Konvertierung.	Die Abfolge belegt im geprüften Umfang keine Kontinuität.
Der Vorgang wurde vom Gerät des Kontoinhabers ausgeführt.	Zugriffs-, Geräte- und Sitzungsprotokolle.	Von einer anderen Person verwendete Anmeldedaten.	Nachgewiesen wird die Verwendung von Anmeldedaten, nicht die physische Identität.
Es gab keine Exfiltration.	Netzwerkprotokolle und Übertragungen.	Unvollständige Abdeckung oder verschlüsselter Kanal.	In den geprüften Quellen wurde nichts festgestellt.

10.2 Chronologie und Zeitzonen

Eine Chronologie dokumentiert Datum, Zeitzone, Zeitquelle und Genauigkeit. Die Uhr des Geräts kann falsch eingestellt sein; die Zeitangabe der Datei kann Erstellung, Änderung oder Download bezeichnen; die Serverzeit kann einer anderen Zone folgen. Der ursprüngliche Wert und die Umrechnung werden aufbewahrt, ohne sie als dasselbe Ereignis zu vermischen.

Eine Abfolge von Dateinamen kann bei bestimmten Kameras Hinweise auf Kapitel und Kontinuität geben, beweist für sich allein jedoch nicht, dass das Video vollständig ist. Nomenklatur, Datumsangaben, Struktur, Inhalt und Herkunft werden verglichen. Ein fehlendes Kapitel ist eine offene Frage, kein automatischer Beweis böswilliger Bearbeitung.

10.3 Auswertung von Gesprächsdatenlisten und Protokollen

Bei Gesprächsdatenlisten werden Ereignistyp, Beginn, Dauer, Richtung, Teilnehmer, Funkzellen und Leerfelder geprüft. Ein eingehender Anruf ist nicht dasselbe wie ein ausgehender, und die Funkzelle kann während des Ereignisses wechseln. Technische Kennungen sind nicht automatisch mit Personen gleichzusetzen. Die Auswertung vergleicht Zeitraum und Kontext, nicht nur Nummernübereinstimmungen.

Der Standort einer Funkzelle beweist nicht den genauen Standort einer Person. Erforderlich sind Dokumentation von Abdeckung, Technologie und Zeit sowie weitere Quellen. Wenn eine Bewegungsstrecke behauptet wird, werden Genauigkeitsgrade und Alternativen dargestellt. Eine ansprechende Karte darf nicht in eine nicht vorhandene Gewissheit verwandelt werden.

10.4 Wiederholbarkeit und Reproduzierbarkeit

Wiederholbarkeit zielt auf dasselbe Ergebnis in derselben Umgebung, Reproduzierbarkeit auf dasselbe Ergebnis in einer anderen dokumentierten Umgebung. ISO/IEC 27037 unterscheidet beide Eigenschaften. Der Bericht gibt an, welche Bedingungen variieren können: Werkzeug, Version, System, Filter oder Quelle. Eine Übereinstimmung zwischen Werkzeugen beseitigt keine gemeinsam geteilte Hypothese.

Die Analyse dokumentiert positive, negative und nicht eindeutige Ergebnisse. Es wird nicht versprochen, Ergebnisse zu wiederholen, die von einem Anbieter oder einer flüchtigen Quelle abhängen. Relevante Abfragen und Ausgaben werden aufbewahrt, damit andere die Argumentation prüfen und Fehler aufzeigen können.[4]

Kapitel 11. Bericht, Präsentation und Widerlegung

Die Arbeit klar und ohne übertriebene Gewissheit erläutern.



Abbildung 11. Die Arbeit klar und ohne übertriebene Gewissheit erläutern.

11.1 Struktur des Berichts

Der Bericht beginnt mit Auftrag und Umfang, identifiziert Quellen und Objekte, erläutert die Methode, stellt die Befunde dar, analysiert Alternativen, kommt innerhalb des Umfangs zu einem Ergebnis und weist Einschränkungen aus. Die Anhänge enthalten Protokolle, Manifeste, Hashwerte, Aufzeichnungen und Abbildungen. Die Schlussfolgerung beantwortet die Fragen, ohne neue Anschuldigungen oder nicht angeforderte Rechtsratschläge aufzunehmen.

