ACCCF

应用知识 · 西班牙语美洲

西班牙语数字证据手册 2026 V1

保护、验证并解释西班牙语世界的数字证据。



编写并签署

Jocsan Laguna Romero

ACCCF 主席

理事会机构版

目录

通用技术指南。不构成法律意见或专家鉴定意见。示例均为虚构或匿名化；图示为编辑重构。可见页码对应 PDF 版本。Word 打开文档时可能会更新此索引；标题保留内部导航。

手册前言 7

如何使用本手册 8

第1章 范围、问题与授权 9

1.1 统领工作的问题 9

1.2 授权先于访问 10

1.3 数据源初步清单 10

1.4 完整示例：销售款项争议 11

1.5 依据与结语：方法同样保护人员 12

第2章 完整性、原始材料与语境 14

2.1 原始材料不一定就是设备 14

2.2 完整性、真实性、归属与内容真实性 14

2.3 哈希是控制手段，而非教条 15

2.4 内部元数据与系统日期：避免错误的关键区分 16

2.5 照片与长椅案例 17

2.6 可访问性与语境保存 17

第3章 角色、职责与决策 19

3.1 职能先于职务 19

3.2 不凭临时应对的第一响应 19

3.3 操作沟通 20

3.4 独立性、隐私与第三方 21

3.5 角色三段论 21

第4章 生命周期与取证准备 23

4.1 接收案件前做好准备 23

4.2 不可逆节点 24

4.3 记录在案的流程与交付物 26
4.4 保存期限与纵向分析 27
4.5 作为社会责任的准备工作 27
第5章 不同情景下的决策树 28
5.1 设备开机或关机 28
5.2 本地、远程或通过供应商取证获取 29
5.3 移动设备与隔离 29
5.4 光盘：标识符与格式 30
5.5 何时停止 31
5.6 决策树是推理工具，不是装饰 32
第6章 现代数据源与通话记录表 34
6.1 云服务、SaaS 与导出文件 34
6.2 电子邮件与 EML 35
6.3 通话记录表的申请与接收 36
6.4 供应商申请正文示例 37
6.5 虚拟化、物联网与合成内容 37
6.6 现行效力：修订后被废止的示例 39
6.7 数据源并非只存在于一个位置 40
第7章 接收与初步保全 41
7.1 清晰易懂的接收记录 41
7.2 包装与封存 42
7.3 标签与对象关系 43
7.4 配件和连接也是接收的一部分 44
7.5 文件和消息的接收 45
第8章 取证获取与技术记录 47
8.1 物理、逻辑、易失性与文档化获取 47
8.2 实际连接：数据源、写保护器和工作站 48
8.3 介质和适配器：NVMe、SATA 与光盘 48
8.4 逻辑取证获取与清单文件 49

8.5 现场内存获取与工具验证 50
8.6 可复现的导出与查询 51
8.7 错误与异常 51
第9章 保管、移交与保存 53
9.1 能回答问题的保管链 53
9.2 电子移交与密钥 54
9.3 存储与后续访问 55
9.4 拆封与更换封条 55
9.5 访问、共同保管与冲突 56
第10章 检查、时间线与其他假设 58
10.1 检查不是寻找责任人 58
10.2 元数据：倾听文件，但不全盘相信 58
10.3 时间线：先校准时钟，再排列事件 60
10.4 天线、覆盖范围与方位角：地理分析不能走捷径 61
10.5 具有区分力的印证 63
10.6 假设矩阵：允许证据推翻假设 64
10.7 重复、复现与知道何时停止 65
第11章 报告、推理与质证 67
11.1 报告是返回数据源的路径 67
11.2 事实、结果、推论与意见 68
11.3 三段论与错误推论 68
11.4 解释矛盾，而不是掩盖矛盾 69
11.5 撰写证据能够承载的结论 70
11.6 质证与独立复核 70
11.7 交付、附录和后续访问 71
第12章 错误、学习与公共服务 73
12.1 不能通过改写过去来纠正错误 73
12.2 接收和保全中的错误 74
12.3 数据源、截图和导出错误 74

12.4 解读错误 75
12.5 法律和时效错误 76
12.6 改变程序的经验教训 77
12.7 最终衡量标准：避免下一次滥用 78
附录A 功能法律等效对照 79
执行摘要 79
1. 比较方法与局限 79
2. 按法律功能划分的核心矩阵 80
3. 墨西哥：法律基础与过渡 89
4. 秘鲁：分散制度与金融监管更新 91
5. 智利：签名、日期与安全监管 93
6. 阿根廷：有限推定与介质可靠性 94
7. 哥伦比亚：数据电文、保存与回执 95
8. 厄瓜多尔：文件等效与支付系统 96
9. 西班牙与欧盟：不歧视、信任服务与程序 97
10. 金融日志与事件的功能比较 98
11. 国际方法标准 102
12. 使用矩阵并避免虚假等效的规则 103
A.13 实际应用：先选择制度，再作结论 104
A.14 墨西哥调查期间的数据保护 105
附录B 范围与授权表 106
B.1 格式内容 106
附录C 接收与初步保全记录 108
C.1 物理接收记录示例 108
C.2 文件或消息的接收 109
附录D 取证获取记录 110
D.1 完整示例 110
附录E 保管链与移交 112

E.1 事件序列示例 112
E.2 电子移交 113
附录F 通过供应商申请与取证获取 114
F.1 申请模板 114
F.2 导出或 API 记录 114
附录G 对象清单与清单文件 116
G.1 清单文件示例 116
附录H 时间线与时区 118
H.1 时间线示例 118
H.2 矛盾日期处理规则 118
附录I 假设与印证矩阵 120
I.1 完整示例 120
附录J 合成内容审查 122
J.1 应用格式 122
附录K 报告结构和结论 123
K.1 建议顺序 123
K.2 完整结论示例 124
附录L 操作核查清单 125
L.1 接收与取证获取 125
L.2 分析、报告与交付 126
附录M 版本、来源和经验教训控制 127
M.1 法律和技术记录 127
M.2 将经验转化为改进 127

手册前言

保全数字证据，不是把文件存到看似足够为止，而是保护这样一种可能性：另一位人员采用不同判断和工具，也能得出与事实相符的结论。设备不能替代证人，截图不能替代文件，意见不能替代方法。工作早在打开其中任何一项之前就开始：先确定需要证明什么，以及采取行动会产生什么后果。

本手册源于一个令人不安却必须回答的问题：如果第一位接收证据的人把最简单的事情做好，可以避免多少滥用？识别对象、拍摄状态、界定授权、索取原生文件、保存完整消息、记录日期和时区、不把天线当成个人、不把直觉包装成科学。基础并非装饰，它能防止指控建立在推测之上，也能防止辩护因可避免的疏漏而崩溃。

统领其他工作的规则可以写成：数据源、授权、状态、方法、记录、验证和限定性结论。首先确定哪些内容能够提供信息，再核实谁可以授权访问及其条件。记录对象到达时的状态，选择适当方法并留下记录。只有此后才进行验证，并在数据源允许的范围内作出结论。如果某一环节出错，下一环节不能靠修辞弥补：必须承认局限，并确定可以补救什么，而不是编造完美历史。

这里的魔幻现实主义并非文学装饰，而是承认日常物品也能讲述非凡事实：长椅可以描述一次停留，中心环可以识别一张光盘，袋子可以造成隔离有效的假象，一个时钟可以与另一个时钟矛盾。类比是理解的桥梁，不能替代证据。严谨在于始终回到数据源，追问它究竟能证明什么，又有哪些只是看似暗示。

本书宗旨

提供基础，使任何人都不必通过挫折来学习数字证据。分享一套警务人员、鉴定人、律师、工程师和组织负责人均可使用的方法，同时不回避艰难决策和不确定领域。

示例均为虚构或匿名化。图像为编辑重构：展示设备和操作，不构成案件的真实证据。法律规范按功能、条文、适用范围和查询日期引用。国家之间的等效如果只是部分或限于特定行业，就会明确说明，因为相似措辞并不产生相同法律效力。

如何使用本手册

如果你是第一个接收案件的人，请从第 1、3、5 和 7 章开始。这里说明如何界定委托、分配职能、根据对象状态选择路径并规范记录接收。避免初期错误并不要求你成为分析师，但要求你知道应保全什么、何时请求帮助。

如果负责取证获取或分析，请使用第 4、6、8、9 和 10 章。技术部分说明如何选择数据源、记录获取、核验文件、构建时间线并评估其他假设。如果负责出示或复核，请使用第 2、11 和 12 章以及法律和操作附录。目标不是重复程序，而是理解每项决策为何会留下有用痕迹。

格式本身不是目的。一份名称漂亮却空泛的记录可能只是伪保管，正如一张没有 URL 的照片可能只是残缺图像。每种格式都应记录一项决策或核验：授权了什么、收到了什么、发生了什么变化、由谁验证、存在哪些局限。不能帮助回答这些问题的字段应当删除。

阅读应当循序渐进。概念反复出现，是因为每次都会增加一层含义：数据源可能在有限意义上属于原始材料，导出文件可能是比设备更好的数据源，天线描述的是覆盖范围而非精确位置，签名可以具有效力却不能证明哪只手点击了按钮。不要急于跳到命令；判断清晰之后，速度自然会提高。

第1章 范围、问题与授权

1.1 统领工作的问题

委托表述不清会导致调查无限扩张。“检查一切”没有说明需要证明什么、结果将用于何处，也没有说明可接受何种改动风险。相反，精确的问题可以决定需要哪些数据源、哪些不得触碰：哪些交易存在争议、发生在哪个时期、涉及哪些系统，以及会产生什么法律或企业后果。

应分别记录各方说法。一方声称已完成销售但未获付款，另一方则称未收到这些交易。不要把它们混成同一个故事。第一种假设不能成为只寻找支持证据的搜索指令，第二种假设也不能因令人不适而被排除。方法的作用是让两种假设都能接受检验，而不是帮助其中一种提前获胜。

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，要求并不相同。前者可能只需一个能够恢复工作的受控副本；后者则需要授权、完整性、语境、可追溯性、可复核性，以及不依赖签署人声望的解释。混淆这些目标会产生两类错误：为简单恢复做得过多，或为具有严重后果的主张做得过少。

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、事实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。
哪些内容可以排除在外？	被排除的数据、设备、账户或时间段。	减少不必要的暴露。

1.2 授权先于访问

能够打开文件，并不意味着有权检查文件。授权应载明授权人、允许的操作、系统、负责人、排除事项和沟通渠道。如果需要访问第三方信息、共享账户或供应商，应记录合法途径。技术能力不会产生授权，只能用于执行授权允许的事项。

比例原则要求审查数据源和方法是否为目标所必需。管理性导出可能比全面检查设备更能回答问题，同时减少改动和暴露。收集一切并不等于全面，可能只会带来噪声、数据暴露，并以看似周全的方式迷失问题。如果某个数据源区分能力更强且侵扰更小，就应作为初步候选。

保密应从接收时确定，而不是到报告结尾才考虑。必须明确谁可以查看、复制、传输和发布信息，尤其是涉及第三方、未成年人、受害人或商业秘密的数据。个人数据处理必须合法、限于已告知的目的并适合必要范围，安全和保密措施应与风险相称。新法律还要求立即报告重大数据泄露，使相关人员能够维护自身权益。[1]

行动规则

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

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。同时列出不可用项及原因：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。缺失同样会改变计划和可能结论。不完整的案卷不得伪装成完整全貌。

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及其能回答什么问题。奥卡姆剃刀原则要求从区分能力最强的数据源入手，而不是从最有技术声望的工具入手。

[1]《联邦私人持有个人数据保护法》，新法于 20-03-2025 发布，并于 14-11-2025 修订。第 5–9、18–20 和 31 条：原则、安全、保密、数据泄露和期限。官方在线来源

清单字段	有效记录示例	为何重要
标识符和保管人	商业汇款批次、支付处理方、银行和获授权的负责人。	避免向错误的保管人索取数据。
类型、时间段和格式	一周的交易、原生 CSV 和字段字典。	便于比较结构和含义。
可用性	文件缺失、链接有效或供应商待回复。	从一开始就声明局限。
风险	日志滚动覆盖、远程擦除、第三方信息暴露或物理丢失。	确定优先级和方法。
授权与联系方式	授权人、安全渠道和代理人。	避免可疑访问和无记录的延误。

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。问题不是“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。每个数据源分别回答事件序列中的不同部分。

