TEQUILA SO
Jocsan Laguna

数字证据处理

保存、获取、记录、分析与呈现

实用手册 · 2026



手册前言

本手册说明如何以可供他人复核的方法接收、保全、取证获取、移交、分析和出示数字证据。读者对象为警务人员、鉴定人、律师及组织负责人。无需具备工程师背景：每个术语均配有操作说明和示例。本手册也不替代各案所需的授权、法律依据和专业判断。

核心规则很简单：不是打开设备寻找能够印证怀疑的内容，而是先确定需要证明什么、证据可能位于何处，选择适当且侵扰最小的方法，并记录所实施的操作。有用的结论并非语气最笃定，而是能够清楚区分事实、推论和待解问题。

如何使用本手册

如果你是第一个接收案件的人，请阅读第 1、3、5 和 7 章，了解如何界定委托范围、分配职责、选择取证获取路径并规范记录接收过程。如果负责取证获取或分析，请使用第 4、6、8、9 和 10 章。如果需要审查申请、报告或出示材料，请使用第 2、11 和 12 章以及附录 A、K、L 和 M。

示例均为虚构，内容完整，用于展示推理过程，而非要求照搬固定做法。各类格式包含填写字段和说明。法律矩阵比较的是功能，并不声称两个条文完全等同。日期和版本至关重要：使用某项规范前，应确认其现行有效，并适用于相关事实、主体、渠道和程序。

指导原则

原则	实际应用
最小改动	选择改动最少的方法，并记录任何不可避免的改动。
授权先于访问	获得许可不等于具备访问的技术能力，两者缺一不可。
语境先于片段	孤立截图不能替代文件、完整消息或原始发布内容。
奥卡姆剃刀	应从最能区分不同假设的数据源入手，而不是一味堆叠工具。
决策不带自我偏见	如果证据与最初说法相矛盾，应修正结论，而不是改动原始材料。
可复现性	另一位具备资质的人员必须能够定位、复核并重复该程序。
明确局限	未观察到或无法证明的事项应如实声明，不得用推测填补。
保护人员	保全证据并不意味着可以传播数据或使任何人再次受害。

目录

手册前言 2
如何使用本手册 3
指导原则 4
目录 5
第1章 范围、问题与授权 8
1.1 统领全部工作的问题 8
1.2 授权、比例原则与保密 9
1.3 数据源初步清单 9
1.4 完整示例：销售款项争议 10
第2章 完整性、原始材料与语境 11
2.1 原始材料不一定就是设备 11
2.2 完整性、真实性、归属与内容真实性 11
2.3 哈希是控制手段，而非教条 12
2.4 可访问性与语境保存 12
第3章 角色与职责 14
3.1 职能先于职务 14
3.2 操作沟通 15
3.3 独立性与复核 15
第4章 生命周期与取证准备 16
4.1 接收案件前做好准备 16
4.2 不可逆节点 16
4.3 记录在案的流程 17
第5章 不同情景下的决策树 18
5.1 设备开机或关机 18
5.2 本地、远程或通过供应商取证获取 18
5.3 移动设备与隔离 19
5.4 何时停止 19
第6章 现代数据源与通话记录表 20
6.1 云服务、SaaS 与导出文件 20
6.2 电子邮件与 EML 20
6.3 通话记录表的申请与接收 21

6.4 供应商申请正文示例 22
6.5 虚拟化、物联网与合成内容 22
6.6 法规与现行效力：不得仅凭孤立示例 23
第7章 接收与初步保全 24
7.1 清晰易懂的接收记录 24
7.2 包装与封存 25
7.3 标签与对象关系 25
7.4 文件和消息的接收 25
第8章 取证获取与技术记录 26
8.1 物理、逻辑、易失性与文档化获取 26
8.2 工具与验证 26
8.3 可复现的导出与查询 27
8.4 错误与异常 27
第9章 保管、移交与保存 28
9.1 能回答问题的保管链 28
9.2 电子移交 28
9.3 存储与后续访问 29
第10章 检查、分析与假设 30
10.1 问题先于工具 30
10.2 时间线与时区 31
10.3 通话记录表与日志的解读 31
10.4 可重复性与可复现性 31
第11章 报告、出示与质证 32
11.1 报告结构 32
11.2 面向非技术读者的语言 32
11.3 引文与法律规范 33
11.4 质证复核 33
第12章 常见错误与持续改进 34
12.1 会改变案件的错误 34
12.2 经验教训 35
12.3 整个组织的最低指南 35
附录A 简明功能法律矩阵 36

A.1 如何阅读比较表 36
A.2 更新方法 37
附录B 范围与授权表 38
B.1 格式 38
附录C 接收记录 39
C.1 最低数据要求 39
附录D 取证获取记录 40
D.1 按对象记录 40
附录E 保管链与移交 41
E.1 按事件记录 41
附录F 供应商申请与 EML 交付 42
F.1 申请字段 42
F.2 接收时验证 42
附录G 文件清单与清单文件 43
G.1 清单文件列 43
附录H 时间线与时区 44
H.1 对应关系表 44
附录I 假设与分析矩阵 45
I.1 推理模板 45
附录J 合成内容审查 46
J.1 最低案卷要求 46
附录K 技术报告模板 47
K.1 写作结构 47
附录L 核查清单 48
L.1 接收与取证获取 48
L.2 报告与发布 48
附录M 法律规范与手册版本控制 49
M.1 变更记录 49
M.2 使用说明结语 49

第1章 范围、问题与授权

在接触证据之前，先确定需要证明什么。



图1 在接触证据之前，先确定需要证明什么。

1.1 统领全部工作的问题

有效的委托不会只说“检查一切”，而会说明发生了什么、需要证明什么、结果将用于何处以及截止日期。答案决定需要哪些数据源，以及何种程度的改动具有正当性。用于恢复业务连续性的文件恢复，与必须经受司法质证的鉴定并不相同，即使二者使用相同工具。

用简明语言记录事实：谁提出主张、主张什么、另一方否认什么，以及根据最初陈述存在哪些证据。区分某人亲眼所见与某人主观推测。这种区分可以防止初始假设演变成只寻找支持该假设证据的指令。

问题	应书面记录的内容	避免临时处置的决策
各方分别主张什么？	按人员和日期分别记录的说法。	避免把一方的说法当作已证实的事实。
需要证明什么？	事实、时间段、系统和预期结果。	界定数据源和方法。
结果将用于什么？	业务连续性、内部调查、司法鉴定或诉讼程序。	确定文档记录的详细程度。

问题	应书面记录的内容	避免临时处置的决策
哪些内容可以排除在范围之外?	被排除的数据、设备、账户或时间段。	减少不必要的暴露。

1.2 授权、比例原则与保密

授权应载明授权人、范围、允许实施的操作、系统、负责人和沟通渠道。如果需要访问第三方信息、共享账户或供应商系统，应记录合法获取途径。鉴定人不会因为知道如何取得访问权限，就有权自行授予访问权限。

比例原则要求审查数据源和方法是否为达成目标所必需。如果管理性导出比全面检查设备更能回答问题，就应选择前者。保密并非附加要求：从接收时起，就必须决定谁可以查看、复制、传输和发布信息，尤其是涉及第三方或受害人的数据时。

行动规则

如果授权或范围不明确，应停止行动并予以澄清。“不知道是否可以”不能成为可辩护的保管依据。应记录疑问、收到的答复、答复人及答复时间。

1.3 数据源初步清单

列出能够提供语境的设备、账户、文件、服务器、供应商、文档和人员。同时列出不可用的数据源及原因：设备遗失、密码未知、保存期限届满、供应商未答复或访问未获授权。缺失同样会改变工作计划和可能得出的结论。

应根据解决假设的能力、易失性和丢失风险确定优先级。RAM、活动会话、滚动覆盖的日志和即将失效的链接，可能需要采取不同措施。优先级不取决于哪台设备看似更重要，而取决于哪些信息可能最先消失，以及这些信息能回答什么问题。

- 数据源标识符和当前保管人。
- 数据类型、时间段和预期格式。
- 与待证事实的关系。
- 状态：可用、受限、不确定或无法访问。
- 改动、丢失或暴露风险。

- 授权途径和下一步联系人。

1.4 完整示例：销售款项争议

一家连锁商声称其已完成销售但未收到款项。目标不是“检查其所有计算机”，而是确定交易是否被记录、传输和结算。应界定日期、金额、参考编号和支付处理方。优先数据源包括商家报告、汇款批次文件、支付处理方记录、互联设备和银行报告。