Die Darstellung unterscheidet beobachtete Tatsachen, Werkzeugergebnisse, Ableitungen und juristische Bewertung. Der Leser muss die Grundlage jeder Aussage erkennen können. Eine Abbildung fasst eine Abfolge oder einen Widerspruch zusammen; sie dient nicht dazu, den Bericht technischer erscheinen zu lassen, als er ist.

- Auftrag, Umfang und Ausschlüsse.
- Objekte, Herkunft und Verwahrung.
- Werkzeuge, Versionen und Parameter.
- Befunde mit überprüfbarem Speicherort.
- Alternative Hypothesen und negative Ergebnisse.
- Schlussfolgerung, Einschränkungen und vollständige Anhänge.

11.2 Sprache für ein nichttechnisches Publikum

Eine technische Erklärung kann präzise und dennoch verständlich sein. Anstatt „die forensische Erfassung von Beweisen wurde durchgeführt“ schreiben Sie „es wurde eine kontrollierte Kopie des Datenträgers erstellt

und ihre Integrität dokumentiert“. Erforderliche Fachbegriffe werden einmal definiert und konsistent verwendet. Abkürzungen ersetzen keine Erklärung.

Die Managementzusammenfassung stellt dar, was geprüft und gefunden wurde und welche Entscheidung getroffen werden kann. Die technischen Details stehen zur Verfügung, ohne dass die Geschäftsleitung sie interpretieren muss. Polizei und Rechtsanwälte müssen die Abfolge ohne Kenntnis der Befehle nachvollziehen können; der Spezialist muss sie anhand der Anhänge wiederholen können.

11.3 Zitate und Rechtsnormen

Eine Quellenangabe enthält Rechtsinstrument, Artikel, Funktion, Version und offizielle Quelle. Ein Gesetz wird nicht wegen eines ähnlichen Namens zitiert und eine Initiative nicht als Dekret dargestellt. Die vergleichende Entsprechung beschränkt sich auf Funktion und Umfang und impliziert nicht dieselben prozessualen Wirkungen. Wurde eine Vorschrift aufgehoben, wird sie als historischer Hintergrund und nicht als geltende Regel erläutert.

Die Prüfung stellt sicher, dass die technische Aussage und die Quellenangabe denselben Gegenstand betreffen. Eine Regel für Nachweise belegt nicht jede Urheberschaft; eine Aufbewahrungsregel bestätigt keinen Wahrheitsgehalt; eine Vorschrift zu Vorfällen beweist keine konkrete Übertragung. Die Quelle dient nicht als Schmuck für eine bereits vorhandene Schlussfolgerung.

11.4 Prüfung auf Widersprüche

Vor der Übermittlung wird geprüft, ob eine andere Person das Objekt finden, die Abfrage wiederholen, die Ableitung nachvollziehen und die Einschränkungen finden kann. Schwierige Fragen werden anhand der Akte beantwortet, nicht mit persönlicher Autorität. Fehlt eine Dokumentation, wird dies anerkannt und der Umfang korrigiert.

Die Prüfung umfasst Titel, Text, Anhänge, Bilder und Metadaten der Übermittlungsdatei. Eine visuelle Validierung darf nicht behauptet werden, ohne das Endergebnis geöffnet zu haben. Für die übermittelte Datei wird ein SHA-256-Hashwert berechnet und ein Manifest aufbewahrt, damit Quelle und Ziel verglichen werden können, ohne dies mit einem Beweis des Inhalts zu verwechseln.

Kapitel 12. Häufige Fehler und kontinuierliche Verbesserung

Bekannte Fehler vermeiden und verbessern, ohne Gewissheit vorzutäuschen.