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。可能是交易不存在、汇款批次不完整、使用了其他渠道，或导出存在缺陷。负责任的结论应从数据源中记录到的缺失开始，而不是直接指控现成的第一个嫌疑人。



图1 行动前界定数据源：哪些可以检查、哪些排除在外。编辑重构；不构成真实证据。

该示例的启示

界定清楚的问题可以避免对个人设备进行侵扰性检查，并要求比较相互独立的数据源。

证据不是越多越好，而应根据其解决某项主张的能力来选择。

1.5 依据与结语：方法同样保护人员

识别、收集、取证获取和保全不只是技术操作。ISO/IEC 27037 将其表述为必须记录在案、以便事后复核的决策。数据源和授权决定方法；不能仅因某人掌握密码或手持设备，就认为访问合法。这一顺序还能防止调查给受影响人员造成二次伤害。[2]

在墨西哥，电子信息在证明方法可靠性、归属、可访问性和完整性后，可以被采纳为证据。孤立截图或鉴定人声称曾在屏幕上看到某内容，并不能满足这一要求。必须能够说明信息如何生

[2]ISO/IEC 27037:2012。数字证据识别、收集、取证获取和保全指南。该版本经 ISO 确认现行有效。官方在线来源

成、传输、接收或归档，以及自生成以来如何保持完整。准确界定这些事项，才能确定此后可以作出什么断言。[34]

限定性结论

接触证据之前，必须能够回答：正在调查哪项主张、由谁授权、哪些数据源区分能力最强、哪些排除措施可以保护第三方，以及预期结果是什么。如果缺少任何答案，第一项交付物就不应是取证获取，而应是一份记录在案的澄清。

[3]《联邦民事诉讼法典》第 210-A 条：电子信息方法的可靠性、归属、可访问性和完整性。该法典由 07-06-2023 的法令废止，适用渐进过渡制度。官方在线来源

[4]墨西哥《商法典》第 89–94 和 1205 条：中立性、归属、书面形式、原件、完整性、可访问性和数据电文采纳。官方汇编。官方在线来源

第2章 完整性、原始材料与语境

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及保留或丢失的信息，每种形式都可能有用途。问题不只是“我是否持有该对象”，而是“我能用这种表现形式证明什么”。

介质的逐位镜像可以保留已分配和未分配扇区；逻辑导出可能只保留某些文件；截图可以展示画面却不保留结构或元数据；打印件可以使内容易读，却不提供原始文件。没有哪种形式绝对优于其他形式。选择取决于问题和复核需要。不得为了制作一种后来发现并不充分的表现形式而破坏源对象。

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。[56]

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。

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。即使密码学序列正确，也可能需要解释当时谁控制密钥和设备。

[5]墨西哥《商法典》第 89–94 和 1205 条：中立性、归属、书面形式、原件、完整性、可访问性和数据电文采纳。官方汇编。官方在线来源

[6]《国家民事和家庭诉讼法典》第 348–350 条。汇编包含 15-01-2026 的修订。逐步适用，并取决于相关宣告。官方在线来源

稳妥表述	所需证据	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。刚刚计算的哈希值只能证明自计算之时起的完整性。

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。”



图2 哈希用于比较对象，不能证明作者身份或内容真实性。编辑重构；不构成真实证据。

2.4 内部元数据与系统日期：避免错误的关键区分

操作系统显示的属性可能反映文件何时被复制、下载或修改到该计算机，而不一定是文件的原始创建时间。这些日期并非无用：它们有助于还原该对象在该系统中的历史。错误在于未经其他核验，就将其当作原始拍摄或创建日期。必须明确每个字段的含义、所在系统及其用于支持哪项主张。

照片的内部元数据可能包括拍摄日期、设备型号，以及定位功能启用时记录的坐标。ExifTool 等工具可以读取这些信息，但它们并非不可改变，也不能单独证明场景确如描述。文件可能被编辑，元数据可能改变，设备时钟也可能错误。拍摄日期必须结合内容、应用程序日志、备份、位置、序列和证言等其他来源印证。

NOM-151 规定了墨西哥的保存和数字化要求，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。可见日期只是更严谨核查的起点。[7]

2.5 照片与长椅案例

在作者分析的一起案件中，一组照片提供的日期和坐标与指控所称地点不同，但与另一位置相符。手机加速度计还显示了一段停顿，与某人自称坐在长椅上的时间相符。关键不在长椅这个物体，而在停顿这一日常模式：它有助于核查一种说法，而不必诉诸戏剧化解释。

传感器没有记录悲伤或意图，也没有把数据变成形而上学的确定性。它们可能与某个事件序列一致，但结论仍需照片、消息、移动记录、云端数据源、证言，以及数据究竟由传感器生成还是手工录入的审查来印证。科学表述不是“手机说出了真相”，而是“这些来源因其生成方式和行为，与这一事件序列相符，而与另一种序列不符”。[8]

方法启示

数据源不会因为信息丰富或技术复杂就自动真实。只有理解元数据是什么、何时生成、可能发生何种改动，以及与其他哪些来源一致，元数据才有帮助。可信度来自信息汇聚，而不是形容词。

2.6 可访问性与语境保存

无法访问的对象无法接受复核。保存要求能够打开、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。一份无法定位数据来源的精美报告只是展示材料，不是完整调查。

[7]NOM-151-SCFI-2016，数据电文的保存和数字化，发布于 30-03-2017。关于记录、完整性、可访问性和电子数字指纹的要求。官方在线来源

[8]Jocsan Laguna。Libro abogados，第 1 章。作者提供的叙事研究材料。手册中更改姓名以保护身份。



图3 数据源、导出文件、工作副本和打印件：覆盖范围不同的表现形式。编辑重构；不构成真实证据。

限定性结论

完整性不等于真实性，归属不等于自然人身份，日期不等于事件。应分别记录每个概念，避免把控制工具变成绝对结论。

第3章 角色、职责与决策

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；律师不能替代技术验证；保管人也不能为了方便分析而改动数据源。

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。独立复核人核查主张与证据是否相关，不受报告提交人影响。

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。
复核人	核对方法、发现和局限。	复核意见和处理结果。

3.2 不凭临时应对的第一响应

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、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，不得为了使记录看似完美而隐瞒。接收记录应说明材料到达前实际发生了什么，而不是为了呈现理想顺序而选择有利说法。

肉眼检查可以提供方向，但添加表格、截图或结论并不能使其成为鉴定。计算机鉴定人必须解释方法、数据源、工具、参数、验证和局限。不具备相应专业知识的人把感知包装成科学分析时，问题不在词汇，而在方法论权限和可复核性。



图4 独立复核核对数据源、方法和结论，而不只是修改文风。编辑重构；不构成真实证据。

3.3 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不可逆操作的唯一记录。沟通是决策证据的一部分，而不是单独的行政备注。

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。如果约定排除内容或重新导出，应纳入授权和变更记录。如果通过链接收到答复，应记录打开人、权限、日期和下载版本。

最低沟通记录要求

记录谁向谁提出请求、谁授权了什么、使用何种渠道和日期、产生了哪些变更，以及事后进行了什么核验。对话不是可选背景，而是解释决策原因的依据。

3.4 独立性、隐私与第三方

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，但不得为了迎合初步版本而改动原始材料。只寻求印证分析师既有结论的复核不是独立复核。

隐私要求区分调查目的和不必要的暴露。第三方数据必须按照比例、安全和保密原则审查。隐私告知不是形式文件：它说明处理哪些数据、为何处理、谁可以访问以及如何行使权利。案件涉及个人数据时，负责人必须采取必要且充分的措施，不得把鉴定变成公开传输信息的过程。[9] 自 2025 年起，个人数据保护的联邦主管机关是反腐败与善治部，而不是 INAI。这一变化不会取消保护义务，也不会使所有调查自动成为例外：需要时，应更新提交申请或申诉的对象，避免把历史机构当作现行主管机关引用。[10]

3.5 角色三段论

大前提：鉴定需要专业知识、方法和可复核性。小前提：没有数据源识别、参数和验证的目视检查，三者皆不具备。结论：看似分析并不足以把感知变成鉴定。解决办法不是解雇检查人员，而是正确分配职能，并保全确实能够证明的内容。

第一响应可以记录状态和保管情况，无需把自己包装成分析。专业人员随后可以以规范方法取证获取，复核人则检查做了什么、没做什么。这样既避免善意变成无法辩护的断言，也使每个人只作出其职能真正能够支撑的陈述。[11][12]

---

[9]《联邦私人持有个人数据保护法》，新法于 20-03-2025 发布，并于 14-11-2025 修订。第 5–9、18–20 和 31 条：原则、安全、保密、数据泄露和期限。官方在线来源

[10]反腐败与善治部。第 011 号公告，21-03-2025：个人数据保护职能由 INAI 移交至该部。官方在线来源

[11]ISO/IEC 27037:2012。数字证据识别、收集、取证获取和保全指南。该版本经 ISO 确认现行有效。官方在线来源

[12]Jocsan Laguna。Sinaloa。计算机取证技术意见的形成和结论。作者提供的材料；在不暴露个人数据的情况下归纳错误。

限定性结论

能力应通过职能和方法证明，而不是通过职务。无法解释数据源、程序和验证的人，其介入应如实表述为接收、指导或检查，而不是技术鉴定意见。

第4章 生命周期与取证准备

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语境恢复。保存不是无限积累，而是决定哪些信息可能需要以及需要多久。
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账户。正确的联系人、应急授权和接收记录副本必须在事件发生前准备好，而不是等到日志滚动覆盖或无法访问时才寻找。

最低准备要求	应检查的内容	可避免的错误
资产和负责人清单	负责人、数据源、格式和位置保持更新。	向错误的保管人索取日志。
保存期限和格式	可用时间段、字段、时区和导出过程。	事后才发现数据已不存在或无法理解。
通讯录和代理人	技术、法律、保管人和供应商联系人及其替代人选。	依赖单一个人。
时间同步	时间来源、偏差和定期复核。	因时钟不一致而构建错误时间线。
演练	虚构证据、接收、取证获取、移交和复核。	在危机中临时制定程序。



图5 事件前准备：数据源清单、保存期限和访问权限。编辑重构；不构成真实证据。

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。关机可能保留状态，也可能破坏内存和会话；停用账户可能停止活动，也可能使人无法访问唯一可用的导出文件。

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。评价遏制措施时，不仅要看避免了什么损害，还要看能否解释做了什么、为何这样做，以及付出了何种证据代价。

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。

紧急决策	证据风险	建议事先采取的措施
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。
删除链接	版本或下载渠道丢失。	保存 URL、权限、版本、日期和收到的文件。



图6 不可逆节点：可能使后续分析无法进行的操作。编辑重构；不构成真实证据。

4.3 记录在案的流程与交付物

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，下一阶段得到的只是假设，而不是可验证的依据。只装有结论的文件夹无法支撑这条链。

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，但不会把方法论当作对内容的自动认证。[13][14]

阶段	最低交付物	验收问题
授权	范围、许可、排除事项和负责人。	我们能否以该目标和范围实施此操作？
识别	对象、状态、保管人、标识符和照片。	我们是否确切知道持有什么、它如何到达？
取证获取	方法、工具、参数、输出和异常情况。	他人能否重复该过程并将其与对象关联？
保管	移交、访问、封条和验证。	我们能否还原谁访问过以及为何访问？
分析	假设、数据源、结果和其他解释。	是否也寻找与最初说法相矛盾的内容？
报告与保存	结论、局限、附录和后续访问。	今后能否复核、打开并理解？

[13]ISO/IEC 27037:2012。数字证据识别、收集、取证获取和保全指南。该版本经 ISO 确认现行有效。官方在线来源

[14]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. 方法指南，并非法律，也不保证证据可采性。官方在线来源

4.4 保存期限与纵向分析

孤立事件看似异常，可能只是因为不了解日常规律。如果要判断是否存在异常行为、准备或重复，应把一天的活动与此前和此后的时期比较。一次短暂访问可能是长期准备的最后阶段；许多小额访问也可能表明分散式行为。纵向分析可以避免把事件快照当作对过去的完整解释。

日志保存并非无限期，也不统一。墨西哥《电信和广播法》区分了首个十二个月的阶段：系统须允许主管机关实时查询和交付；随后十二个月则使用电子存储系统，并须在申请通知后四十八小时内交付。重点不是死记期限，而是在保存期限和覆盖范围改变分析可能性之前，及时申请数据源。[15]