授权仅限于这些系统和相应时间段。如果交易未出现在商店自行生成的汇款批次文件中，该发现可以引导调查，但尚不能证明是谁造成了不一致。该计划既避免了对个人设备的侵扰性检查，也要求比较相互独立的数据源。

1. 委托内容及各方说法分别记录。
2. 授权和排除事项已明确。
3. 按问题和易失性排列数据源优先级。
4. 第三方数据和保密措施已明确。
5. 预期结果和初始局限已记录。

第2章 完整性、原始材料与语境

理解关于文件可以断言什么、不能断言什么。

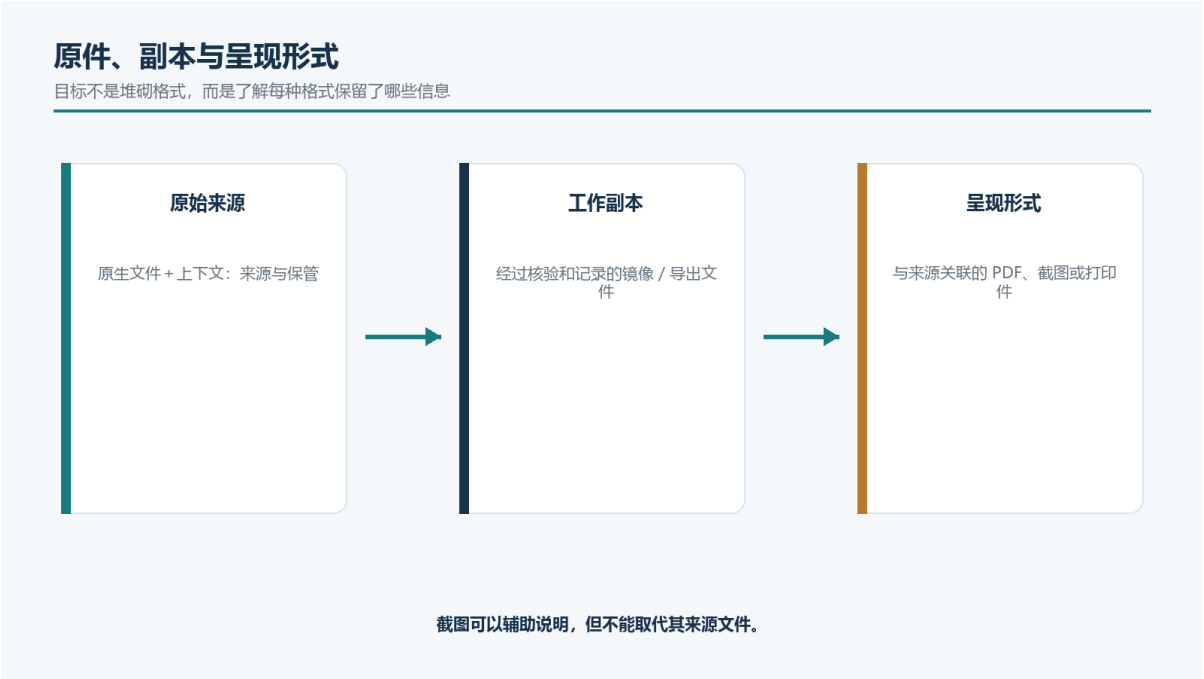


图2 理解关于文件可以断言什么、不能断言什么。

2.1 原始材料不一定就是设备

在数字证据中，“原始”的概念以最终形式下的完整性和事后可查阅性为基础，而不只是保留某台设备。原生文件、逐位镜像、导出文件、截图和打印件是不同的表现形式。只要清楚其与来源的关系，以及保留或丢失了哪些信息，每种形式都可能有其用途。

墨西哥《商法典》第 93 和 93 Bis 条涉及书面形式、原件、完整性和可访问性，CNPCF 第 348 至 350 条则对电子信息规定了类似功能。这些规则不会把所有副本都变成原件，也不会让所有 PDF 都成为完整数据源。必须记录所持的是哪种表现形式，以及它是如何取得的。[1][2]

2.2 完整性、真实性、归属与内容真实性

完整性是指对象在所声明的范围内保持完整且未改动。真实性要求有依据证明对象确如其所称。归属将某项操作或文件与来源联系起来；内容真实性则关注所叙述的事件是否确实发生。混淆这些概念会导致过度结论：一个文件可以保持完整，却自创建之时起就是虚假的。

[1]墨西哥《商法典》，第 89–94 和 1205 条，官方汇编。https://www.diputados.gob.mx/LeyesBiblio/pdf/CCom.pdf

[2]《国家民事和家庭诉讼法典》，第 348–350 条，查阅的汇编包含 15-01-2026 的修订。https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPCF.pdf

有效签名在相应法律制度下可以产生作者身份和完整性的推定，但不能证明某个自然人点击了某个具体按钮，也不能证明全部陈述均为真实。审查应包括证书、有效期、方法、语境和密钥泄露的可能性，并寻求独立印证。

稳妥表述	需要哪些证据	应避免的表述
哈希值一致。	记录相同的算法、比较对象和比较时间。	内容是真实的。
文件自那时起未发生变化。	接收时计算哈希值，并在其后进行验证。	文件从未被篡改。
导出文件包含这些字段。	供应商的方法、参数和格式。	导出文件是完整的。
在检查范围内未观察到活动。	数据源、筛选条件、时间段和可复现的查询。	该活动从未存在。

2.3 哈希是控制手段，而非教条

哈希函数生成可用于比较对象的值。如果两个文件使用同一算法得到相同值，则在本次比较中，二者的逐位内容一致。如果文件发生变化，哈希值也会变化。这有助于发现替换或差异，但不能解释差异为何发生，也不能证明来源、日期、作者身份或内容真实性。

应记录算法、操作员、日期和时区、具体对象、位置及其与证据的关系。SHA-256 是完整性控制的常用选择，并非神奇咒语。同一信息的两种不同表现形式可能具有不同哈希值，这并不能证明其虚假；即使可见内容相似，格式转换也可能改变文件。

报告中的正确表述

“接收文件的 SHA-256 为 [值]，计算时间为 [日期和时区]。后续验证结果一致。这证明该对象在两次校验之间未发生变化，但不证明其为真实文件，也不证明其自形成之初即内容完整。”

2.4 可访问性与语境保存

无法访问的对象无法接受复核。保存不仅要求留存，还要能够打开、读取、解读信息，并将信息与其语境联系起来。专有格式文件可能需要特定软件版本、格式文档或补充导出文件。可视化副本有助于展示，但不得因此删除原生文件或验证所需的数据。

NOM-151-SCFI-2016 规定了墨西哥的保存和数字化要求。它不能替代个案方法，也不能证明内容真实性。保存工作应涵盖访问条件、完整性、与原始材料的关系、可用元数据、负责人，以及任何相关记录或参与的第三方。[3]

[3]NOM-151-SCFI-2016，数据电文的保存和数字化。https://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017

第3章 角色与职责

明确谁决策、谁执行、谁记录、谁复核。



图3 明确谁决策、谁执行、谁记录、谁复核。

3.1 职能先于职务

在案件允许的情况下，同一人可以承担多项职能，但每项操作都必须对应一项具体职能。授权、执行、记录、保管、复核和沟通并不相同。主管不一定负责取证获取；技术人员不能独自决定发布什么；律师也不能替代技术验证。

对于执法机构，这种区分使未受过工程培训的人员也能接收和保护案件材料，而不必充当临时分析师。第一响应人员记录状态和风险、保护对象并请求支持。专家根据接收记录决定方法，而不是依据不完整的电话描述。

职能	主要职责	预期记录
委托授权方	界定范围、许可和排除事项。	授权及获批的变更。
第一响应	识别状态、避免丢失并请求支持。	初始记录和照片。
专业人员	选择并实施方法。	取证获取、工具和异常情况。
保管人	控制访问、位置和移交。	保管链。