Abbildung 12. Bekannte Fehler vermeiden und verbessern, ohne Gewissheit vorzutäuschen.

12.1 Fehler, die Fälle verändern

Die kostspieligsten Fehler sind oft einfach: aus Neugier öffnen, aus Gewohnheit ausschalten, ohne URL erfassen, ohne Zeitzone exportieren, Original und Ausdruck verwechseln, eine IP-Adresse einer Person zuordnen, einen Hashwert als Gesamtbeweis darstellen und eine aufgehobene Vorschrift zitieren. Die Prävention beginnt mit klaren Verfahren und einer geschulten ersten Reaktion.

Ist der Fehler bereits aufgetreten, wird er dokumentiert, ohne eine fehlerfreie Kette zu erfinden. Es wird bewertet, was sich verändert hat, was noch überprüft werden kann und welche Schlussfolgerung eingeschränkt werden muss. Frühere Protokolle umzuschreiben, um den Fehler zu verbergen, zerstört Vertrauen und kann der Akte mehr schaden als der ursprüngliche Fehler.

Fehler	Folge	Korrekte Vorgehensweise
Ausschalten nach allgemeiner Regel	Verlust von Speicherinhalten oder Sitzungen.	Den Zustand vor der Entscheidung bewerten.
Antistatik als Faraday-Abschirmung	Falsches Gefühl der Isolierung.	Tatsächliche Isolierung einsetzen und überprüfen.
Hashwert in eine separate Notiz kopieren	Der Bezug zur Übermittlung geht verloren.	EML-Datei, Nachrichtentext und Anhänge aufbewahren.
Auf einen KI-Detektor vertrauen	Falsche Schlussfolgerung über Herkunft oder Wahrheitsgehalt.	Durch Quelle, Methode und Kontext unabhängig bestätigen.

Fehler	Folge	Korrekte Vorgehensweise
Eine veraltete Reform zitieren	Es wird eine nicht geltende Vorschrift behauptet.	Gültigkeit und Aufhebungen prüfen.

12.2 Gewonnene Erkenntnisse

Eine nachträgliche Überprüfung identifiziert, was bei Quellen, Entscheidungen, Werkzeugen, Kommunikation und Präsentation fehlgeschlagen ist. Verbesserungen werden Verantwortlichen zugewiesen und durch Übungen überprüft. Es wird kein nachträglicher Erfüllungsnachweis erzeugt: Dokumentiert wird, wann die neue Praxis in Kraft trat.

Eine neue Version des Handbuchs bewahrt den Verlauf und den Grund der Änderung. Ändert eine Plattform ihren Export, werden Kapitel 6 oder 8 aktualisiert; ändert sich ein Gesetz, werden Anhang A und Register M aktualisiert. Widersprüchliche Anmerkungen werden nicht ohne Prüfung des Haupttexts angehäuft.

12.3 Mindestleitfaden für die gesamte Organisation

Die Organisation muss fünf Fragen beantworten können, ohne von einer einzigen Person abhängig zu sein: Wer autorisiert, wo befinden sich die Beweise, wie wurden sie erlangt, wer hat sie berührt und was kann behauptet werden? Fehlt eine Antwort, beschreibt der Plan, wie die Informationen beschafft oder die Schlussfolgerung eingeschränkt wird.

Das Handbuch dient als Ausgangspunkt, nicht als unveränderliches Dokument. Die Praxis wird an den Fall angepasst, dokumentiert und überprüft. Ziel ist, dass jedes Team methodisch arbeiten, Wissen teilen und eine Erklärung vertreten kann, auch wenn das Ergebnis nicht den Erwartungen entspricht.

Anhang A. Zusammengefasste funktionale Rechtsmatrix

Die Funktion bestimmen, ohne Entsprechungen zwischen Ländern zu erfinden.