保全决策

不要等到最低保存期限将至才申请日志。法定保存不能保证无限期可用，也不能保证覆盖所有事件。应尽早保全、记录时间段并比较模式，然后再断言某事是否异常。

4.5 作为社会责任的准备工作

准备可以避免紧急情况演变为任意决策。组织如果知道谁负责、保存什么、如何导出以及哪些内容不得触碰，就不太可能破坏有用证据或暴露第三方数据。准备也使工作更加普惠：即使第一响应人员不是工程师，也能依既有程序和联系人有序行动。

限定性结论

准备不是记录一切，而是能够连同语境恢复相关内容。如果关键数据源没有负责人、已知保存期限、格式文档或授权访问，这就是必须在事件发生前解决的弱点。

[15]《电信和广播法》，发布于 16-07-2025。第 182 和 183 条：数据要求和保存、实时查询，以及按阶段在 48 小时内交付。官方在线来源

第5章 不同情景下的决策树

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。应根据问题和可用能力决定，而不是沿用惯例。

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。如果没有能力安全进行现场取证获取，应先记录并请求支持，再改变设备状态。首要决策不是选择工具，而是理解每种选择会失去什么。

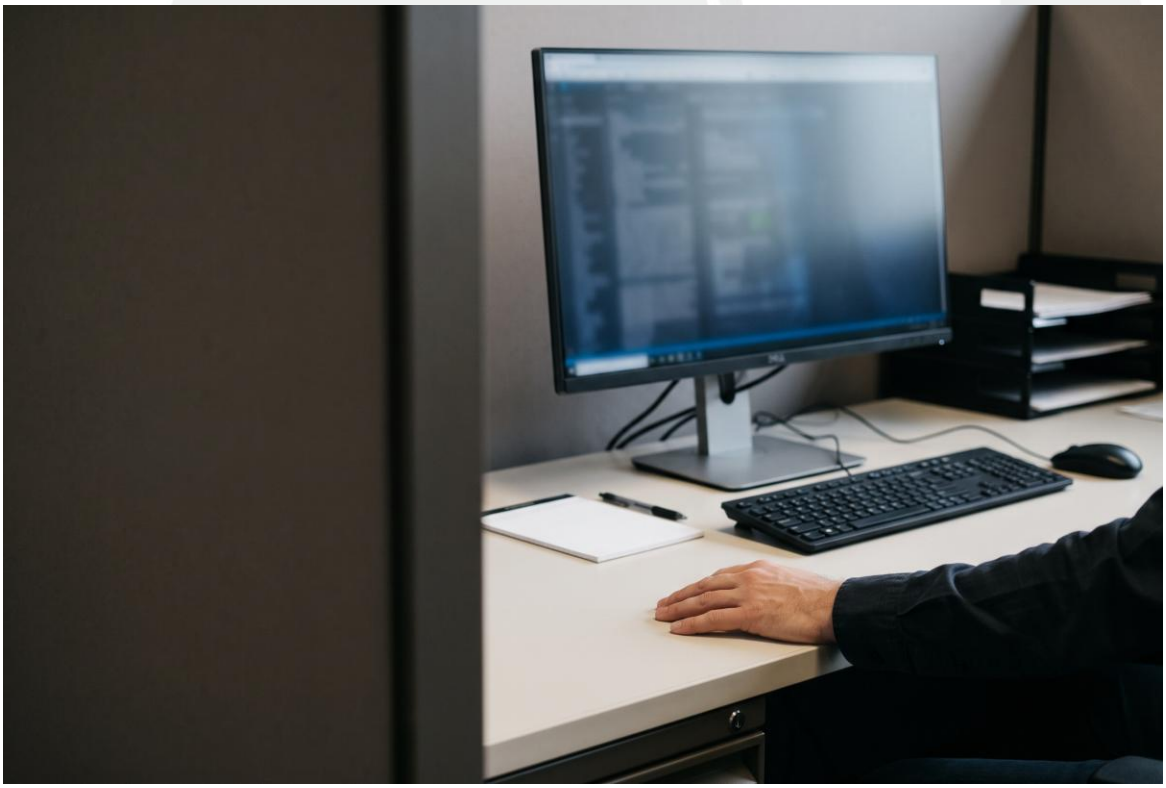


图7 开机设备：决定前记录状态和活动。编辑重构；不构成真实证据。

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。远程途径必须记录执行人身份、参数、日期、时区、格式和传输渠道。关键不是可见文件在哪里，而是覆盖范围更广、改动更小的数据源在哪里。

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。供应商提供的原生文件，可能比他人打印同一文件形成的材料更具证据价值。

条件	首选路径	必需记录
需要内存或会话	经授权并验证后进行现场取证获取。	状态、进程、输出、时间和不可避免的改动。
设备关机且稳定	根据目标制作镜像或进行逻辑取证获取。	数据源、连接、方法、覆盖范围和异常情况。
平台或第三方事件	管理性导出或供应商。	角色、筛选条件、时区、格式、字段和 EML 交付。
访问受限或工具未经验证	停止并上报，保持状态不变。	原因、状态、风险和后续负责人。

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，而且许多设备无法在不造成损坏或改动的情况下拆卸电池。导出或保全账户可能需要连接，因此隔离并不总是首要措施。

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。包装标有“法拉第”并不足够，还必须能够在具体场景中实现并验证隔离功能。



图8 防静电与射频隔离并非同一功能。编辑重构；不构成真实证据。

5.4 光盘：标识符与格式

光盘必须准确识别。当标签、公文和目视检查不一致时，只写“一张 CD”或“一张 DVD”并不足够。应记录介质类型、品牌和型号（如有）、容量、状态、可用读取设备和任何可见标识符。中心环可能包含代码或制造标识，应在不接触数据面的情况下检查，并结合整体语境拍照。并非所有光盘都有相同的唯一标识符，也并非所有可见代码都是具有证明作用的序列号。正确做法是检查中心环并如实记录显示内容，不存在时不得编造。还应区分可重写介质和只读介质：DVD-RW 并非只是外观差异，其重写可能性不同，必须如实记录。



图9 检查中心环：可能用于识别光盘的标识符和代码。编辑重构；不构成真实证据。

识别先于结论

无法识别介质，就不能声称分析了正确对象。伪保管始于“有一张光盘”；真正的保管则始于标识符、状态、格式、照片及其与接收记录的对应关系。

5.5 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。有记录的停止不是失败，而是保留分析可能性、避免无法辩护行动的措施。

停止记录应包括原因、对象最终状态、此前操作、已识别风险和后续负责人。如果疑问后来得到解决，还应记录答复人及其采用的方法。暂停不会改写过去，而是解释为何选择不让案件进一步恶化。



图10 停止并上报：继续操作破坏的证据可能比获得的更多。编辑重构；不构成真实证据。

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。

5.6 决策树是推理工具，不是装饰

决策树只有迫使人员回答输入条件、行动和记录要求时才有用，而不是展示一串无人遵循的图标。每个分支都应以有依据的行动、理由和记录结束。条件改变，路径也应改变。加密设备、联网手机或能够提供更优导出文件的供应商，不应默认导向同一操作。

限定性结论

正确路径取决于状态、目标、授权和风险。如果只能以习惯解释决策，就说明决策树设计或应用有误。记录引导至某一路径的条件，与记录最终行动同样重要。

第6章 现代数据源与通话记录表

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。下载界面不等于获取账户的完整历史。

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。输出必须能够说明实施了什么查询及其覆盖范围。



图11 通过供应商或 API 导出：筛选条件、字段、时区、格式和交付。编辑重构；不构成真实证据。

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。只保存附件会破坏文件与完整性声明之间的联系。

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。渠道真实性应结合邮件头、服务器和语境审查，而不是只看邮箱截图。

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。



图12 EML 保存正文、邮件头和附件，截图不能替代。编辑重构；不构成真实证据。

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。

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。
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。

申请示例

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。取证获取必须指明层级，而不只是产品：摄像头不是全部证据，路由器也不是整个网络。



图13 虚拟化：宿主机、客户机、快照和共享存储。编辑重构；不构成真实证据。

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。

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。[16][17]

[16]墨西哥。《联邦刑法典》第 199 Octies 和 199 Nonies 条，汇编包含 13-03-2026 的修订：涉及未经同意的私密性内容的特定行为，包括材料与所识别人员并不对应的情形。官方在线来源

[17]（UE）2024/1689 号《人工智能条例》，第 50 条，截至 27-07-2026 的合并文本：特定深度伪造的透明度，以及对创意、讽刺、艺术或虚构作品的调整。官方在线来源

6.6 现行效力：修订后被废止的示例

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。[18]

更新规则

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法律，也不得把提案当作法令。比较等效仅限于功能和范围，不意味着程序效力相同。

[18]圣路易斯波托西州。《议会公报》，30-07-2026：废止第 187 Ter 条以及包含第 272 Bis 和 272 Ter 条的章节。历史先例，并非现行规则。官方在线来源

6.7 数据源并非只存在于一个位置



图14 设备、应用程序、账户和供应商：现代证据的各个层级。编辑重构；不构成真实证据。

限定性结论

用户界面并不能涵盖数据源的全部。正确的导出文件可能存在于供应商、云服务、版本历史或交付邮件中。分析内容之前，应先识别所在层级并保存其语境。

第7章 接收与初步保全

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。如果有光盘，应注明介质、容量、格式和中心环代码（如可见）。

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、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。目标不是制造完美接收，而是记录初始条件。

字段	应包含的内容	虚构示例
对象和标识符	类型、品牌、型号、序列号、容量和分配的编号。	2.5 英寸 SSD，512 GB，序列号 demo-003。
交付与接收	姓名、职能、日期、时间、时区和地点。	保管人 A 交给分析师 B，11 月 09 日 14:32 −06。
状态	开机、锁定、网络、损坏和配件。	已关机，无可见损坏，SATA 数据线和电源。
封条与包装	类型、标识符、状态和照片。	01 号封条完好，硬质包装盒和防静电袋。
先前操作	打开、连接、复制、变更或情况不明。	不知道交付前是否曾开机。
初始决策	保全、上报、取证获取或请求澄清，并注明负责人。	保持现状并请求专业人员协助。



图15 分析前拍摄对象及配件的初始状态。编辑重构；不构成真实证据。

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。拆封和更换封条都是保管事件，不是旁注。

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。材料应根据证据所需功能选择，而不是根据容器的专业外观。



图16 接收与包装：物理保护、封条、标签和对象关系。编辑重构；不构成真实证据。

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。物理标签和接收记录必须与数字清单及最终报告一致。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。标识符不能替代原始对象：同一数据源的不同导出文件应获得关联标识符和关系说明。标识符必须便于定位，同时不得泄露客户、持有人或敏感信息。

虚构标识符示例

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



图17 标记对象、状态、日期、保管人和标识符。编辑重构；不构成真实证据。

7.4 配件和连接也是接收的一部分

电缆、适配器、SIM 卡、SD 存储卡或电源，可以解释信息是如何访问的，或哪些连接曾经可行。这些应作为关联对象记录，而不是隐形配件。只拍摄手机可能遗漏获取或解读数据所需的证据。清单必须包括收到的每个元件及其与主设备的关系。



图18 配件和连接：接收和取证获取可能性的一部分。编辑重构；不构成真实证据。

7.5 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。下载也是接收事件，不能成为不可见的操作。

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。秩序应通过清单建立，而不是通过改动收到的对象。

限定性结论

接收是方法的第一项检验。如果对象、状态、标识符和先前操作不清楚，后续任何断言都会从一开始就带有本可避免的不确定性。

第8章 取证获取与技术记录

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。每种方法满足不同需要，也产生不同局限。

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。“取证获取”这句话本身不能说明实施了什么操作及其覆盖范围。

方法	何时可能适用	必须声明的局限
物理镜像	需要完整介质，包括未分配空间。	不保证能够分析每个文件或每个平台。
逻辑取证获取	需要选定的文件或数据源。	选择和筛选条件决定覆盖范围。
易失性内存	会话、密钥、进程或临时状态具有相关性。	授权和理由，以及改变状态可能造成的损失。
官方导出	最佳数据源位于供应商或平台。	供应商的参数、格式和覆盖范围。
文档化获取	没有其他可用表现形式，且需要展示可视化内容。	不保留原始材料的全部属性。

8.2 实际连接：数据源、写保护器和工作站

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。数据源连接到写保护器，工作站连接到另一端。配置必须与实际实施一致，而不是与手册中的理想示意图一致。