职能	主要职责	预期记录
复核人	核对方法、发现和局限。	复核意见和处理结果。

3.2 操作沟通

行动前，应明确谁可以解答技术、法律和保管问题。通讯录包括姓名、职能、渠道、可联络时间和代理人。紧急决策应记录日期和理由；非正式电话不得成为某项不可逆操作的唯一记录。

向供应商交付材料时，应以能够还原对话的格式保存沟通记录。供应商通过电子邮件发送文件时，应保存包含正文、邮件头和附件的 EML。如果约定排除某些内容或重新导出，应将其纳入授权和变更记录。

3.3 独立性与复核

独立复核旨在发现错误，而不是追究过错。复核检查对象是否正确、方法是否回应委托、日期是否一致，以及结论是否超出发现。复核人可以要求重复查询或增加数据源，但不得为了使原始材料与初步版本一致而改动原始材料。

记录假设和不利结果有助于控制自我偏见。只为印证分析师既有结论的复核不是独立复核。报告应使他人能够理解发现了什么、排除了什么以及哪些问题仍未解决，即使答案不利于委托人。

第4章 生命周期与取证准备

在事件发生前避免证据丢失。



图4 在事件发生前避免证据丢失。

4.1 接收案件前做好准备

取证准备是指了解有哪些资产、每项资产产生哪些日志、谁可以导出、保存多久以及如何请求协助。准备充分的组织不会永久记录一切，而是识别相关数据源、确定适度的保存期限，并确认日志能够连同其语境一并恢复。

还应准备各类格式、应急凭据、供应商联系人、时间同步机制和保全程序。第一响应不应依赖临时上网查找如何封存设备，或查明谁管理某个账户。

- 资产和负责人清单保持更新。
- 日志来源、格式和保存期限。
- 技术、法律和供应商联系人及其代理人。
- 时区和时间同步情况有记录。
- 具备取证获取、封存和移交流程。
- 定期使用虚构证据开展演练。

4.2 不可逆节点

某些操作可能使后续分析无法进行：重置手机、重装系统、加密却不保存密钥、删除账户、任由日志滚动覆盖，或替换链接而不保存旧版本。遏制措施必须评估这些后果，不得凭本能执行。

如果为保护人员或业务连续性而必须采取不可逆操作，应记录由谁授权、为何必不可少、事先保全了哪些证据，以及丧失了哪些分析能力。良好意图无法恢复已删除的数据。

紧急决策	证据风险	建议事先采取的措施
关机或重启	内存和会话丢失。	评估现场取证获取并记录状态。
停用账户	无法访问日志或内容。	导出日志并要求供应商保全。
锁定设备	可能被远程加密或擦除。	确认密钥和获授权的访问方法。
更换服务器	日志被覆盖或丢失。	保全镜像、日志和配置。

4.3 记录在案的流程

整个流程包括授权、识别、初步保全、取证获取、保管、检查、分析、报告和保存。每个阶段都会形成供下一阶段使用的交付物。如果某一阶段缺少记录，下一阶段得到的就只是假设，而不是可验证的依据。

ISO/IEC 27037 为识别、收集、取证获取和保全提供指导；NIST SP 800-86 将流程组织为收集、检查、分析和报告。它们是方法参考，不是法律，也不保证有效性。本手册将其转化为易懂的操作和可证明工作过程的格式。[4][5]

[4] ISO/IEC 27037:2012。数字证据识别、收集、取证获取和保全指南。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

第5章 不同情景下的决策树

根据状态、目标和风险选择路径，而不是凭习惯。

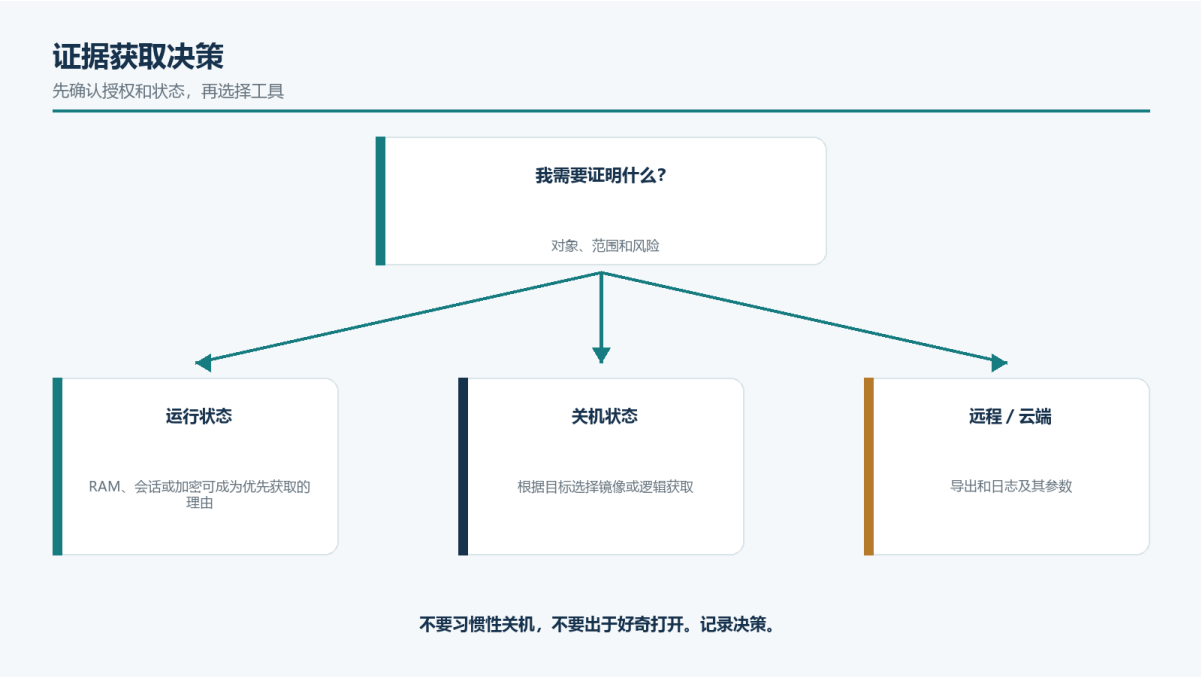


图5 根据状态、目标和风险选择路径，而不是凭习惯。

5.1 设备开机或关机

开机设备可能包含易失性内存、会话、密钥、连接和进程，这些信息在关机后会消失。设备在观察期间也可能继续修改数据。关机设备可能更稳定，适合制作镜像，但加密和休眠状态会改变可选方案。应根据待答问题和可用能力作出决定。

不能按统一规则一律关机，也不能因焦虑而一直保持开机。应记录设备状态、可见活动、已知加密情况、连接、授权和内存获取必要性。如果没有能力安全地进行现场取证获取，应先记录并请求支持，再改变设备状态。

5.2 本地、远程或通过供应商取证获取

本地取证获取可以观察设备及其语境，但并不总是最佳数据来源。管理性导出可能保留设备未存储或已在本地删除的事件。远程取证获取必须记录执行人身份、参数、日期、时区、格式和传输渠道。

应向供应商请求适当的数据源，而不是“全部信息”。申请应界定时间段、账户、字段、格式、各列含义和生成过程。如果使用官方门户，应记录由谁使用、以何种角色登录以及应用了哪些筛选条件。如果供应商交付文件却未说明其生成方式，应书面记录这一局限。

5.3 移动设备与隔离

对于手机，应评估开机状态、锁定、加密、网络、同步、远程擦除和电池情况。隔离可以防止远程改动，但也可能阻碍合法取证获取或触发锁定。取出电池并非通用指令，而且许多设备在不造成损坏或改动的情况下无法拆卸电池。

隔离措施必须真实有效并经过验证。防静电袋不等于法拉第笼。应记录所用技术、验证方式、仍处于活动状态的连接以及已接受的风险。如果不具备安全决策条件，应保持现状并上报处理。

5.4 何时停止

停止操作同样是一项专业决定。缺乏授权、危及人员、无法保全、缺少经过验证的工具或存在破坏证据的危险时，都必须暂停并上报。为了“看看能否发现什么”而继续操作，造成的损害可能大于获得的信息。

停止记录应包括原因、对象最终状态、此前实施的操作、已识别的风险和后续负责人。这不应被视为失败，而是保留分析可能性、避免采取无法辩护行动的措施。

> **安全规则**
>
> 不得在个人设备或生产网络中运行未知样本。应在获得授权并明确目标后，于隔离环境中使用受控副本。好奇心不能成为使第三方暴露于风险的理由。