A.1 So lesen Sie den Vergleich

Vergleichbar bedeutet funktionale Entsprechung, nicht Identität von Inhalt, Vermutungen, Normadressaten, Fristen oder prozessualen Wirkungen. Die vollständige Matrix wird als separate Datei bereitgestellt, damit sie aktualisiert werden kann, ohne das Handbuch neu zu erstellen. Vor der Anwendung einer Regel werden Instrument, Artikel, sachlicher und persönlicher Geltungsbereich, Kanal, Thema und Version zum Zeitpunkt des Ereignisses geprüft.

Die Tabelle fasst Ausgangsinstrumente zusammen und ist kein vollständiger Katalog. Konnte eine Funktion in der Recherche nicht belegt werden, wird dies vermerkt und nicht durch eine Analogie ergänzt. Zivil-, Straf-, Verwaltungs-, Archiv- und Finanzvorschriften sind nicht austauschbar.[121112131415166]

Jurisdiktion	Funktionale Ausgangsgrundlage	Zentrale Warnung
Mexiko	CCom 89–94 und 1205; CNPCF 348–350; NOM-151; CNBV 316 Bis und Serie.	Schrittweiser Übergang; jeder CNBV-Artikel hat einen eigenen Gegenstand und eine eigene Frist.
Peru	Ley 27269 und Verordnung; CPC 188–197; Archivregime; SBS 504-2021 und 2286-2024.	Das Rechtsregime ist verteilt; nicht alles der Ley 27269 zuschreiben.
Chile	Gesetz 19.799; RAN 20-7, 20-8 und 20-10.	Fortgeschrittene Signatur und Datumsangabe sind zwei verschiedene Fragen.
Argentinien	Ley 25.506; CCyC 318–319; BCRA A 7783 und A 8280.	Vermutungen nur im jeweiligen Rechtsregime; Aufhebungen prüfen.
Kolumbien	Gesetz 527; CPACA; anwendbare SFC-Anweisungen.	Herkunft, Ziel, Datum und Uhrzeit aufbewahren; SFC-Nummern bestätigen.
Ecuador	Ley 67; Resolución JPRM-2025-006-M für Zahlungen.	Das Zahlungssystem reproduziert nicht die gesamte CNBV.

[11] Peru. Ley 27269 und Reglamento de Firmas y Certificados Digitales. https://www.gob.pe/institucion/indecopi/normas-legales/5570542-ley-27269

[12] Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur. https://www.bcn.cl/leychile/navegar?idNorma=196640

[13] Argentinien. Ley 25.506 de Firma Digital. https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

[14] Kolumbien. Ley 527 de 1999 über Datennachrichten und elektronischen Handel. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

[15] Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. https://ventas.icert.fje.gob.ec/documents/10181/11670/leyComercioElectronico.pdf/e0a3116a-acd9-42ce-97ac-4d28b32a2f2e

[16] Spanien. Ley de Enjuiciamiento Civil, Artikel 326 und 384, konsolidierter Text. https://www.boe.es/buscar/act.php?id=BOE-A-2000-323

Jurisdiktion	Funktionale Ausgangsgrundlage	Zentrale Warnung
Spanien / EU	eIDAS; LEC 326 und 384; RD-ley 19/2018, 45, 66 und 67.	Einfache, fortgeschrittene und qualifizierte Signaturen haben nicht dieselben Wirkungen.

A.2 Aktualisierungsmethode

Die Aktualisierung dokumentiert offizielle Quelle, Konsultationsdatum, gelesenen Artikel und operative Änderung. Eine Vorschrift wird nicht durch eine Nachricht oder ein Gesetzesvorhaben durch ein Dekret ersetzt. Die vollständige Matrix enthält Quellenangaben zu Anerkennung, Schriftform, Zurechnung, Integrität, Original, Zugänglichkeit, Aufbewahrung, Zulässigkeit, Beweislast und Finanzregulierung.

ISO/IEC 27037 und NIST SP 800-86 werden als Methodik zitiert, nicht als nationale Gesetze. Der Anhang soll Orientierung dazu geben, was aufzubewahren, anzufordern, zu überprüfen und einzuschränken ist, und nicht eine Akte anhand einer Tabelle ähnlicher Formulierungen entscheiden.[45]

Anhang B. Formular für Umfang und Befugnisse

Ausgangsformular zur Abgrenzung der Arbeit.