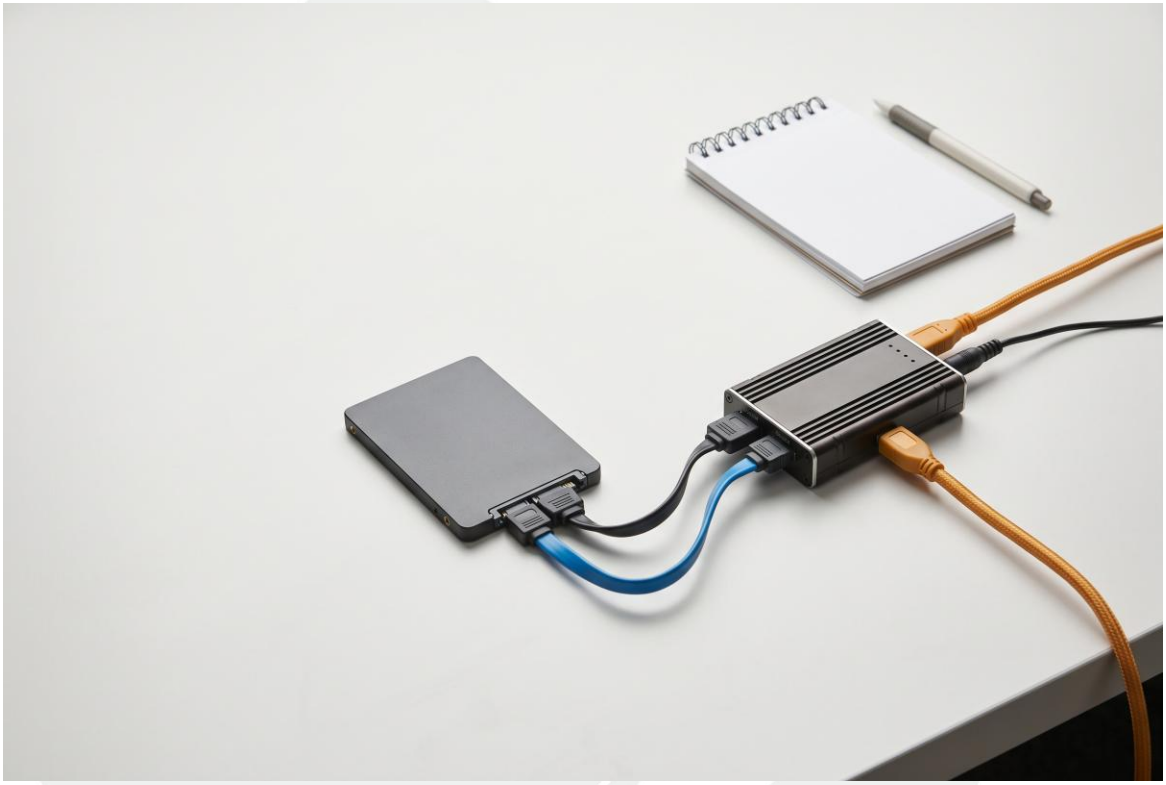


图19 数据源、写保护器和工作站：连接本身也是证据。编辑重构；不构成真实证据。

应记录写保护器的型号和序列号（如有）、所用端口、电缆、供电、指示灯状态和任何异常。工具出现错误时，应保存相关信息并评估其影响，而不是隐瞒。保护是否有效，应通过配置和验证证明，而不是仅凭设备名称。

8.3 介质和适配器：NVMe、SATA 与光盘

介质形态会改变取证获取方式。M.2 NVMe 的连接方式不同于 2.5 英寸 SATA，3.5 英寸 SATA 又需要不同供电。适配器必须兼容并记录在案。适配器照片有助于解释连接路径，但记录还应包括型号、接口、供电，以及工作站能否正确识别介质。



图20 介质和适配器：形状、连接器和取证获取程序。编辑重构；不构成真实证据。

对于光盘，应记录读取设备、格式、容量、读取方法、不可读扇区及其与所收介质的关系。如果图像显示的是计算机上的文件夹而不是光盘，就不能声称已完成 DVD 取证获取。读取失败时，应保留错误并评估第二个驱动器或其他方法，不能用笼统断言掩盖问题。

8.4 逻辑取证获取与清单文件

逻辑取证获取取得选定的文件或数据源。执行前应界定文件夹、文件类型、日期、筛选条件和排除事项。输出应附清单文件，记录标识符、名称、路径、对象类型、来源、方法、大小、格式、哈希值和备注。没有清单文件，装满文件的文件夹可能只有数量，并不一定是组织有序的证据。

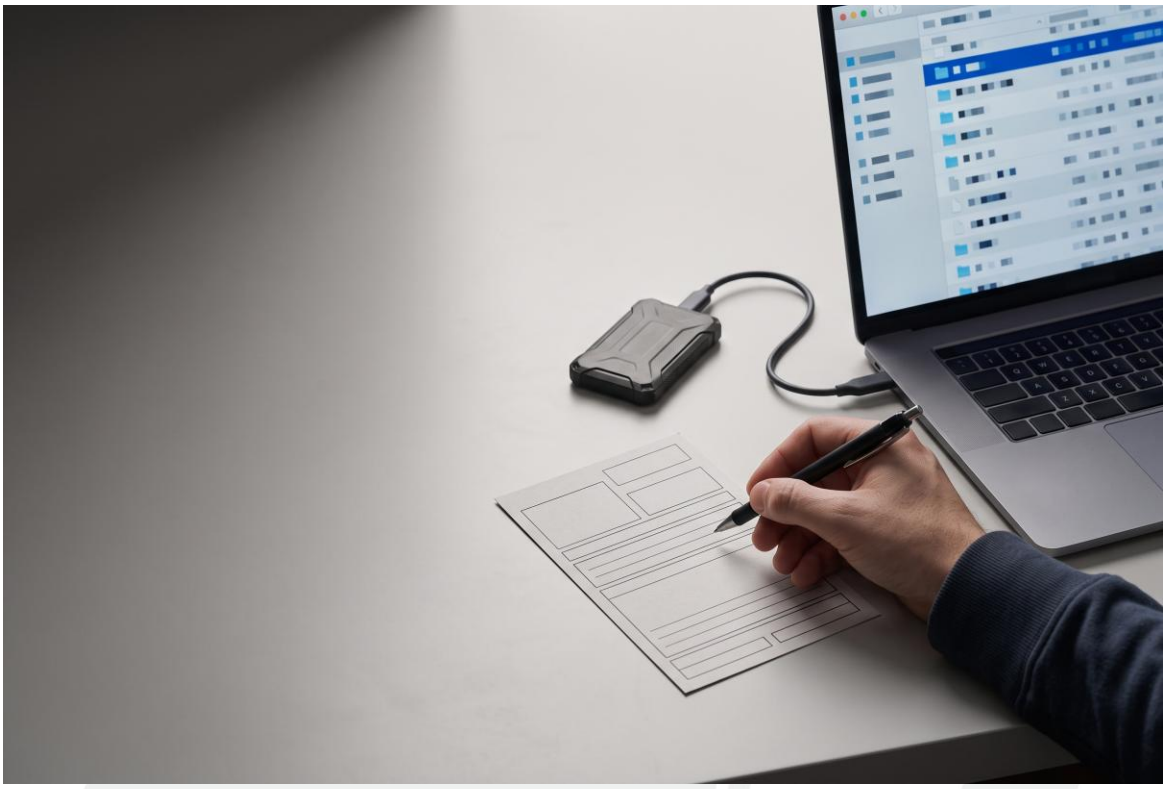


图21 文件清单：来源、派生对象、格式和各对象的完整性。编辑重构；不构成真实证据。

清单文件规则

清单文件不得公开秘密信息或不必要的敏感数据。如果路径会泄露受保护信息，公开版本可以缩写，但必须保留足够关系，以便在受控案卷中定位对象。

8.5 现场内存获取与工具验证

当内存、会话、密钥或进程具有相关性，且具备授权和执行能力时，现场取证获取才有正当理由。应记录状态、工具、版本、参数、不可避免的改动和输出。不具备这些条件时，应上报处理。不能仅因为导出文件更难申请，就实施侵扰性取证获取。

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。



图22 使用前验证工具：虚构数据、可读输出和预期对象。编辑重构；不构成真实证据。

8.6 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。可重复性取决于有记录的条件，而不是记忆。

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。缺失可能具有意义，但仅限于已核实的覆盖范围。

8.7 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。重复获取不会抹去首次尝试，而会生成具有不同历史的关联对象。

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。一份只有表面完美的案卷，不如如实声明异常及其处理方式的案卷更具可辩护性。

限定性结论

取证获取并不是生成一个文件就结束，而是得到能够打开、与对象关联、验证并在有记录的条件下重复的输出。如果发生故障，应写入记录，不能从叙述中删去。

第9章 保管、移交与保存

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。它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。封条即使在接收时完好，也可能无法说明此前由谁拆封。保管链应记录接收、拆封、复制、访问、移交、验证和返还等事件。每个事件都有负责人和目的，不只是姓名和日期。



图23 保管移交：对象、负责人、封条和验证。编辑重构；不构成真实证据。

9.2 电子移交与密钥

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。共享链接却不知道谁可以打开，不属于受控保管。

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。密钥或接收方发生变化时，也必须记录。



图24 加密与密钥：保护内容，同时不失去接收控制。编辑重构；不构成真实证据。

密钥规则

仅加密并不足够：应记录谁持有密钥、通过哪个独立渠道交付，以及如何验证接收。密钥不得写入接收记录或邮件正文。

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。保存还包括未来可读性、格式文档和可用密钥。

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。首个工作副本不得与原始包装混淆；任何拆封、换封或移交都必须记录。



图25 备份与迁移：保存原始材料、工作副本和后续访问能力。编辑重构；不构成真实证据。

9.4 拆封与更换封条

为了工作而打开容器，不会抹去封条和历史。应记录由谁拆封、为何拆封、依据何种授权、封条原状态以及其中装有何对象。完成后，应使用新的封条标识符重新封存；程序要求时，还应保留旧封条。保管链依靠可验证的行动，而不是“包裹已关闭”的笼统声明。



图26 拆封与更换封条：同样必须记录的移交。编辑重构；不构成真实证据。

9.5 访问、共同保管与冲突

后续访问必须记录查询、目的和授权。如果有人复核、导出或共享，该操作必须与其职能关联。共同保管不会消除责任，反而需要明确谁决策、谁执行、谁验证。利益冲突应申报，并在独立性要求时进行隔离。



图27 访问记录：谁可以经授权打开、查阅和移交。编辑重构；不构成真实证据。

限定性结论

保管并不是把对象存好就结束，而是必须能够还原每次访问、移交和验证，包括如何保持今后打开对象的能力。

第10章 检查、时间线与其他假设

10.1 检查不是寻找责任人

检查始于数据源已识别、获取并与委托关联之后。其目的不是寻找能证明第一印象正确的文件，而是把大量数据转化为可核验的观察。分析师打开工作副本、记录工具并提出具体问题：存在什么文件、显示什么日期、字段意味着什么、发生了什么变化、哪个系统生成记录，以及其他哪些数据源可能推翻它。每个答案都必须回到清单文件中的具体对象。

检查与分析的区别，就像观察钟表零件与解释钟表为何停止的区别。检查观察齿轮、磨损和位置；分析则比较不同解释：动力不足、机械损坏、人为操作或读数错误。如果直接跳到偏好的解释，任何零件都看似能够支持它。工作规范要求先描述、后解释，并保留不符合预期的内容。[19]

工作规则

分析中的每项陈述都必须能够逆向追溯：从结论到发现，再到查询、被分析对象、取证获取，最终回到数据源。如果其中任何环节无法展示，就必须重新表述结论或寻找其他数据源。

10.2 元数据：倾听文件，但不全盘相信

元数据是关于对象的信息，不是事件主动作出的供述。文件系统的创建日期可能对应文件复制到该介质的时间；照片内部日期可能取决于相机时钟；作者标签可能是任何人配置的账户名称。每个字段都有生成者、生成机制和改动可能。正确解读需要知道由谁、何时、在何种条件下写入，以及分析是否改变了它。

文件名也能提供方向，但不能单独证明事实。IMG_0041、IMG_0042、IMG_0043 的序列暗示相机或应用程序内的生成顺序，却不能排除复制、重命名、编号重置或文件导入。审慎分析

[19]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. 方法指南，并非法律，也不保证证据可采性。官方在线来源