第6章 现代数据源与通话记录表

结合语境处理云服务、电子邮件、供应商、日志和合成内容。



图6 结合语境处理云服务、电子邮件、供应商、日志和合成内容。

6.1 云服务、SaaS 与导出文件

用户界面只是其中一个层面。平台还可能在其他层面保存版本历史、访问日志、角色、令牌、IP 地址、管理活动、共享链接、通知和备份。导出记录应注明由谁生成、使用何种角色、筛选条件、时区、格式、时间段和局限。

PDF 下载文件可能便于阅读，却不足以分析结构和元数据。如有原生格式，应一并索取字段文档和生成过程说明。如果平台提供 API，应记录端点、版本、参数、分页、限制和响应，但报告中不得包含秘密信息。

6.2 电子邮件与 EML

EML 保存邮件正文、附件和邮件头，截图无法完整汇集这些要素。当正文包含参考编号、字段说明或附件哈希值时，EML 尤其重要。它可以用于核查交付时作出了哪些声明，并将每个文件与相应声明关联起来。

应保存原始邮件，并记录其取得方式：客户端导出、服务器下载或他人交付。分别计算 EML 和附件的哈希值，并记录二者关系。EML 证明的是所收到邮件的内容，并不证明发件人的全部陈述属实，也不证明发件人的自然人身份。

> **不要混淆对象**
>
> EML 的哈希值不是附件的哈希值，附件的哈希值也不是生成数据的系统的哈希值。每个值对应不同对象，必须记录名称、算法、日期和相互关系。

6.3 通话记录表的申请与接收

通话记录表是电信记录的导出文件。解读时不能只看一张包含号码的表格，还需要了解时间段、时区、事件类型、方向、时长、标识符、基站小区、技术、空字段和提取方法。申请中应要求提供可用的原生格式、列说明以及生成该文件的系统证明。

供应商应在交付邮件正文中列明每个交付文件的哈希值及所用算法。该值可以验证收到的附件是否与供应商所指文件一致。此外，必须提交并保存包含该正文、邮件头和附件的 EML。仅将哈希值抄录到单独备注中，或只保存表格，都不够。

接收时，应验证正文中的值是否与附件匹配。匹配则记录；不匹配则记录差异并要求澄清，不得编辑文件。如果供应商未提供哈希值，应记录这一缺失，并在接收时计算一个哈希值，同时明确它只能证明自该时点起的完整性。任何哈希值本身都不能证明通话内容的真实性或电话使用人的身份。[6]

申请要素	向供应商请求什么	接收时检查什么
时间段与时区	开始、结束、时区和夏令时。	时间段内的事件和一致的转换。
格式与字段	可用的 CSV/XLSX/PDF、字段字典和提取过程。	原生文件、列、空值和单位。
完整性	邮件正文中每个文件的哈希值和算法。	本地计算结果，以及记录在案的一致或差异情况。

[6]墨西哥。适用于信贷机构的一般性规定，第 316 Bis 条及相关条款系列。 https://www.cnbv.gob.mx/Prensa/Presentaciones%20Seminario%20Corresponsales/i.%20Circular%20%C3%9Anica%20de%20Bancos.pdf

申请要素	向供应商请求什么	接收时检查什么
交付	包含正文、邮件头和附件的 EML。	完整的 EML 和相关文件，不得将各对象分开。
语境	网络类型、事件、漫游、基站小区和可用标识符。	每个字段能够推断什么、不能推断什么。

6.4 供应商申请正文示例

以下示例为虚构，可作调整，但不得通过普通渠道传输敏感数据。授权和案卷应通过相应的安全渠道发送。目的是使答复带有足够的语境以供分析，并使交付对象的完整性可以验证。

主题：EXP-DEMO-2026-001 · 申请记录及完整性证明

尊敬的保管团队：

通过已获授权的安全渠道，我申请 2026 年 11 月 1 日至 3 日的记录，并明确注明适用的时区和夏令时。请在可用时提供开始日期和时间、时长、事件类型、方向、线路和设备标识符、基站小区、技术，以及空字段说明。

请提供可用原生格式的文件（CSV 和/或 XLSX）、供查阅的 PDF 副本、字段字典，以及提取过程和提取日期说明。对于每个文件，请在答复正文中注明相应算法和哈希值。

交付时必须保留本邮件的 EML 格式，包括正文、邮件头和附件。任何格式、保存或覆盖范围方面的限制，都必须明确说明。

此致敬礼！
获授权的技术负责人 · EXP-DEMO-2026-001

6.5 虚拟化、物联网与合成内容

虚拟化环境中应区分宿主机、客户机、快照、共享存储和管理日志。物联网环境中应区分设备、应用程序、枢纽、云服务、固件和同步。数据出现在屏幕上，并不能说明它在哪里生成，也不能说明存在多少副本。取证获取必须指明所在层级，而不只是产品名称。

对于由人工智能生成或篡改的内容，应区分生成、编辑、转换和发布。在可用时，应保存原始材料、历史记录、工具和版本，以及授权和人工复核记录。检测器只能提供线索，不能给出定论。法律分析应审查同意、身份、行为、用途和现行有效性，不能把“人工智能”当作普遍适用的刑事类别。[7]

[7] （UE）2024/1689 号《人工智能条例》，第 50 条，截至 27-07-2026 的合并文本。https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/spa/pdf

6.6 法规与现行效力：不得仅凭孤立示例

墨西哥《联邦刑法典》第 199 Octies 和 199 Nonies 条规定了某些涉及未经同意的私密性内容的行为，包括材料与所识别人员并不对应的情形。欧洲《人工智能条例》第 50 条涉及深度伪造的透明度，并对创意作品和编辑审查的某些义务作出调整。这些制度不同，不得混同为某种所谓的全球人工智能禁令。

圣路易斯波托西州说明了为何要核实现行效力：2025 年 11 月通过的改革增加了有关人工智能的具体罪名，但第 187 Ter、272 Bis 和 272 Ter 条已于 2026 年 7 月 30 日被废止。该例仅是地方先例，不是普遍规则，也不是一般授权。必须依据现行规范和其他可能适用的罪名分析相关行为。[8][9][10]

[8]《联邦刑法典》，第 199 Octies 和 199 Nonies 条，汇编包含 13-03-2026 的修订。https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

[9]圣路易斯波托西州议会。批准关于不当使用人工智能的改革，14-11-2025。https://congresosanluis.gob.mx/content/aprobada-reforma-para-sancionar-uso-indebido-de-inteligencia-artificial

[10]《圣路易斯波托西州议会公报》。废止第 187 Ter 条以及包含第 272 Bis 和 272 Ter 条的章节，发布于 30-07-2026。http://congresosanluis.gob.mx/sites/default/files/unpload/tl/gpar/2026/07/%C3%9ANICO.pdf