B.1 Format

Wird vor jeder Maßnahme ausgefüllt. Fehlt eine Angabe, werden der Grund und die Person vermerkt, die sie bestätigen muss. Kritische Felder bleiben nicht leer, um sie erst nach der Erfassung auszufüllen.

Feld	Zu registrierender Inhalt	Fiktives Beispiel
Kennung	Eindeutiger Auftragscode.	EXP-DEMO-2026-001
Frage	Nachzuweisender Sachverhalt.	Feststellen, ob die Verkäufe übermittelt und abgerechnet wurden.
Zeitraum	Beginn, Ende und Zeitzone.	1.–3. November 2026, UTC−06:00.
Einbezogene Quellen	Autorisierte Systeme, Dateien und Verwahrer.	Abrechnungsdatei, Zahlungsabwickler und Bankberichte.
Ausschlüsse	Daten oder Geräte außerhalb des Mandats.	Nicht damit zusammenhängende persönliche Geräte.
Autorisierung	Inhaber, Handlungen und Kanal.	Autorisierte Adresse; registrierter sicherer Kanal.
Ergebnisdokument	Berichtsart und Anhänge.	Technischer Bericht, Manifest und Protokolle.
Risiken	Veränderung, Verlust und Vertraulichkeit.	Rotation von Protokollen und Daten Dritter.

Anhang C. Entgegennahmeprotokoll

Dokumentieren Sie den Zustand vor jeder Analyse.

C.1 Mindestdaten

Dem Protokoll werden Übersichtsfotografien und Fotografien der Kennungen beigefügt. Frühere Handlungen werden auch dann dokumentiert, wenn sie fehlerhaft waren; sie werden nicht nachträglich korrigiert, um eine ideale Entgegennahme vorzutäuschen.

Feld	Erforderlicher Inhalt
Objekt und Kennung	Typ, Marke, Modell, Seriennummer, Kapazität und zugewiesener Code.
Übergabe und Entgegennahme	Name, Funktion, Datum, Uhrzeit, Zeitzone und Ort.
Zustand	Betriebszustand, Sperrung, Netzwerk, Schäden und Zubehör.
Siegel und Verpackung	Typ, Kennung, Zustand und Fotografien.
Frühere Handlungen	Öffnungen, Verbindungen, Kopien, Änderungen oder Unbekanntes.
Risiken	Volatilität, Fernlöschung, Daten Dritter und Priorität.
Erste Entscheidung	Sicherung, Weiterleitung, Erfassung oder Klärung sowie Verantwortlicher.

Anhang D. Erfassungsprotokoll

Quelle, Methode, Ausgabe und Überprüfung verknüpfen.

D.1 Protokoll für jedes Objekt

Jede Erfassung erhält ein eigenes Protokoll. Wird sie wiederholt, wird eine neue verknüpfte Kennung vergeben und der Grund erläutert, ohne den ersten Versuch zu löschen.

Feld	Erforderlicher Inhalt
Quelle und Verwahrer	Genaue Kennung und Person, die die Quelle aufbewahrt.
Methode und Begründung	Physisch, logisch, flüchtig, entfernt oder dokumentarisch sowie Begründung.
Werkzeug	Name, Version, Umgebung und Validierung.
Parameter	Filter, Felder, Datum, Zeitzone und Konfiguration.
Ausgabe	Name, Pfad, Format, Größe und Beziehung zwischen Original und Kopie.
Integrität	Algorithmus, Wert, Datum und abgedecktes Objekt.
Vorkommnisse	Fehler, Auslassungen, Sektoren, Zugriffe und Auswirkungen auf den Umfang.
Überprüfung	Öffnung, Vergleich, Wiederholung und Prüfer.

Anhang E. Beweismittelkette und Übertragungen

Jeden Zugriff und jede Bewegung rekonstruieren.