应核查内部标识符、缩略图、日期、应用程序日志和备份是否保持该序列。文件名是调查线索，不是时间戳印章。

假设一张图像显示 18:42，而指控称其拍摄于 20:42。第一种冲动是断言证据被伪造；第二种同样危险，是把 18:42 当作绝对时间。正确方法是保存原生文件，在不改动文件的情况下提取字段、核查时区、检查设备时钟、比较前后序列，并寻找独立数据源：发送消息、云端副本、购买收据、其他摄像头视频或活动日志。只有此后，才能判断是时区差异、时钟配置错误、格式转换，还是更严重的不一致。



图28 元数据需要明确生成者、含义、语境和印证，并非不会出错的证言。编辑重构；不构成真实证据。

观察到的数据	技术问题	尚不能作出的结论
系统日期	它在此文件系统中代表什么事件?	它就是事件的原始日期。
EXIF 日期	时钟和时区如何设置?	场景必然发生于该时间。

观察到的数据	技术问题	尚不能作出的结论
作者或账户	谁可以配置或使用该账户？	自然人身份已确定。
连续文件名	其他数据源是否保留该序列？	不存在复制、导入或重命名。
坐标	位置的精度和来源是什么？	当事人就在该精确位置。

10.3 时间线：先校准时钟，再排列事件

有用的时间线不是一列排序后的日期，而是对可能处于不同时区、与不同服务器同步或带有人为误差的时钟进行校准。首先记录数据源的原始值，然后记录声明或推定的时区、所应用的转换和可用精度。原始数据绝不能被转换值替代。如果供应商使用 UTC 而手机记录本地时间，报告必须同时显示两者并说明比较方法。

精度与日期同样重要。只包含日期的记录不能为了画面整齐而写成 14:32；带秒的文件也不一定具有秒级准确性。如果时钟存在已知偏差，应记录测量方式及影响哪些数据源。无法解决时，应使用时间窗口或声明不确定性。这样可以避免视觉上完美的序列把两个不兼容事件变成因果关系。

时间序列还应保留否定事件和无数据时段。日志中断可能源于无活动、滚动覆盖、连接丢失、配置或删除，时间线不得在没有证据的情况下任选一种解释。每个事件都应标记为观察所得、计算所得、人员陈述或推定。把这四类混为一谈，是在隐蔽地制造确定性。



图29 时间线保留每个数据源的原始时间、时区、转换和不确定性。编辑重构；不构成真实证据。

时间规范化示例
对象：ED-20261109-DEMO-SRV-001-A00
原始值：2026-11-03 20:14:07
供应商声明的时区：UTC
工作转换值：2026-11-03 14:14:07 -06:00
可用精度：秒；服务器同步未获证实
关系：该事件早于 14:20:11 -06:00 收到的邮件
局限：时间接近不能证明由谁实施操作，也不能证明一个事件导致另一个事件。

10.4 天线、覆盖范围与方位角：地理分析不能走捷径

通话记录表可能显示某条线路通过某个基站小区通信。该数据不会把天线变成个人，也不能证明携带者就在天线下方。小区描述的是在网络、覆盖、拥塞、技术和配置条件下形成的无线通

信关系。分析需要小区位置、方向或方位角（如有）、技术类型、日期、功率或可用测量值，以及对实际区域的理解。地图上的一个点表示设备，不是用户照片。

方位角表示天线指向的扇区，不是终止于某栋房屋的激光线。覆盖取决于传播、障碍物、频率、地形、干扰、功率和网络决策。通话可能由并非最近的小区提供服务。导出文件中没有另一个小区，也不能证明不存在替代覆盖：可能只是未使用、未交付该数据，或系统未保存。

在作者复核的一起匿名案卷中，某个位置被当作个人行动轨迹描述，但数据源只能支持对覆盖范围的讨论。其他要素也使该说法更复杂：视频序列与所声称的解释不一致，证人对事实的描述也相互矛盾。分析的价值不是用一个同样绝对的故事替代另一个故事，而是表明该结论并非必然来源于数据源。天线仍然只是天线，携带者身份需要其他证据。[20]



图30 天线提供潜在覆盖范围，不能证明精确位置或携带者身份。编辑重构；不构成真实证据。

[20]Jocsan Laguna。Sinaloa。计算机取证技术意见的形成和结论。作者提供的材料；在不暴露个人数据的情况下归纳错误。

可辩护的结论方式

“交付的记录将事件与所识别的小区关联起来。在没有额外测量和参数的情况下，该数据不能确定精确位置，也不能把终端使用归属于某个自然人。”

10.5 具有区分力的印证

两个内容相同的文件不一定来自两个独立数据源。同一张截图及其打印件只是重复同一表现形式。相反，服务器日志、第三方收到的消息和传感器序列可能来源不同、误差也不同。当数据源不共享同一依赖关系，且各自原本都有可能推翻该说法时，印证才更有力量。

信息汇聚不能按页数衡量，而应评估独立性、与事件的接近程度、误差能力和区分假设的能力。一百张没有来源的截图，可能不如一份包含邮件头、可验证附件和服务器日志的完整 EML。奥卡姆剃刀原则并不要求选择最方便的解释，而是要求在一个简单序列能够解释数据且不忽视矛盾时，不随意增加原因。

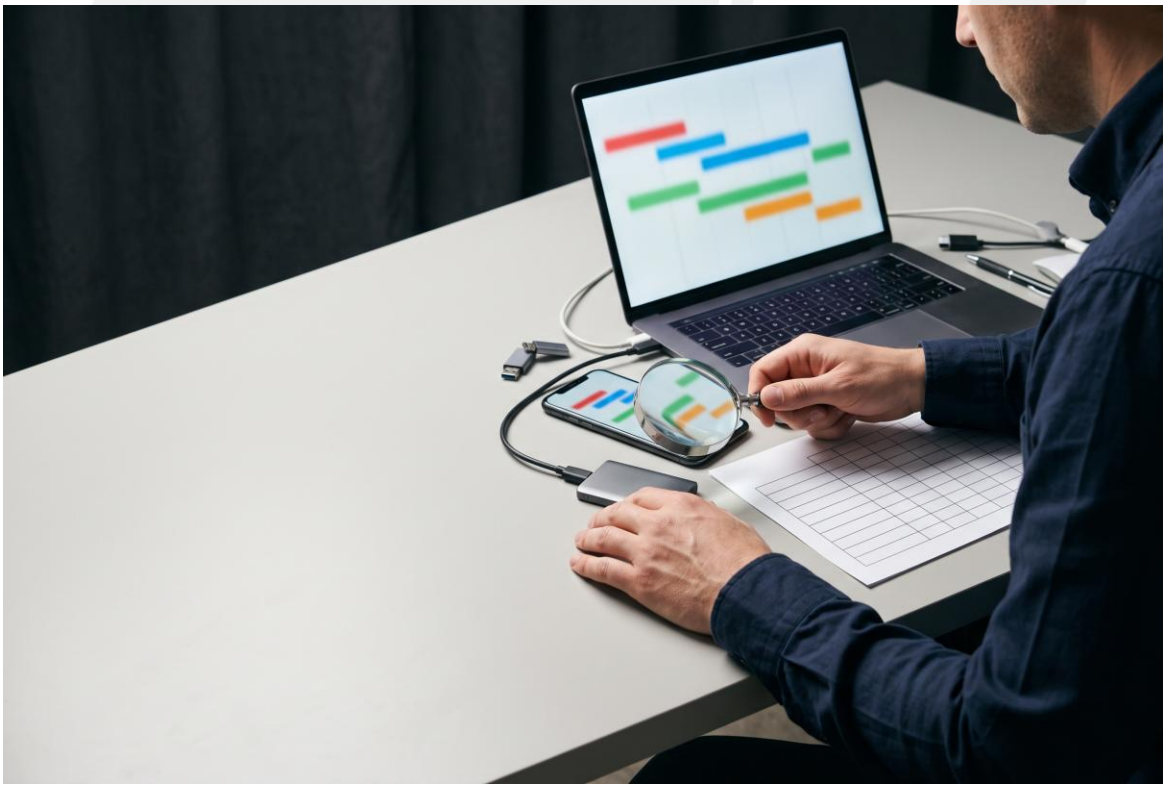


图31 印证是比较来源和误差不同的数据源，不是重复同一张截图。编辑重构；不构成真实证据。

10.6 假设矩阵：允许证据推翻假设

分析前，最好至少写出两种可能的解释，以及区分它们的条件。如果企业声称某文件由一名员工在离职当天创建，假设可以包括：指定账户于该日创建；事后复制先前文件；修改元数据；或他人使用该账户。各种假设不必具有相同概率，但都必须接受具体核验。

结果可能为肯定、否定或无法定论。有记录的否定结果不是失败：它可以排除某种解释并避免不公正的指控。无法定论也不能伪装成确认。当数据源无法作出区分时，正确做法是申请其他数据源、调整范围或声明局限。分析师不会因为坚持错误假设而得分，却会因为数据要求时愿意放弃假设而赢得信任。

假设	核验	虚构结果	限定性解读
该文件创建于 11 月 3 日。	内部元数据、版本历史和云端日志。	历史显示 10 月 28 日的先前版本。	可见日期不能证明初始创建时间。
账户由持有人使用。	会话、第二验证因素、设备和并发活动。	存在来自未登记设备的会话。	账户归属仍不能识别具体个人。
该图像属于同一事件。	序列、缩略图、备份和相邻文件。	备份包含一致的序列。	与该事件相符；其含义仍需结合语境。
不存在其他访问。	完整查询、保存期限、筛选条件和错误。	导出文件仅覆盖七天。	在所查询期间未观察到；不能断言完全不存在。



图32 同时寻找推翻初始假设的证据，避免把分析变成单纯印证。编辑重构；不构成真实证据。

10.7 重复、复现与知道何时停止

可重复的查询能够在有记录的条件下再次执行，并对同一对象产生相容结果。可复现性还要求另一位具备资质的人员能够充分独立地理解和评估程序。如果不知道文件、工具版本、筛选条件或查询，仅保存结果截图不能满足这两项要求。目标是让复核能够依据数据提出不同意见，而不是只能相信分析师的记忆。[21]

当委托问题已在范围内得到回答、新增数据源不再具有区分力，或继续操作会造成不相称的侵扰时，应停止分析。遇到新的数据源需要授权时，也应暂停。全面并不意味着打开每个可能的文件夹，而是不要让任何现有证据能够解决的合理假设未经审查。

[21]ISO/IEC 27037:2012。数字证据识别、收集、取证获取和保全指南。该版本经 ISO 确认现行有效。官方在线来源

本章交付物

分析矩阵包括陈述、数据源、查询、原始发现、相容假设、被削弱假设、局限和后续行动。结论应从矩阵中产生，不能先写结论再倒填矩阵。

第11章 报告、推理与质证

11.1 报告是返回数据源的路径

鉴定报告不应以厚度或英文术语数量取胜。它必须让持不同判断的人能够定位对象、理解实施了什么，并审查结论是否源自发现。报告结构是一条路径：委托、范围、授权、数据源、方法、结果、分析、结论、局限和附录。如果某项陈述不能沿这条路径逆向追溯，报告就会沦为依赖权威的写作。

主要读者并不总是工程师。法官、律师、管理人员或被指控的人都需要理解推理，而不必先学习一套秘密语言。清晰的写作不会削弱科学性，反而使其接受检验。因此，专业术语首次出现时应解释，每张截图都应附原始对象，或说明其不可用的原因。解释的简洁程度应与工作严谨性相称，而不是与严谨性的缺失相称。



图33 报告使数据源、方法、发现和结论可供验证，不依赖签署人的声望。编辑重构；不构成真实证据。

11.2 事实、结果、推论与意见

文本必须区分四个层面。文档事实是接收记录所载内容：文件以特定名称和大小到达。技术结果是核验产生的输出：计算得到的哈希值与另一个值一致。推论是对多项结果进行合理解读：收到的附件与供应商声明的附件一致。意见是委托范围内的专业结论：该交付自那时起保留了可验证的完整性机制。混淆这些层面，会使意见看起来像观察到的数据。

法律问题和技术问题也必须分开。鉴定人可以描述记录如何取得、包含哪些字段以及存在哪些不一致，无需断言某人有罪、某种行为构成犯罪或某一方应当胜诉。这种克制不会降低报告价值，反而能防止属于其他专业权限的结论污染真实发现的力量。

层面	正确示例	应避免的过度表述
接收	“在标识为 EV-04 的 EML 中收到 adjunto.csv。”	“银行交付了全部真相。”
结果	“计算得到的 SHA-256 与正文中记录的值一致。”	“内容自形成以来从未被改动。”
分析	“该一致性将附件与供应商的声明关联起来。”	“该通话由持有人实施。”
结论	“交付与接收之间存在完整性验证。”	“该证据不可反驳且具有决定性。”