第7章 接收与初步保全

在任何分析之前，先记录对象及其状态。

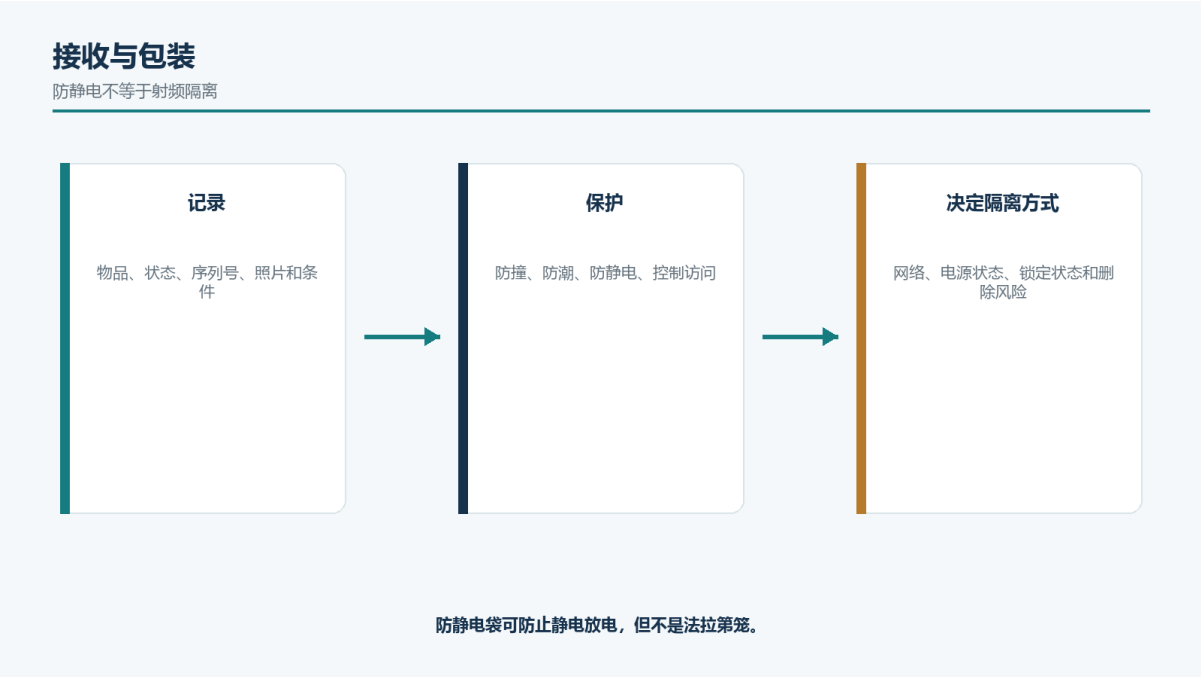


图7 在任何分析之前，先记录对象及其状态。

7.1 清晰易懂的接收记录

接收记录应说明收到了什么、如何送达、由谁交付、由谁接收、何时、何地以及处于何种状态。记录包括可用标识符、配件、封条、照片和备注。不能只写“一台计算机”或“一个 USB”：还应记录品牌、型号、序列号（如有）、容量、物理状态和任何既有标签。

第一响应人员无需掌握取证获取技术也能做好接收工作。其应避免未经授权开机、查看或连接，拍摄状态照片、记录可见信息并请求支持。如果有人已经打开过文件，也必须记录；不得为了使接收记录看似完美而隐瞒。

- 案件和对象的唯一标识符。
- 日期、时间、时区、地点、交付和接收。
- 物理描述、序列号、容量和配件。
- 开机、锁定、网络状态和可见损坏。
- 整体照片和标识符照片。
- 已知的先前操作和即时风险。

7.2 包装与封存

包装用于防止物理损坏、静电、潮湿、未经授权的访问和替换，应根据对象及其状态选择。封条应包括标识符、日期、负责人和有助于发现拆封的条件。如果工作需要拆封，应记录并按程序重新封存，同时保留历史记录。

防静电与射频隔离并不等同。前者保护组件免受放电影响，后者旨在阻止无线通信且必须验证。正确的包装无法弥补此前的错误决定，但可以防止新的改动，并有助于还原谁曾接触过该对象。

7.3 标签与对象关系

每个对象都应使用稳定且不含客户名称的标识符。派生对象通过来源字段与原始对象关联。不同的导出文件不得重复使用同一标识符，而应创建具有自身日期、方法和哈希值的关联对象。这样可以避免仅因文件同名就进行比较。

一种可行的命名规则是 ED-AAAAMMDD-CASO-FUENTE-SECUENCIA-VERSION。如果组织已有其他规则，只要唯一且一致，就可以继续沿用。物理标签和接收记录必须与数字清单及最终报告一致。

```
虚构示例：
ED-20261109-DEMO-MBL-003-A00

ED = 数字证据
20261109 = 接收日期
DEMO = 虚构案件
MBL = 移动数据源
003 = 第三个对象
A00 = 初始取证获取
```

7.4 文件和消息的接收

数字接收应记录来源、渠道、日期、自称的发件人、收件人、名称、大小和格式。文件应原样保存，并在到达时计算哈希值。如果供应商在正文中提供哈希值，应进行核验并保存 EML。如果通过链接接收，应记录打开人、权限、下载日期和版本。

保全前，绝不能为了“整理”而修改原始文件名。原始文件与工作副本的关系应记录在清单文件中。如果文件此前已被他人重命名或转换，应记录这段历史，并保存所有可用版本。

第8章 取证获取与技术记录

以规范方法、验证和可追溯性获取数据。

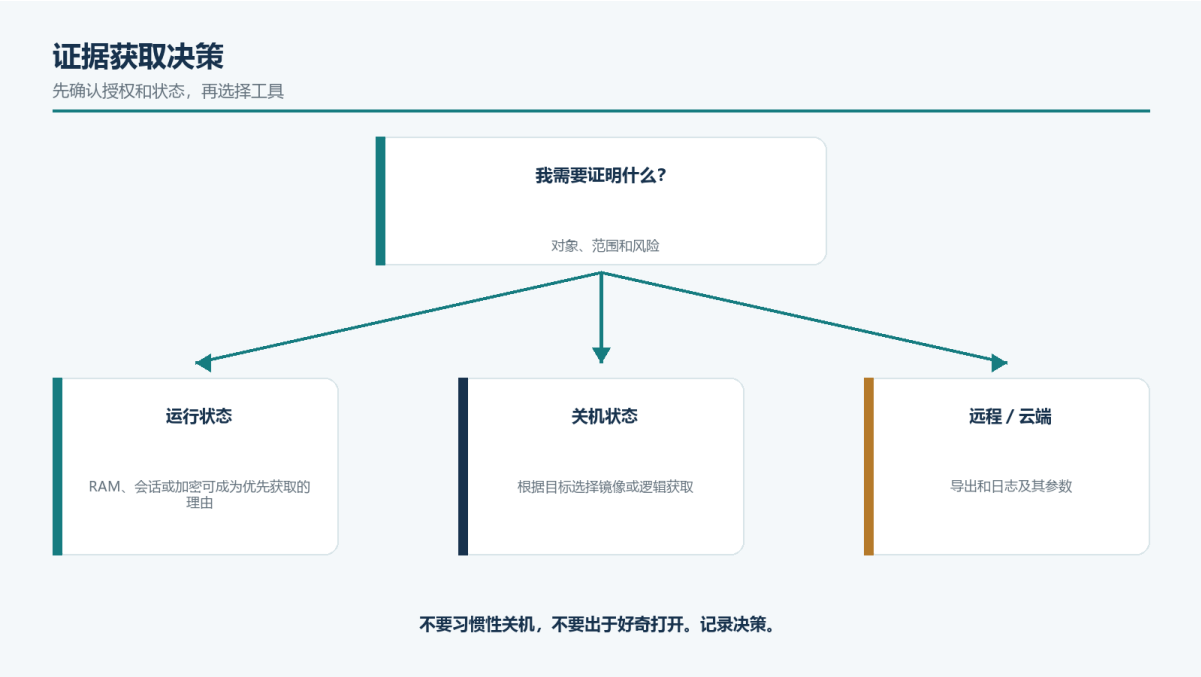


图8 以规范方法、验证和可追溯性获取数据。

8.1 物理、逻辑、易失性与文档化获取

物理取证获取复制整个介质，可以包括未分配空间；逻辑取证获取取得选定的文件或数据源。易失性获取在有正当理由时收集内存和临时状态。文档化获取在其他方式不可用时记录可视化内容，但不得将其表述为保留了原始材料的全部属性。

选择取决于待答问题，而不是工具的声望。重建已删除活动可能需要镜像；获取平台记录可能只需官方导出文件。方法说明应包括先决条件、授权、工具、版本、参数、输出和错误。

8.2 工具与验证

工具必须为了解并针对预期用途经过验证。应记录名称、版本、环境、配置和测试结果。更新可能改变格式或行为，不得未经核实就照搬旧命令。验证应使用虚构数据，证明输出能够打开并可与预期对象关联。

写保护器和其他保护措施应在适用时使用，但不能将其视为绝对保证。应记录实际流程：设备、连接、状态、错误和验证。工具出现异常时，应保存相关信息并评估其影响，而不是隐瞒。

取证获取字段	虚构示例	证明内容
数据源	磁盘 DEMO-SSD-003	具体对象和保管人。
方法	在受控副本上制作逐位镜像	覆盖类型。
工具	经实验室验证的名称和版本	执行条件。
日期与时区	2026-11-09T14:32:07-06:00	时间顺序。
完整性	所获对象的 SHA-256	该值所对应的对象。
异常情况	记录在案的不可读扇区	结果的范围和局限。