E.1 Protokoll für jedes Ereignis

Auch das Öffnen eines Behältnisses, ein entfernter Download und die Erstellung einer Arbeitskopie werden dokumentiert. Die Übertragung ist erst abgeschlossen, wenn Empfang und Zustand des Objekts bestätigt wurden.

Datum und Zeitzone	Gegenstand	Übergabe	Entgegennahme	Zweck	Siegel/Integrität
09. November 14:32 −06	ED-DEMO-003	Verwahrer A	Analyst B	Erfassung	Siegel 01 intakt
09. November 16:05 −06	ED-DEMO-003-A00	Analyst B	Verwahrer C	Verwahrung	Übereinstimmender Hashwert
10. November 09:10 −06	ED-DEMO-003-A01	Verwahrer C	Prüfer D	Überprüfung	Dokumentierter Zugriff

Anhang F. Anfrage an einen Anbieter und EML-Übermittlung

Format, Kontext und Integrität bei entfernten Protokollen sicherstellen.

F.1 Felder der Anfrage

Die Anfrage wird an Anbieter und autorisierten Kanal angepasst. Passwort oder Anmeldedaten werden weder im Protokoll noch im Nachrichtentext aufgeführt. Der sichere Kanal wird durch eine Referenz bezeichnet, nicht durch Geheimnisse.

Element	Erforderlicher Inhalt
Fallakte und Autorisierung	Code, Inhaber und Verweis auf den sicheren Kanal.
Konto und Umfang	Autorisierte Kennungen, Zeitraum, Zeitzone und Ausschlüsse.
Format	Verfügbares natives Format und Lesekopie, Feldverzeichnis und Extraktionsprozess.
Integrität	Algorithmus und Hashwert jeder Datei im Nachrichtentext der Antwort.
Übermittlung	EML-Datei mit Nachrichtentext, Kopfzeilen und Anhängen; gegebenenfalls Link und Berechtigungen.
Einschränkungen	Aufbewahrung, fehlende Felder, Abdeckung, Fehler und Klarstellungen.

F.2 Überprüfung bei Empfang

Die EML-Datei wird gespeichert, bevor mit den Anhängen gearbeitet wird. Hashwerte der EML-Datei und der Dateien werden getrennt berechnet und mit dem Nachrichtentext verglichen. Abweichungen werden dokumentiert und eine Klärung angefordert. Fehlt der Hashwert des Anbieters, wird dies vermerkt und ein lokaler Wert berechnet, ohne ihn dem Anbieter zuzuschreiben.

6. Vollständige EML-Datei aufbewahrt und lesbar.
7. Empfangene native Dateien und ihre Verknüpfung mit dem Nachrichtentext.
8. Algorithmus und Werte verglichen und dokumentiert.
9. Felder, Einheiten, Zeitzone und Extraktionsprozess nachvollzogen.
10. Einschränkungen und Abweichungen dokumentiert.

Anhang G. Inventar und Dateimanifest

Beziehung zwischen Herkunft, abgeleiteten Objekten und Ergebnissen aufrechterhalten.

G.1 Spalten des Manifests

Das Manifest enthält Kennung, Name, Pfad, Objekttyp, Herkunft, Methode, Größe, Format, Hashwert und Anmerkungen. Es veröffentlicht keine sensiblen Daten oder Geheimnisse. Der Pfad kann in der öffentlichen Version abgekürzt werden, wenn er geschützte Informationen offenlegt.

Kennung	Beziehung	Datei	Format	Integrität
ED-DEMO-003	Empfangenes Original	sabanas.csv	CSV	SHA-256 bei Entgegennahme berechnet
ED-DEMO-003-A00	Zugehörige Übermittlung	entrega.eml	EML	Objekt unabhängig von der CSV-Datei
ED-DEMO-003-A01	Arbeitskopie	sabanas_trabajo.csv	CSV	Anderer Hashwert bei geänderter Struktur
ED-DEMO-003-R01	Präsentation	informe.pdf	PDF	Hashwert der übermittelten Datei

Anhang H. Chronologie und Zeitzonen

Verborgene Umrechnungen und falsche Übereinstimmungen vermeiden.