11.3 三段论与错误推论

三段论用于排列前提和结论。在鉴定工作中，它有助于发现热情容易掩盖的逻辑跳跃。大前提：小区记录网络与终端在覆盖条件下的关系。小前提：所分析的记录将一次通信与小区 A 关联。有效结论：该通信与小区 A 之间存在有记录的关联。但不能由此推出某个具体的人位于某个具体地点，因为还缺少有关位置、终端和用户的前提。

错误推论是指用一个真实陈述为另一个并不随之成立的陈述放行。文件包含 IP 地址，因此嫌疑人写了消息；签名验证通过，因此全部陈述都曾发生；视频显示时钟，因此整段录制真实；磁

盘已封存，因此分析的副本来自该磁盘。每项结论都需要额外前提和不同核验。加强推理的方法不是省略这些步骤，而是把它们展示出来。

对于物理介质，识别信息矛盾可能足以阻止推论。如果接收记录描述一种磁盘，而图像或容量对应另一种，就不能简单称之为小错误。首先必须澄清收到了哪个对象、获取了哪个对象，以及每项操作涉及哪个对象。数据源身份解决之前，应暂停结论。对象错误，就不可能有优秀分析。[22]

“因此”检验

每写下一个“因此”，都应列出使结论成立所必需的前提。如果该前提只是惯例、直觉或声望，就应把绝对推论改成限定性观察，或完成缺失的核验。

11.4 解释矛盾，而不是掩盖矛盾

矛盾并不总意味着伪造，也可能揭示时区、时钟偏差、不同筛选条件的导出、两个同名对象、字段解释，或确实不兼容的数据源。报告应列出差异的原始值并分析可能的解释。因为削弱某种说法而隐藏矛盾，是放弃科学职能；不加调查地利用矛盾，则是另一种错误。

假设一段视频有不可能的日期、一张通话记录表含有不符合预期格式的号码，两名证人又描述了不相容的位置。不能选择最方便的矛盾加以忽略。应检查视频是否保留计数器或未初始化的系统日期、号码是否被错误转录或导出，以及证人是否从不同地点观察了同一事件。如果解释不能成立，就应将其保留为未解决的不一致，并准确说明它对结论的影响。

照片与长椅案例展示了建设性的一面：日常数据源可以提供一种解释，支持一个原本看似不太可能的说法。天线案例展示了预防性的一面：技术数据源可能被用来支持它实际无法证明的结论。两种案例的方法相同：保全、理解、比较和限制。证据不是指控或辩护的装饰，而是用来接近一个经得起复核的事件序列。[23][24]

[22] Jocsan Laguna。Sinaloa。计算机取证技术意见的形成和结论。作者提供的材料；在不暴露个人数据的情况下归纳错误。

[23] Jocsan Laguna。Libro abogados，第 1 章。作者提供的叙事研究材料。手册中更改姓名以保护身份。

[24] Jocsan Laguna。Sinaloa。计算机取证技术意见的形成和结论。作者提供的材料；在不暴露个人数据的情况下归纳错误。

11.5 撰写证据能够承载的结论

有力的结论不一定是绝对结论。“在这些日期、筛选条件和覆盖范围内的导出文件中未观察到事件”，比“事件从未发生”更有力，因为它可以核验，也能经受敌意提问。同样，“所审查的数据与序列 A 相符，但与 B 存在这些不一致”，比“A 已得到充分证明”更能说明分析的分量。

断言程度应与方法的区分能力相称。只有可视化表现形式时，应描述可见内容并索取原生文件；有多个独立数据源时，应解释其汇聚及局限；缺少决定性数据源时，不得用形容词弥补。读者必须知道作出了什么断言、依据是什么、排除了什么，以及哪些新信息可能改变答案。

情形	可辩护的表述	可能改变表述的信息
哈希值一致	对象在两次有记录的验证之间保持不变。	对象或所记录算法的识别错误。
账户归属	事件与账户关联；仅凭这一点不能识别实际使用人。	第二验证因素、设备、凭据控制和印证记录。
日期元数据	内部日期与调查时段相符，但取决于时钟和时区。	独立备份、原生序列和同步。
查询无结果	在所声明的覆盖范围和筛选条件下未观察到记录。	扩大导出范围、修正筛选条件或恢复保存期限内的数据。

11.6 质证与独立复核

交付前，另一位人员应在不改动对象的情况下尝试推翻推理，核查标识符是否与接收记录一致、副本是否源自数据源、查询是否产生相同结果，以及结论是否超出数据。复核不能只纠正逗号；单纯美化报告，会让可能改变案件的错误原样保留。

出庭时，专业回答不是把每个字当作私人财产来捍卫。日期错误就应更正；数据源不可用就应声明；方法无法支持某项断言就应撤回。鉴定人的权威在于方法质量和接受复核的意愿，而不是拒绝承认局限。质证是对制度的检验，不是侮辱。



图34 独立复核在交付前查找数据源、方法和推论错误。编辑重构；不构成真实证据。

质证问题

能否定位具体对象？能否重复查询？数据源是否独立于待评说法？是否存在其他相容解释？哪些内容未审查？如果撤回某个前提，哪项断言将不再成立？

11.7 交付、附录和后续访问

交付包包括报告、清单文件、所引用的附录，以及适用时的受控副本。附录在正文和文件中的名称必须一致。交付公开版本时，应分离个人数据和秘密信息，同时保留完整的保存版本。报告不得公开密码、私钥或可能促成新损害的信息。

应确认文件能够打开、图像清晰、内部链接有效、所引用的附录确实存在。电子交付应使用获授权的渠道，适用时加密并验证接收。报告哈希值可用于版本控制，但不能使其内容成为真实。交付对象必须能够在数年后复核，并保留可用的格式和语境。

本章交付物

报告应回答委托中的每个问题，识别数据源，区分观察与推论，保留矛盾，声明局限，并提供足以支持独立复核的附录。

第12章 错误、学习与公共服务

12.1 不能通过改写过去来纠正错误

每个实际程序都包含不完美决策：有人先连接后拍照、忘记时区、收到打印件而非文件，或使用含糊名称。专业做法不是删除事件并编造理想记录，而是保留事实、记录其影响范围，并确定能否通过其他数据源恢复信息。改进始于案卷的真实性，而不是外观。

事后纠正可以减少损害，但不能制造追溯性的保管。如果今天为一个月前收到的文件计算哈希值，该值只能从今天起发挥控制作用，不能证明对象此前一个月一直完好。如果申请第二次导出，应将其作为具有独立接收记录的新对象保存，并与第一次比较。承认差异既能保护调查，也能保护相关人员。



图35 保存原始材料；分析在受控副本上进行。例外情况须说明理由并记录。编辑重构；不构成真实证据。

12.2 接收和保全中的错误

按习惯关机可能破坏内存和会话；不受控制地保持开机可能继续修改数据。在原始材料上工作，会使人难以证明哪些变化来自分析。把手机放入防静电袋却称为法拉第隔离，是混淆两种功能。包装没有标识符，会使人无法确认返还的对象是否同一个。这些问题不能靠购买更多工具解决，而应通过状态、授权、职能和记录预防。

把配件当作无关物品也是错误。电缆或适配器可以解释连接方式，额外存储介质可能包含数据源，电源则可以在决策期间帮助保持设备状态。接收时应查看整体，但不得出于好奇触碰。拍照、识别、关联和请求支持都是简单操作，却能避免数年后无法解释。

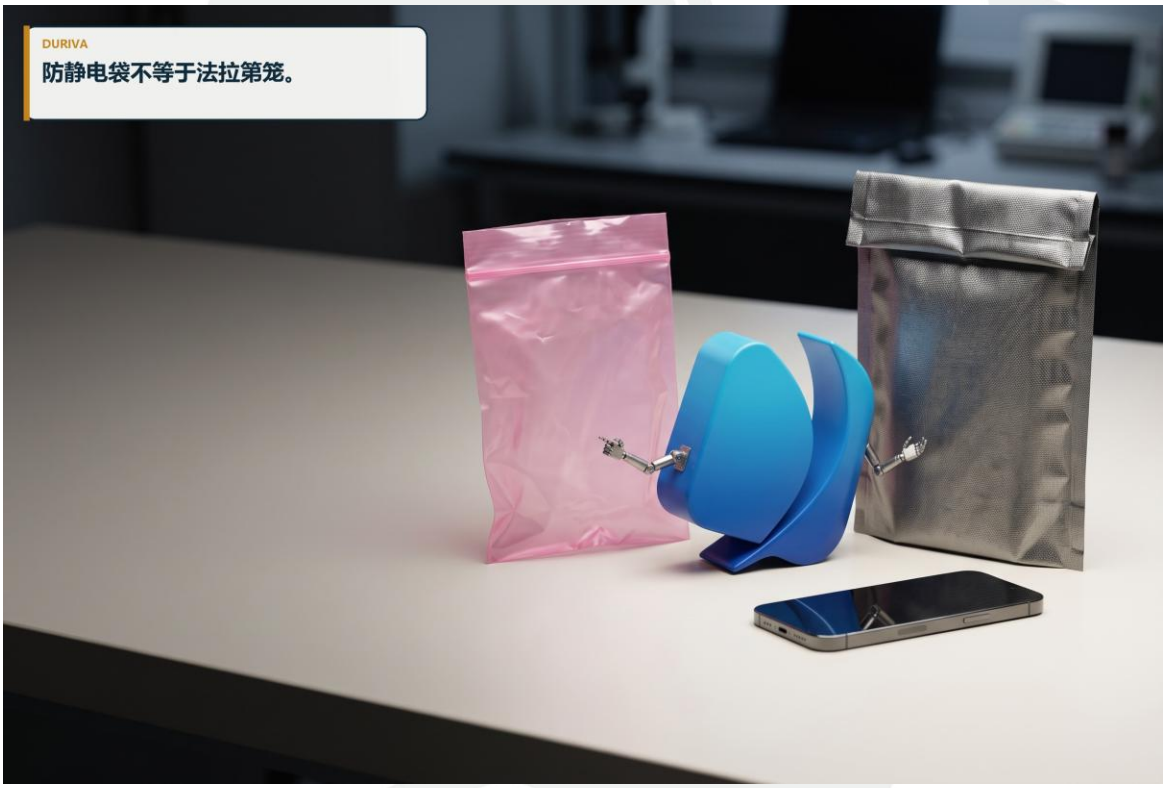


图36 静电防护与射频隔离具有不同功能。编辑重构；不构成真实证据。

12.3 数据源、截图和导出错误

没有 URL、日期、账户和语境的截图，就像撕下一页书后拍下的照片：可以阅读片段，却无法了解整本书。存在原生数据源时应予保存，同时记录截图路径、时间和获取人。如果只有可视化内容，就应如实说明，不能声称已检查完整历史。图像可以有用，但不能假装它就是全部。

导出时不记录筛选条件、时区、角色和字段字典，即使文件正确，也可能无法理解。只接收通话记录表的 PDF，却丢弃包含完整性声明的邮件，也会产生同样问题。稳健程序应要求原生格式、参数、生成过程、字段、局限、正文中的哈希值和交付 EML。这不是官僚主义，而是确定所持内容所必需的信息。



图37 没有 URL、日期、账户和语境，即使图像清晰，截图仍然不完整。编辑重构；不构成真实证据。

12.4 解读错误

不核查分配、会话、设备、共享和语境，就把 IP 地址归属于个人，是把网络数据误当作自然人身份。把天线当作住址，是把覆盖范围误当作在场证明。把日期视为不可改变或完全无用，是同一问题的两种表现：没有追问字段如何生成。严谨分析不会在轻信和轻视之间摇摆，而是根据生成机制和印证情况评价每个数据源。

合成内容检测器也需要同样谨慎。百分比本身不能识别作者、工具或行为。压缩、裁剪、重新录制和检测器训练都可能改变结果。应保存文件、版本、发布记录、历史和语境，比较不同方法，并说明假阳性和假阴性。线索可以引导数据源申请，但不能替代数据源。



图38 人工智能检测器提供带有局限的线索，不能替代文件、历史、语境和印证。编辑重构；不构成真实证据。

12.5 法律和时效错误

因措辞相似而建立等效关系，可能比不引用任何规范更危险。简单、高级、数字和合格签名在不同国家并不产生相同效力。银行规则不适用于所有企业，档案规范不能解决所有私人争议，提案也不是法令。有效引文应包含法律文件、条文、功能、适用范围、版本和官方来源；未核实的部分应予声明。