8.3 可复现的导出与查询

查询必须能够使用相同参数重复执行。应记录系统、账户、角色、筛选条件、时区、格式、字段、日期、操作员和结果。如果平台更改界面，应保存所用路径的版本或证据。截图可以展示配置，但不能替代原生输出。

查询返回零条记录时，必须先检查筛选条件、覆盖范围、时区、保存期限和错误，不能据此断定不存在。报告应说明查询内容和获得的响应。这种有记录的未发现结果比绝对断言更具可辩护性。

8.4 错误与异常

异常情况不得从案卷中删除：不可读扇区、损坏文件、缺失密码、网络中断、哈希差异和供应商变更都应记录。应评估其是否影响覆盖范围、真实性或分析，并在可能时要求再次交付。

如果需要重复取证获取，应使用不同标识符保留两个对象并说明原因。不得为了避免难堪的解释而删除第一个文件。可追溯性也包括出错决策及其纠正过程。

第9章 保管、移交与保存

保持对象、负责人、位置和验证之间的对应关系。



图9 保持对象、负责人、位置和验证之间的对应关系。

9.1 能回答问题的保管链

保管链可以说明存在过什么对象、位于何处、谁可以访问、为何移动以及如何验证。它不是一份没有标识符的签名清单。每次移交都包括对象、交付人、接收人、日期、时区、目的、封条状态，以及适用时的完整性验证。

保管链还应记录未发生物理移交的合法访问：打开容器、制作工作副本、临时借用、变更位置或远程下载。只记录最终交付会留下缺口，使历史无法还原。

9.2 电子移交

通过链接移交需要记录接收方、权限、渠道、日期、版本和下载验证。加密可以保护内容，但密钥管理必须通过单独渠道进行，且不得在记录中包含秘密信息。接收方应先确认对象和哈希值，再继续操作。

如果供应商在邮件正文中提供哈希值，应保存完整的 EML 和附件。正文将声明与交付关联起来，收到的文件则在本地验证。如果供应商更改文件，必须形成新的交付和新的哈希值，不得悄然替换先前文件。

9.3 存储与后续访问

应按照政策分别保存受保护的原始材料和工作副本。备份应加密、验证并测试恢复。无人能打开的备份不是有效的保存。迁移到其他格式必须记录，且不得删除原始材料。

法定保存、企业政策和证据保存的目的和期限并不相同，不能采用统一数字。应依据规范、案件和需要确定，并限制访问、记录查询。保存还包括未来可读性、格式文档和可用密钥。

第10章 检查、分析与假设

将数字痕迹转化为有依据的解释，避免凭空跳跃。

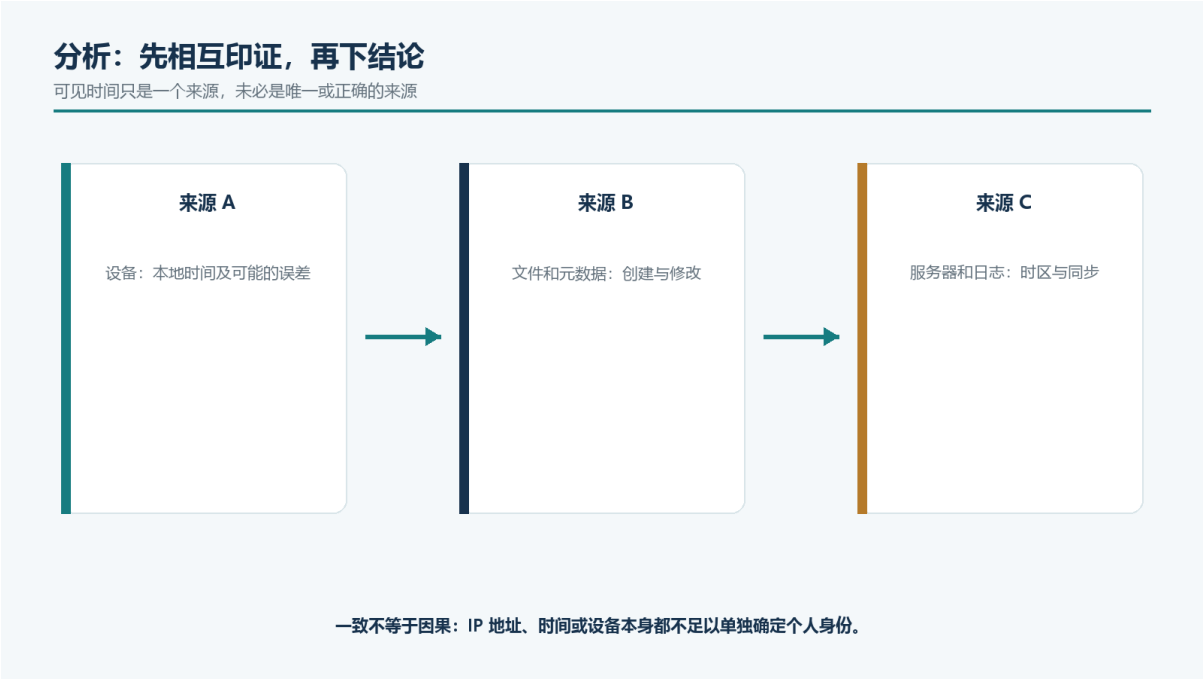


图10 将数字痕迹转化为有依据的解释，避免凭空跳跃。

10.1 问题先于工具

分析始于可以被证实或削弱的陈述，并将每项陈述与数据源和证据关联。目标不是找到一处匹配就停止，而是还要寻找其他解释以及可能推翻最初说法的结果。

假设矩阵记录陈述、数据源、方法、发现、其他解释和局限。这种做法可以减少凭直觉挑选数字痕迹的风险，并说明结论为何改变。某个数据源中缺少证据可能很重要，但必须结合其覆盖范围解读。

陈述	数据源与证据	其他解释	限定性结果
该视频是一段连续录制的影像。	名称、日期、章节和连续性。	事后选择或转换。	在已检查的范围内，该序列无法支持连续性的结论。
该操作源自持有人的设备。	访问日志、设备和会话记录。	他人使用的凭据。	证明的是凭据被使用，而不是自然人的身份。
未发生数据外泄。	网络日志和传输记录。	覆盖范围不完整或渠道加密。	在已审查的数据源中未观察到。

10.2 时间线与时区

时间线应记录日期、时区、时间来源和精度。设备时钟可能配置错误；文件时间可能表示创建、修改或下载；服务器时间可能采用另一时区。应同时保留原始值和转换值，不得将它们混作同一事件。

在某些相机中，文件名序列可以帮助判断章节和连续性，但其本身不能证明视频完整。应比较命名规则、日期、结构、内容和来源。缺少某个章节是一个待查问题，不能据此自动认定存在恶意剪辑。

10.3 通话记录表与日志的解读

通话记录表中应检查事件类型、开始时间、时长、方向、参与者、基站小区和空字段。呼入与呼出并不相同，事件期间使用的小区也可能变化。技术标识符不能自动等同于个人。解读时应比较时间段和语境，而不只是号码匹配。

基站小区的位置不能证明个人的确切位置，还需要覆盖范围、技术、时间和其他数据源的文档。如果断言行动轨迹，应说明精度级别和其他可能解释。分析不得把一张美观的地图变成并不存在的确定性。

10.4 可重复性与可复现性

可重复性是在同一环境中获得相同结果；可复现性则是在另一个有记录的环境中获得相同结果。ISO/IEC 27037 区分这两种属性。报告应说明哪些条件可能变化：工具、版本、系统、筛选条件或数据源。不同工具结果一致，也不能排除共同假设的影响。

分析应记录肯定、否定和无法定论的结果。对于依赖供应商或易失性数据源的结果，不得承诺可以重复。应保存相关查询和输出，使他人能够核查推理并指出错误。[4]

第11章 报告、出示与质证

清晰说明工作过程，不夸大确定性。



图11 清晰说明工作过程，不夸大确定性。

11.1 报告结构

报告以委托和范围开篇，识别数据源和对象，说明方法、呈现发现、分析其他解释，在范围内作出结论并声明局限。附录包括记录、清单文件、哈希值、日志和图示。结论应回答问题，不得加入新的指控或未经请求的法律建议。