H.1 Korrelationstabelle

Der ursprüngliche Wert jeder Quelle wird aufbewahrt und durch die Umrechnung ergänzt, nicht ersetzt. Ist die Geräteuhr unzuverlässig, werden die bekannte Abweichung oder die Unsicherheit angegeben.

Ereignis	Zeitquelle	Ursprünglicher Wert	Zeitzone	Umrechnung und Einschränkung
Videoaufzeichnung	Geräteuhr	06:04:16	Unbekannt	Nicht UTC annehmen; mit einer anderen Quelle vergleichen.
Export	Server	2026-11-01T12:04:16Z	UTC	06:04:16 in UTC−06; Sommerzeit aufzeichnen.
EML-Empfang	E-Mail-Client	09. November 07:05	UTC−06	Empfangszeit, nicht Zeitpunkt des untersuchten Geschehens.

Anhang I. Hypothesen- und Analysematrix

Bestätigung, Alternative und Einschränkung dokumentieren.

I.1 Vorlage für die Argumentation

Jede Aussage wird anhand von Quellen geprüft, die sie bestätigen oder schwächen können. Der Prüfer ergänzt Alternativen, die der Analyst nicht berücksichtigt hatte, und es wird dokumentiert, wie sich die Schlussfolgerung ändert.

Behauptung	Quelle/Prüfung	Alternative	Ergebnis
Die Datei ist das Original.	Herkunft, Metadaten und Verwahrung.	Vorheriger Export oder vorherige Bearbeitung.	Nur die empfangene Darstellung wird nachgewiesen.
Der Benutzer hat den Vorgang autorisiert.	Authentifizierung, Gerät und Sitzung.	Kompromittierte Anmeldedaten.	Die Verwendung von Anmeldedaten ist nicht gleichbedeutend mit der physischen Identität.
Es gibt keine weiteren Dateien.	Dokumentierte Abfrage und Abdeckung.	Filter, Aufbewahrung oder Format.	Im abgefragten Umfang wurden keine weiteren Dateien festgestellt.

Anhang J. Prüfung synthetischer Inhalte

Erstellung, Bearbeitung, Konvertierung und Veröffentlichung trennen.

J.1 Mindestunterlagen

Ziel ist nicht, etwas allein aufgrund seines Aussehens als „Deepfake“ zu erklären. Jede bekannte Umwandlung wird mit ihren Beweisen und Einschränkungen dokumentiert. Der Detektor wird mit Version und bekannter Fehlerrate angegeben, sofern verfügbar; er wird nicht als einziger Beweis verwendet.

11. Empfangene Originaldatei und Herkunft.
12. Verfügbare Angaben zu Werkzeug, Version und Erstellungs-/Bearbeitungsverlauf.
13. Codec, Komprimierung, Metadaten und Versionen verglichen.
14. URL, Veröffentlichung, Kennzeichnung, Publikum und Kontext.
15. Einwilligung, Identität, Zweck und geltende Vorschrift geprüft.
16. Detektoren und unabhängige Bestätigung mit ausdrücklich genannten Einschränkungen.

Anhang K. Vorlage für einen technischen Bericht

Befunde darstellen, ohne Tatsachen und Ableitungen zu vermischen.

K.1 Aufbau des Berichts

Der Abschlussbericht enthält Deckblatt, Auftragsidentifikation, Inhaltsverzeichnis, Managementzusammenfassung, Umfang, Quellen, Methode, Befunde, Analyse, Schlussfolgerung, Einschränkungen und Anhänge. Jede Aussage verweist auf eine Fundstelle und ist entsprechend ihrer Beweiskraft formuliert.