CNPCF 的过渡说明，在选择适用制度前必须审查相关宣告和修订。圣路易斯波托西州对人工智能专门规定的废止表明，一项备受讨论的修订也可能失效。本手册不试图冻结法律，而是教导如何在不丢失方法的情况下更新法律。案件发生时的法律版本必须复核并记录在变更控制中。[25][26]

[25]《国家民事和家庭诉讼法典》第 348–350 条。汇编包含 15-01-2026 的修订。逐步适用，并取决于相关宣告。官方在线来源

[26]圣路易斯波托西州。《议会公报》，30-07-2026：废止第 187 Ter 条以及包含第 272 Bis 和 272 Ter 条的章节。历史先例，并非现行规则。官方在线来源



图39 核实现行效力、适用范围和修订情况，避免把历史引文当作现行依据。编辑重构；不构成真实证据。

12.6 改变程序的经验教训

经验教训必须转化为可观察的改变。如果导出文件缺少时区，就修改申请以明确要求；如果混淆了两个对象，就复核标识符和照片；如果工具改变了格式，就更新验证和示例。只在异常文件夹中添加一句话而不改变程序，只会积累记录在案的懊悔。

复核应根据风险和环境变化安排，而不是机械遵循空泛日程。应检查官方来源、工具版本、供应商格式和存储条件。更新手册时，应替换适用内容并保留历史，而不是堆积相互矛盾的备注。历史记录不得修改，但现行程序可以改进。

虚构事件	后果	可验证的变更
附件缺少 EML	哈希声明和交付语境丢失。	接收清单要求提供 EML、附件并进行比较。

虚构事件	后果	可验证的变更
日期缺少时区	时间线可能使事件错位。	包含原始值、时区、转换和不确定性的模板。
更换封条但未记录	无法还原拆封过程。	必须记录拆封和重新封存事件。
结论超出发现	推论经不起质证。	审查前提和可作出陈述表。
规范已过时	适用已不再适当的效力。	结合来源和查询日期核实现行效力。

12.7 最终衡量标准：避免下一次滥用

本手册的目的不是培养会制造更多技术文书的人，而是让正确的接收避免基于错误对象的指控，让诚实的时间线避免基于不兼容时钟的定罪，让企业保存能够证明事件经过的记录，让个人理解为什么截图不足以及可以请求什么。技术只有减少任意性，才能成为服务。

开放双手并不意味着公开秘密或提供伤害指南，而是分享有尊严地工作的基础：识别、保护、提问、验证、承认局限和纠正。知识不应像拳头一样紧握，而应以方法交付，使他人能够做得更好，也使任何人类或技术权威都不必在本应提供验证的地方要求盲从。

手册结语

保全证据，就是保存查明真相的可能性。方法不承诺胜诉，只承诺陈述可以接受复核、错误可以得到承认、结论不会超出事实。

附录A 功能法律等效对照

研究法域：墨西哥、秘鲁、智利、阿根廷、哥伦比亚、厄瓜多尔和西班牙/欧盟。文献复核：2026 年 11 月 9 日。指导原则是功能等效，而不是规范同一。

执行摘要

本矩阵回答一个操作问题：在每个法域中，哪项规范承担本手册需要记录的功能。它不是从寻找相同条文编号或相似措辞开始。功能等效可以比较电子文件的法律认可、书面形式、归属、完整性、原始概念、可访问性、保存、可采性、评价和举证责任，以及行业性的日志和事件义务。两项规定可能追求相同目的，却具有不同推定、接收方、期限和后果，因此主题相似绝不能被表述为产生相同程序效力。

结果显示出共同但不统一的结构。墨西哥、哥伦比亚和厄瓜多尔对数据电文、书面形式、原件、完整性和保存有特别明确的规定；智利和阿根廷精确区分不同签名类别的效力；秘鲁的制度分布在第 27269 号法律及其条例、民事诉讼法典、档案规范和 SBS 监管之间；西班牙则结合 eIDAS、程序立法和支付服务规范。在所有情况下，电子形式本身都不足以证明作者身份、完整性或内容真实性。本手册必须要求来源、方法、语境、连续性和可验证性；哈希值有助于比较对象，但不能单独证明由谁创建文件或所叙述事件是否发生。

1. 比较方法与局限

本比较使用官方文本、法律汇编、官方公报和监管机关文件。每个条目都记录实际找到的法律文件和条文。“直接”表示该功能以类似结构得到明确覆盖；“部分”表示只覆盖一个方面或依赖其他规范；“行业性”表示规则限于档案、签名、支付或受监管实体；“未证实”表示调查未找到经过充分核实的一般规则。最后一类并不声称该国缺乏法律规范，而是不得根据现有证据虚构等效关系。

本比较有三个实际局限。第一，汇编可能在不同日期纳入修订，每起案件都必须核查事实和程序发生时适用的版本。第二，民事、商事、刑事、行政、档案和金融规则不能因术语相似而互换。第三，可采性、真实性、评价和举证责任是不同问题：规范可以允许提交文件，却不赋予

其完全证明力或倒置举证责任。因此，本矩阵用于指导技术记录和定位规范，不能替代案卷法律分析或司法结论。

级别	操作含义	手册引用规则
直接	该功能得到明确认可，并具有可比结构。	说明要求、例外和效力，不只复制条文措辞。
部分	规范仅覆盖部分功能，或需要其他程序规范补充。	引用补充法律文件，并明确哪些内容不在范围内。
行业性	规则仅限于档案、认证、支付或受监管实体。	不得将其扩展到全部数字证据或所有主体。
未证实	未找到经过充分验证的等效规定。	应写“本次复核未证实”，绝不能写“不存在”。

2. 按法律功能划分的核心矩阵

该表集中展示认可和形式功能。引文位于单元格内，使每项命题与来源保持关联。这些类别不评价法律体系优劣，只说明其对本手册的用途和已核实的对应程度。特别是，“原始”并不总要求保留物理设备；多项立法通过最终形式下的完整性和后续可访问性加以规定。本手册既要避免迷信介质，也要避免以为截图保留了源文件的全部属性。

当一个单元格结合多项规范时，说明功能是分散的，不能全部归于首先提及的法律文件。秘鲁尤其具有说明性：第 27269 号法律规范数字签名和证书，但其本身并不包含数据电文原件和保存的一般制度。数字签名文件的采纳见于其条例，缩微载体的保存则有专门档案制度。区分这些来源，可以避免构建优雅却虚假的等效关系。

电子文件的认可

法域	规则、范围和局限
墨西哥	CCom 89 和 89 Bis：中立性，不因数据电文形式而否定。
秘鲁	第 27269 号法律第 1–2 条，用于电子签名；范围特定，并非完整文件制度。
智利	第 19.799 号法律第 1–3 条：介质等效和效力，含排除事项。
阿根廷	第 25.506 号法律第 1、3 和 6 条，涉及数字签名和数字文件。
哥伦比亚	第 527 号法律第 5 条：不得因属于数据电文而否定其效力。
厄瓜多尔	第 67 号法律第 2 条：与书面文件具有同等法律价值，但受该法律及其条例约束。
西班牙 / 欧盟	eIDAS 第 46 条：不得仅因电子格式而否定其效力或可采性。

表格来源： 27282930313233

[27]墨西哥《商法典》第 89–94 和 1205 条：中立性、归属、书面形式、原件、完整性、可访问性和数据电文采纳。官方汇编。官方在线来源

[28]秘鲁。第 27269 号《数字签名和证书法》及 DS 052-2008-PCM 号条例。数字签名和数字签名文件采纳的专门制度。官方在线来源

[29]智利。关于电子文件和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级签名、日期和证据效力。官方在线来源

[30]阿根廷。第 25.506 号《数字签名法》，第 1 和 5–9 条：数字文件、援引遭否认电子签名时的举证责任，以及有限范围的推定。官方在线来源

[31]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。官方在线来源

[32]厄瓜多尔。《电子商务、电子签名和数据电文法》，第 67 号法律，第 2、6–8、10–16 条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。官方在线来源

[33]《（UE）910/2014 号 eIDAS 条例》，第 25–26 和 46 条：不得因电子签名和文件的格式而加以歧视，高级电子签名及合格电子签名的效力。官方在线来源

书面形式与后续可访问性

法域	规则、范围和局限
墨西哥	CCom 93 和 93 Bis；CNPCF 349 要求可访问性。
秘鲁	052-2008-PCM 号条例第 3 条规定签名要求；档案可访问性另行规定。
智利	第 19.799 号法律第 2.d 条要求适当存储以供后续使用；第 3 条规定书面形式。
阿根廷	第 25.506 号法律第 6 条：数字文件满足书面形式要求；第 182/2019 号法令规定保存。
哥伦比亚	第 527 号法律第 6 条：数据电文可供后续查阅。
厄瓜多尔	第 67 号法律第 6 条：信息可供后续查阅。
西班牙 / 欧盟	eIDAS 未规定与 93 Bis 完全相同的通用规则；LSSI 和行业规范提供补充。属于部分等效，不得强行对应。

表格来源： 343536373839

[34]《国家民事和家庭诉讼法典》第 348–350 条。汇编包含 15-01-2026 的修订。逐步适用，并取决于相关宣告。官方在线来源

[35]秘鲁。IOFE 条例，DS 052-2008-PCM，第 3 和 4 条：经数字签名的电子文件的要求与认可。官方在线来源

[36]智利。关于电子文件和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级签名、日期和证据效力。官方在线来源

[37]阿根廷。第 182/2019 号法令：在规定期限和条件下进行数字保存和制作经认证副本。官方在线来源

[38]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。官方在线来源

[39]厄瓜多尔。《电子商务、电子签名和数据电文法》，第 67 号法律，第 2、6–8、10–16 条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。官方在线来源

归属与签名

法域	规则、范围和局限
墨西哥	CCom 90–92；CNPCF 349；根据可靠且可归因的方法产生推定。
秘鲁	第 27269 号法律第 3 条及其条例第 3–4 条；IOFE 中的数字签名和签名文件的采纳。
智利	第 19.799 号法律第 2.f–g 和 4–5 条：简单和高级电子签名不具有相同效力。
阿根廷	第 25.506 号法律第 5、7–9 条：援引遭否认电子签名时的举证责任；有效数字签名的推定。
哥伦比亚	第 527 号法律第 7、16–17 和 28 条：可靠方法、归属和数字签名属性。
厄瓜多尔	第 67 号法律第 10、13–16 条：电子签名的来源、身份和效力。
西班牙 / 欧盟	eIDAS 第 25–26 条：不歧视简单电子签名；合格电子签名等同于手写签名；高级电子签名的要求。

表格来源： 40414243444546

原件与最终形式下的完整性

法域	规则、范围和局限
墨西哥	CCom 93 Bis 和 CNPCF 350：最终生成后的完整性和可访问性；第 350 条另有公共链特殊规则。
秘鲁	第 27269 号法律中未证实存在通用规则。缩微载体和档案完整性在 DL 681 和 DS 001-2000-JUS 中有专门制度。
智利	第 19.799 号法律第 2.g 条要求高级签名能够检测改动；第 5 条根据文件类别确定效力。部分等效。
阿根廷	第 25.506 号法律第 8 条：数字验证为真时推定完整性。直接适用于数字签名，并非适用于所有文件。
哥伦比亚	第 527 号法律第 8–9 条：自最终形式形成及出示时提供可靠的完整性保障。
厄瓜多尔	第 67 号法律第 7 条：验证最终形式下的完整性；其条例第 6 条。

[40]《国家民事和家庭诉讼法典》第 348–350 条。汇编包含 15-01-2026 的修订。逐步适用，并取决于相关宣告。官方在线来源

[41]秘鲁。IOFE 条例，DS 052-2008-PCM，第 3 和 4 条：经数字签名的电子文件的要求与认可。官方在线来源

[42]智利。关于电子文件和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级签名、日期和证据效力。官方在线来源

[43]阿根廷。第 25.506 号《数字签名法》，第 1 和 5–9 条：数字文件、援引遭否认电子签名时的举证责任，以及有限范围的推定。官方在线来源

[44]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。官方在线来源

[45]厄瓜多尔。《电子商务、电子签名和数据电文法》，第 67 号法律，第 2、6–8、10–16 条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。官方在线来源

[46]《（UE）910/2014 号 eIDAS 条例》，第 25–26 和 46 条：不得因电子签名和文件的格式而加以歧视，高级电子签名及合格电子签名的效力。官方在线来源