写作应区分观察到的事实、工具输出、推论和法律评价。读者必须知道每项陈述的来源。图示用于概括事件序列或矛盾，而不是让报告显得比实际更具技术性。

- 委托、范围和排除事项。
- 对象、来源和保管情况。
- 工具、版本和参数。
- 发现及其可验证的位置。
- 其他假设和未发现结果。
- 结论、局限和完整附录。

11.2 面向非技术读者的语言

技术说明可以既准确又易懂。与其写“已实施证据取证获取”，不如写“已创建磁盘的受控副本并记录其完整性”。必要术语定义一次后应始终一致使用，缩写不能代替解释。

执行摘要应概括审查内容、发现以及可以作出的决定。技术细节应可供查阅，但不应要求管理层自行解读。警务人员和律师无需了解命令也能跟上事件顺序，专业人员则应能借助附录重复该过程。

11.3 引文与法律规范

引文应包括法律文件、条文、功能、版本和官方来源。不得仅因名称相似而引用某项法律，也不得把提案当作已颁布法令。比较等效仅限于功能和范围，不意味着程序效力相同。规范已被废止时，应将其作为历史先例说明，而不是现行规则。

复核应确认技术陈述和引文指向同一事项。有关凭证的规则不能证明全部作者身份；保存规则不能证明内容真实性；事件规范不能证明某次具体传输。不得用来源装饰事先已有的结论。

11.4 质证复核

交付前，应检查他人能否定位对象、重复查询、理解推理过程并找到局限。困难问题应依靠案卷回答，而不是依靠个人权威。如果某事项没有记录，应予承认并修正结论范围。

复核包括交付文件的标题、正文、附录、图像和元数据。未打开最终结果，不得声称已完成视觉验证。应计算交付文件的 SHA-256 并保存清单文件，以便来源方和接收方比较，同时不得将其与内容真实性的证明混为一谈。

第12章 常见错误与持续改进

避免已知错误，持续更新但不编造确定性。



图12 避免已知错误，持续更新但不编造确定性。

12.1 会改变案件的错误

代价最高的错误往往很简单：出于好奇打开、按习惯关机、截图不记 URL、导出不记时区、混淆原始材料与打印件、把 IP 地址归于个人、把哈希值当作全部证据，以及引用已废止的规范。预防始于清晰的程序和受过训练的第一响应人员。

错误已经发生时，应如实记录，不得编造完美的保管链。应评估发生了什么变化、哪些内容仍可验证，以及哪些结论必须加以限制。重写先前记录以掩盖错误会破坏可信度，对案卷的影响可能比原错误更严重。

错误	后果	正确应对
一律关机	内存或会话丢失。	决定前先评估状态。
把防静电包装当作法拉第笼	造成隔离有效的假象。	使用并验证真正有效的隔离措施。
将哈希值抄录到单独备注中	失去与交付记录的关联。	保存 EML、正文和附件。

错误	后果	正确应对
依赖人工智能检测器	对来源或虚假性作出错误结论。	结合来源、方法和语境进行印证。
引用旧修订案	声称适用一项并不存在的规范。	核实现行效力和废止情况。

12.2 经验教训

事后复核应识别数据源、决策、工具、沟通和展示中的问题。改进措施应分配给负责人，并通过演练验证。不得编造此前已合规的证据，而应记录新做法的生效时间。

手册新版本应保留变更历史和变更原因。平台修改导出方式时，应更新第 6 或 8 章；法律变更时，应更新附录 A 和记录 M。不得只堆积相互矛盾的备注而不修订正文。

12.3 整个组织的最低指南

组织必须能够在不依赖单一个人的情况下回答五个问题：谁授权、证据在哪里、如何取得、谁接触过，以及可以作出什么断言。如果其中任何一项没有答案，计划应说明如何补足信息或如何限制结论。

本手册是起点，不是一成不变的文稿。实践应根据案件调整、记录并复核。目标是让任何团队都能有序工作、共享知识并支撑其解释，即使结果并非预期。

附录A 简明功能法律矩阵

定位法律功能，不虚构各国制度之间的等同关系。

A.1 如何阅读比较表

“可比”是指功能等效，而不是内容、推定、主体、期限或程序效力完全相同。完整矩阵作为独立文件交付，以便无需重做手册即可更新。适用某项规则前，应核实法律文件、条文、主体范围、渠道、事项和事实发生时的版本。

该表汇总的是起始法律文件，不是详尽无遗的目录。如果调查未能证实某项功能，应如实标记，不得通过类比填补。民事、刑事、行政、档案和金融规则不能相互替代。[121112131415166]

法域	起始功能依据	主要警示
墨西哥	CCom 89–94 和 1205；CNPCF 348–350；NOM-151；CNBV 316 Bis 及相关条款系列。	逐步过渡；每项 CNBV 条文的对象和期限各不相同。
秘鲁	第 27269 号法律及其条例；CPC 188–197；档案制度；SBS 504-2021 和 2286-2024。	相关制度分散在不同规范中，不得将所有内容都归于第 27269 号法律。
智利	第 19.799 号法律；RAN 20-7、20-8 和 20-10。	高级电子签名和日期并非同一问题。
阿根廷	第 25.506 号法律；CCyC 318–319；BCRA A 7783 和 A 8280。	推定仅适用于相应制度；应核查废止规定。
哥伦比亚	第 527 号法律；CPACA；适用的 SFC 指令。	保存来源、目的地、日期和时间；确认 SFC 的具体条款编号。

[11]秘鲁。第 27269 号法律及《数字签名和证书条例》。https://www.gob.pe/institucion/indecopi/normas-legales/5570542-ley-27269

[12]智利。关于电子文件和电子签名的第 19.799 号法律。https://www.bcn.cl/leychile/navegar?idNorma=196640

[13]阿根廷。第 25.506 号《数字签名法》。https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

[14]哥伦比亚。1999 年关于数据电文和电子商务的第 527 号法律。https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

[15]厄瓜多尔。《电子商务、电子签名和数据电文法》。https://ventas.icert.fje.gob.ec/documents/10181/11670/leyComercioElectronico.pdf/e0a3116a-acd9-42ce-97ac-4d28b32a2f2e

[16]西班牙。《民事诉讼法》，第 326 和 384 条，合并文本。https://www.boe.es/buscar/act.php?id=BOE-A-2000-323

法域	起始功能依据	主要警示
厄瓜多尔	第 67 号法律；关于支付的 JPRM-2025-006-M 号决议。	支付系统并未复制 CNBV 的全部制度。
西班牙 / 欧盟	eIDAS；LEC 326 和 384；RD-ley 19/2018，第 45、66 和 67 条。	简单、高级和合格电子签名的效力并不相同。

A.2 更新方法

更新时应记录官方来源、查询日期、所读条文和操作变化。不得以新闻替代规范，也不得以提案替代法令。完整矩阵保留有关认可、书面形式、归属、完整性、原件、可访问性、保存、可采性、举证责任和金融监管的引文。

ISO/IEC 27037 和 NIST SP 800-86 作为方法参考引用，而不是国家法律。本附录用于指导保全、申请、验证和限制，不能用一张相似措辞对照表来解决案卷。[45]

附录B 范围与授权表

用于界定工作的初始表单。

B.1 格式

应在行动前填写。如果某项数据不可用，应写明原因和负责确认的人。不得将关键空项留到取证获取后再补填。

字段	记录内容	虚构示例
标识符	委托的唯一编号。	EXP-DEMO-2026-001
问题	需要证明的事实。	确定销售是否已传输并结算。
时间段	开始、结束和时区。	2026 年 11 月 1–3 日，UTC−06:00。
纳入的数据源	经授权的系统、文件和保管人。	汇款批次文件、支付处理方和银行报告。
排除事项	委托范围之外的数据或设备。	无关的个人设备。
授权	授权人、允许的操作和渠道。	获授权的管理部门；已登记的安全渠道。
交付物	报告类型和附录。	技术报告、清单文件和各类记录。
风险	改动、丢失和保密。	日志滚动覆盖和第三方数据。