Abschnitt	Zu beantwortender Inhalt
Auftrag	Was wurde angefordert, zu welchem Zweck und mit welchen Ausschlüssen?
Quellen	Was wurde von wem und in welcher Darstellung empfangen?
Methode	Was wurde mit welchem Werkzeug und welchen Parametern durchgeführt?
Befunde	Was wurde beobachtet und wo kann es aufgefunden werden?
Analyse	Welche Erklärungen sind mit den Befunden vereinbar und welche werden geschwächt?
Schlussfolgerung	Was kann innerhalb des Umfangs behauptet werden?
Einschränkungen	Was wurde nicht nachgewiesen und welche Quellen fehlen?
Anhänge	Protokolle, Manifest, Hashwerte, Aufzeichnungen und Abbildungen.

Anhang L. Checklisten

Die Arbeit vor jeder Übermittlung prüfen.

L.1 Entgegennahme und Erfassung

Die Checkliste wird anhand von Beweisen ausgefüllt, nicht aufgrund von Absichten. Ist ein Punkt nicht anwendbar, werden Grund und Genehmigung vermerkt. Kein kritischer Punkt bleibt unbeantwortet.

17. Befugnis, Umfang und Ausschlüsse dokumentiert.
18. Objekt, Zustand, Fotografien und Verantwortliche identifiziert.
19. Methode anhand von Quelle und Risiko begründet.
20. Werkzeug, Version und Parameter dokumentiert.
21. Hashwerte, EML-Datei und zugehörige Dateien aufbewahrt.
22. Vorkommnisse und Einschränkungen in der Akte enthalten.

L.2 Bericht und Veröffentlichung

Die Endprüfung erfolgt anhand der geöffneten Datei, nicht des Arbeitsentwurfs. Bilder werden für eine Veröffentlichung sowohl in voller Größe als auch als Miniaturansicht geprüft.

23. Schlussfolgerung im Einklang mit Quellen und Umfang.
24. Gültige Quellenangaben, Artikel und Funktionen überprüft.
25. Keine Kundennamen, Anmeldedaten oder unnötigen Daten.
26. Inhaltsverzeichnis, Abbildungen, Tabellen und Anhänge lesbar.
27. Enddateien geöffnet und visuell geprüft.
28. SHA-256-Hashwerte von Quelle und Ziel stimmen überein; Manifest aufbewahrt.

Anhang M. Versionskontrolle für Rechtsnormen und das Handbuch

Aktualisieren, ohne Widersprüche anzuhäufen.

M.1 Änderungsprotokoll

Jede normative oder methodische Änderung dokumentiert Quelle, Datum, betroffenes Kapitel, redaktionelle Entscheidung und Prüfer. Wird eine Vorschrift aufgehoben, werden Haupttext und häufige Fragen geändert, nicht nur eine Anmerkung am Ende ergänzt.

Datum	Quelle	Änderung	Redaktionelle Maßnahme	Überprüfung
30. Juli 2026	Gaceta SLP	187 Ter, 272 Bis und 272 Ter aufgehoben.	Als historischen Hintergrund erläutern; Beiträge und Anhang A aktualisieren.	Vollständig
27. Juli 2026	EUR-Lex	Konsolidierte Fassung der KI-Verordnung konsultiert.	Artikel 50 mit korrektem Geltungsbereich und korrekten Ausnahmen zitieren.	Vollständig
09. November 2026	Handbuch	Überprüfung von Sprache und Formaten.	EML, Gesprächsdatenlisten und Checklisten für die erste Reaktion aufnehmen.	Vollständig

M.2 Abschluss der Nutzung

Dieses Handbuch ist ein allgemeiner Leitfaden. Es stellt weder eine Rechtsberatung noch ein forensisches Gutachten zu einem konkreten Fall dar. Die Anwendung erfordert eine Prüfung von Befugnis, Gerichtsbarkeit, Sachverhalt, Kanal und geltender Vorschrift. Die Version wird mit Ressourcen und einer separaten Matrix bereitgestellt, damit Aktualisierungen geprüft werden können, ohne das Layout des Bandes zu verlieren.