附录C 接收记录

在任何分析之前记录状态。

C.1 最低数据要求

接收记录应附整体照片和标识符照片。即使先前操作有误，也必须记录；不得事后改写，以营造理想接收的假象。

字段	必需内容
对象和标识符	类型、品牌、型号、序列号、容量和分配的编号。
交付与接收	姓名、职能、日期、时间、时区和地点。
状态	开机、锁定、网络、损坏和配件。
封条与包装	类型、标识符、状态和照片。
先前操作	打开、连接、复制、变更或情况不明。
风险	易失性、远程擦除、第三方数据和优先级。
初始决策	保全、上报、取证获取或请求澄清，并注明负责人。

附录D 取证获取记录

关联数据源、方法、输出和验证。

D.1 按对象记录

每次取证获取都应有独立记录。如果重复获取，应分配一个新的关联标识符并说明原因，不得删除首次尝试的记录。

字段	必需内容
数据源和保管人	准确标识符和保管人。
方法与理由	物理、逻辑、易失性、远程或文档化获取及其理由。
工具	名称、版本、环境和验证。
参数	筛选条件、字段、日期、时区和配置。
输出	名称、路径、格式、大小和原始材料/副本关系。
完整性	算法、值、日期和覆盖的对象。
异常情况	错误、遗漏、扇区、访问及其对范围的影响。
验证	打开、比较、重复和复核人。

附录E 保管链与移交

还原每次访问和移动。

E.1 按事件记录

还应记录打开容器、远程下载和制作工作副本。只有确认接收及对象状态后，移交才算完成。

日期与时区	对象	交付人	接收人	目的	封条/完整性
11 月 09 日 14:32 −06	ED-DEMO-003	保管人 A	分析师 B	取证获取	01 号封条完好
11 月 09 日 16:05 −06	ED-DEMO-003-A00	分析师 B	保管人 C	保管	哈希值一致
11 月 10 日 09:10 −06	ED-DEMO-003-A01	保管人 C	复核人 D	复核	访问已登记

附录F 供应商申请与 EML 交付

确保远程记录的格式、语境和完整性。

F.1 申请字段

申请应根据供应商和获授权的渠道调整。密码或凭据不得写入记录或正文。安全渠道应通过引用标识，不得写入秘密信息。

要素	必须载明的内容
案卷与授权	编号、授权人和安全渠道引用。
账户与范围	经授权的标识符、时间段、时区和排除事项。
格式	可用的原生格式和查阅副本、字段字典及提取过程。
完整性	答复正文中每个文件的算法和哈希值。
交付	包含正文、邮件头和附件的 EML；适用时提供链接和权限。
局限	保存期限、缺失字段、覆盖范围、错误和说明。

F.2 接收时验证

处理附件前先保存 EML。分别计算 EML 和各文件的哈希值，并与正文中的值比较。差异应记录并请求澄清。供应商未提供哈希值时，应予注明并在本地计算，但不得将该值归于供应商。

6. 完整保存且可读取的 EML。
7. 收到原生文件，并与正文关联。
8. 算法和值均已比较并记录。
9. 理解字段、单位、时区和提取过程。
10. 局限和差异均有记录。

附录G 文件清单与清单文件

保持来源、派生对象和交付物之间的关系。

G.1 清单文件列

清单文件汇集标识符、名称、路径、对象类型、来源、方法、大小、格式、哈希值和备注，不得公开敏感数据或秘密信息。如果路径会泄露受保护信息，公开版本可以将其缩写。

标识符	关系	文件	格式	完整性
ED-DEMO-003	收到的原始文件	sabanas.csv	CSV	接收时计算的 SHA-256
ED-DEMO-003-A00	相关交付	entrega.eml	EML	独立于 CSV 的对象
ED-DEMO-003-A01	工作副本	sabanas_trabajo.csv	CSV	结构变化时哈希值不同
ED-DEMO-003-R01	展示	informe.pdf	PDF	交付文件的哈希值

附录H 时间线与时区

避免隐蔽转换和错误匹配。

H.1 对应关系表

应保留每个数据源的原始时间值，并添加转换值而不替换原值。如果设备时间不可靠，应注明已知偏差或不确定性。

事件	时间来源	原始值	时区	转换与局限
视频拍摄	设备时钟	06:04:16	未知	不得假定为 UTC；应与其他数据源比较。
导出	服务器	2026-11-01T12:04:16Z	UTC	UTC−06 时为 06:04:16；记录夏令时。
EML 接收	电子邮件客户端	11 月 09 日 07:05	UTC−06	这是接收时间，不是被调查事件的发生时间。

附录I 假设与分析矩阵

记录确认、其他解释和局限。

I.1 推理模板

每项陈述都应接受能够证实或削弱它的数据源检验。复核人应补充分析师未考虑的其他解释，并记录结论如何变化。

陈述	数据源/证据	其他解释	结果
该文件是原始文件。	来源、元数据和保管。	先前导出或编辑。	仅能证明所收到的表现形式。
用户授权了该操作。	身份验证、设备和会话。	凭据已泄露。	使用凭据不等于证明自然人身份。
不存在其他文件。	查询和覆盖范围有记录。	筛选条件、保存期限或格式。	在所查询的范围内未观察到其他文件。

附录J 合成内容审查

区分生成、编辑、转换和发布。

J.1 最低案卷要求

目标不是凭外观就断言为“deepfake”。应记录每次已知的转换、相应证据及其局限。检测器应注明版本和已知错误率（如可获得），不得将其作为唯一证据。

11. 收到的原始文件及来源。
12. 可用的工具、版本和生成/编辑历史。
13. 编解码器、压缩、元数据和版本比较。
14. URL、发布页面、标签、受众和语境。
15. 同意、身份、目的和现行规范已审查。
16. 检测器和印证手段均有明确局限。

附录K 技术报告模板

呈现发现，不混淆事实和推论。

K.1 写作结构

最终报告包括封面、委托标识、目录、执行摘要、范围、数据源、方法、发现、分析、结论、局限和附录。每项陈述都有对应的证据位置，措辞与其证明力度相称。

部分	应回答的内容
委托	请求了什么、目的何在、排除哪些内容。
数据源	收到了什么、由谁交付、以何种表现形式。
方法	实施了什么操作、使用什么工具和参数。
发现	观察到了什么，以及可以在何处定位。
分析	哪些解释得到支持或被削弱。
结论	在范围内可以作出什么断言。
局限	哪些事项未得到证明，以及缺少哪些数据源。
附录	记录、清单文件、哈希值、日志和图示。

附录L 核查清单

每次交付前检查工作。

L.1 接收与取证获取

清单应依据证据勾选，而不是依据意图。如果某项不适用，应写明理由及其批准情况。不得让关键标准得不到答复。

17. 授权、范围和排除事项有记录。

18. 对象、状态、照片和负责人均已识别。

19. 方法已由数据源和风险证明其合理性。

20. 工具、版本和参数已记录。

21. 哈希值、EML 和相关文件均已保全。

22. 异常情况和局限已纳入案卷。

L.2 报告与发布

最终复核应针对打开后的文件，而不是工作草稿。用于发布的图像，应同时检查完整尺寸和缩略图。

23. 结论与数据源和范围一致。

24. 引文、条文和功能均经核实现行有效。

25. 不含客户名称、凭据或不必要的数据。

26. 目录、图示、表格和附录清晰可读。

27. 最终文件已打开并完成视觉复核。

28. 来源和交付文件的 SHA-256 一致，清单文件已保存。

附录M 法律规范与手册版本控制

持续更新而不累积矛盾。

M.1 变更记录

每项法律或方法变更都应记录来源、日期、受影响章节、编辑决定和复核人。规范被废止时，应修改正文和常见问题，不能只在末尾添加备注。

日期	来源	变更	编辑处理	复核
2026 年 7 月 30 日	SLP 公报	第 187 Ter、272 Bis 和 272 Ter 条已废止。	作为历史先例说明；更新帖文和附录 A。	已完成
2026 年 7 月 27 日	EUR-Lex	已查阅《人工智能条例》的合并文本。	引用第 50 条，并准确说明适用范围和例外。	已完成
2026 年 11 月 09 日	手册	语言和格式复核。	纳入 EML、通话记录表和第一响应清单。	已完成

M.2 使用说明结语

本手册为通用指南，不构成法律意见，也不构成针对具体案件的专家鉴定意见。实际应用必须分析授权、法域、事实、渠道和现行规范。本版本随附资源和独立矩阵，以便在不损失本卷设计的情况下审查更新。