法域	规则、范围和局限
西班牙 / 欧盟	eIDAS 第 26.d 条将数据关联以便检测改动；LEC 326 规定对真实性和完整性的质疑。属于部分、程序性等效。

表格来源： 47484950515253

保存及来源、目的地和日期语境

法域	规则、范围和局限
墨西哥	NOM-151 用于保存和数字化；CCom 93 Bis 用于可访问性。
秘鲁	DS 001-2000-JUS 用于缩微载体；IOFE 条例用于签名和证书。行业性。
智利	第 19.799 号法律第 2.d 和 5 条：后续使用，以及高级签名私人文件经认证日期的证明。
阿根廷	第 182/2019 号法令第 5 条：在特定期限内进行数字保存和制作经认证副本。

[47]《国家民事和家庭诉讼法典》第 348–350 条。汇编包含 15-01-2026 的修订。逐步适用，并取决于相关宣告。官方在线来源

[48]秘鲁。DL 681 和 DS 001-2000-JUS：先进技术、缩微载体、真实性、完整性和档案保存。行业范围。官方在线来源

[49]智利。关于电子文件和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级签名、日期和证据效力。官方在线来源

[50]阿根廷。第 25.506 号《数字签名法》，第 1 和 5–9 条：数字文件、援引遭否认电子签名时的举证责任，以及有限范围的推定。官方在线来源

[51]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。官方在线来源

[52]厄瓜多尔。《电子商务、电子签名和数据电文法》条例：附件纳入、非实体化、完整性和验证。司法机构发布的官方来源。官方在线来源

[53]西班牙。《民事诉讼法》第 326 和 384 条：私人文件、质疑、用于归档、了解或复制数据的措施、检查、保管和合理审查。官方在线来源

法域	规则、范围和局限
哥伦比亚	第 527 号法律第 12–13 条：格式、准确复制、来源、目的地、日期和时间；第三方。
厄瓜多尔	第 67 号法律第 8 条：可访问性、格式、来源、目的地、日期、时间和完整性；第三方。
西班牙 / 欧盟	行业和保存规范；本次复核未证实存在与第 527.12 条完全对应的单一通用条款。

表格来源： 545556575859

可采性与证据评价

法域	规则、范围和局限
墨西哥	CCom 1205 采纳数据电文；CFPC 210-A 和 CNPCF 348–350 规定可靠性、归属、可访问性和完整性。
秘鲁	CPC 188–197：目的、合法性、典型/非典型证据和举证责任；其条例第 4 条适用于数字签名文件。

[54]NOM-151-SCFI-2016，数据电文的保存和数字化，发布于 30-03-2017。关于记录、完整性、可访问性和电子数字指纹的要求。官方在线来源

[55]秘鲁。DL 681 和 DS 001-2000-JUS：先进技术、缩微载体、真实性、完整性和档案保存。行业范围。官方在线来源

[56]智利。关于电子文件和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级签名、日期和证据效力。官方在线来源

[57]阿根廷。第 182/2019 号法令：在规定期限和条件下进行数字保存和制作经认证副本。官方在线来源

[58]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。官方在线来源

[59]厄瓜多尔。《电子商务、电子签名和数据电文法》，第 67 号法律，第 2、6–8、10–16 条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。官方在线来源

法域	规则、范围和局限
智利	第 19.799 号法律第 5 条：在规定情形下具有完全证明力；其他文件适用一般规则。
阿根廷	CCyC 318–319：允许以任何方式通信，并评价介质和程序的可靠性。
哥伦比亚	第 527 号法律第 10–11 条：可采性、合理审查、生成、归档、传输、完整性和发起人。
厄瓜多尔	第 67 号法律第 14 条：电子签名可被采纳为证据；第 2 和 7 条对效力和原件提出要求。
西班牙 / 欧盟	eIDAS 第 46 条及 LEC 326/384：采纳、质疑、信任服务和合理审查。

表格来源： 60616263646566

[60]《联邦民事诉讼法典》第 210-A 条：电子信息方法的可靠性、归属、可访问性和完整性。该法典由 07-06-2023 的法令废止，适用渐进过渡制度。官方在线来源

[61]秘鲁。《民事诉讼法典》第 188–197 和 245.5 条：目的、合法性、证据、举证责任、评价和通过技术手段确定日期。官方在线来源

[62]智利。关于电子文件和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级签名、日期和证据效力。官方在线来源

[63]阿根廷。《民商法典》第 318–319 条：允许以任何方式通信，并评价介质和技术程序的可靠性。官方在线来源

[64]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。官方在线来源

[65]厄瓜多尔。《电子商务、电子签名和数据电文法》，第 67 号法律，第 2、6–8、10–16 条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。官方在线来源

[66]西班牙。《民事诉讼法》第 326 和 384 条：私人文件、质疑、用于归档、了解或复制数据的措施、检查、保管和合理审查。官方在线来源

举证责任与推定

法域	规则、范围和局限
墨西哥	不能仅因文件存在就推定作者身份；必须证明方法及其归属。
秘鲁	CPC 196：除另有规定外，由主张其请求所依据事实的人，或以新事实提出抗辩的人承担举证责任。
智利	效力取决于文书和签名类别；私人文件日期须关注经认证的日期。
阿根廷	第 25.506 号法律第 5、7–8 条：援引遭否认电子签名时的举证责任；推定仅适用于其制度。
哥伦比亚	第 527 号法律第 17、21 和 28 条：对来源、接收和签署意图的有限推定。
厄瓜多尔	第 67 号法律第 10 条：除有相反证据和例外情况外推定来源；不自动证明自然人作者身份。
西班牙 / 欧盟	LEC 326.4：在其规定条件下，存在合格服务时，推定受质疑特征及正确履行。

表格来源： 6768697071

[67]秘鲁。《民事诉讼法典》第 188–197 和 245.5 条：目的、合法性、证据、举证责任、评价和通过技术手段确定日期。官方在线来源

[68]阿根廷。第 25.506 号《数字签名法》，第 1 和 5–9 条：数字文件、援引遭否认电子签名时的举证责任，以及有限范围的推定。官方在线来源

[69]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。官方在线来源

[70]厄瓜多尔。《电子商务、电子签名和数据电文法》，第 67 号法律，第 2、6–8、10–16 条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。官方在线来源

[71]西班牙。《民事诉讼法》第 326 和 384 条：私人文件、质疑、用于归档、了解或复制数据的措施、检查、保管和合理审查。官方在线来源

3. 墨西哥：法律基础与过渡

墨西哥为本手册提供了完整体系，但必须区分现行商事制度、历史 CFPC 和 CNPCF 的逐步施行。CFPC 第 210-A 条承认通过电子、光学或其他技术生成或传输的信息可以作为证据，并要求评价方法可靠性、归属和可访问性；其原件以最终形式下的完整性为基础。《商法典》包含电子商务的实体架构：第 89 和 89 Bis 条规定中立性和不歧视；第 90–92 条规定归属、发送、接收和回执；第 93 和 93 Bis 条规定书面形式、原件、完整性和可访问性；第 94 条规定发出和接收地点。第 1205 条已在官方汇编中直接核实，除其他介质外，还采纳照片、视频、声音和数据电文。[72]

所查阅的 CNPCF 官方汇编显示最近一次修订为 2026 年 1 月 15 日。第 348–350 条具有类似结构，并增加区块链等技术。第 350 条还对公共链记录规定了特殊证明规则，但以其未证明受到破坏或缺乏可靠性为条件，不能据此笼统声称任何分布式记录都是真实的。过渡是渐进的，并取决于相关宣告。所查汇编保留了 2027 年 4 月 1 日的一般期限；2026 年 4 月 29 日《议会公报》公布的一项提案曾建议将其改为 2030 年 1 月 31 日，但提案不是已颁布法令。将该过渡适用于真实案件之前，必须核查 DOF 是否此后发布修订，以及相应司法机关适用哪项宣告。[73][74]

法律文件	已验证的功能	手册必须保留的精确说明
CFPC 210-A	电子信息作为证据；可靠性、归属、可访问性和完整性。	这是过渡的历史基础，不是简单更换编号的条文。
CNPCF 348–350	认可、可靠性、原件、可访问性和公共链规则。	逐步施行；案件发生时应核查相关宣告和修订。

[72]墨西哥《商法典》第 89–94 和 1205 条：中立性、归属、书面形式、原件、完整性、可访问性和数据电文采纳。官方汇编。官方在线来源

[73]《国家民事和家庭诉讼法典》第 348–350 条。汇编包含 15-01-2026 的修订。逐步适用，并取决于相关宣告。官方在线来源

[74]众议院。《议会公报》，29-04-2026。提案建议将 CNPCF 的生效日期修改为 31-01-2030。这是提案，不是已颁布法令。官方在线来源

法律文件	已验证的功能	手册必须保留的精确说明
CCom 89–94	中立性、效力、归属、发送/接收、书面形式、原件和地点。	不得把接收回执与内容真实性或任何语境下的有效同意混为一谈。
CCom 1205	明确采纳数据电文和其他介质。	可采不等于完全证明力，也不排除质证和鉴定。
NOM-151-SCFI-2016	保存、数字化、经认可的 PSC、指纹、RFC 3161、记录和可访问性。	这是其适用范围内保存/数字化的技术要求，不是作者身份或内容真实性的神奇证明。
CNBV 316 Bis 及相关条款系列	凭证、通知、加密、访问、事件、异常、日志和复核。	每条规定的接收方、对象和期限不同，不得把“316 Bis”当作单一义务引用。

表格来源： 7576777879

NOM-151 应与程序规则分开，单独进行技术处理。其用途在于保存和核实数据电文以及数字化条件，而不是声称存储的一切都是真实。经济部的标准化页面将其标为现行有效，DOF 文本则规定记录、完整性和可访问性要求。本手册应记录工具、版本、算法、日期和时区、操作员

[75]《联邦民事诉讼法典》第 210-A 条：电子信息方法的可靠性、归属、可访问性和完整性。该法典由 07-06-2023 的法令废止，适用渐进过渡制度。官方在线来源

[76]《国家民事和家庭诉讼法典》第 348–350 条。汇编包含 15-01-2026 的修订。逐步适用，并取决于相关宣告。官方在线来源

[77]墨西哥《商法典》第 89–94 和 1205 条：中立性、归属、书面形式、原件、完整性、可访问性和数据电文采纳。官方汇编。官方在线来源

[78]NOM-151-SCFI-2016，数据电文的保存和数字化，发布于 30-03-2017。关于记录、完整性、可访问性和电子数字指纹的要求。官方在线来源

[79]适用于信贷机构的一般性规定，第 316 Bis、316 Bis 1、316 Bis 10 至 17 条：凭证、加密、访问、事件、异常、日志和复核。官方在线来源

身份，以及原件、副本和记录之间的关系。不得承诺时间戳或记录本身就能解决自然人作者身份、获取合法性或对话完整性问题。[8081]

CNBV 规定可细分如下：316 Bis 规定凭证；316 Bis 1 规定通知；316 Bis 10 规定加密和保护；316 Bis 11 规定访问控制；316 Bis 12 规定事件调查和通知，并须在五个自然日内向委员会报告；316 Bis 14 规定异常和未经认可的操作，保存五年；316 Bis 15 规定日志安全保存 180 天，并在十个工作日内响应用户申请；316 Bis 17 规定至少每年进行安全复核。这些期限不能套用到其他国家或所有类型的企业。鉴定时应申请与相关操作和期间有关的日志，而不是笼统要求“所有服务器”。[82]

4. 秘鲁：分散制度与金融监管更新

分析秘鲁时，必须放弃以单一法律规范全部数据电文的想法。第 27269 号法律经第 27310 号法律修订，规范数字签名和证书；经审阅的官方文本共 16 条。第 1 条承认电子签名，第 2 条界定范围，第 3 条通过非对称密码学定义数字签名。DS 052-2008-PCM 批准的条例发展了 IOFE，其第 3 和 4 条规定该基础设施生成的数字签名的等效性，以及经数字签名的电子文件作为证据的采纳。该规范本身承认电子签名的多样性，不能把任何插入的符号或图像都当作经认可的数字签名。[8384]

在程序方面，《民事诉讼法典》第 188–197 条规定一般规则：目的、时机、相关性、合法性、典型和非典型证据、职权取证、举证责任和评价。第 192 条列举当事人陈述、证人、文件、鉴定和司法检查；第 193 条允许将技术或科学辅助作为非典型证据；第 196 条除另有规定外分配举证责任。第 245.5 条允许法官将能够使其形成确信的技术手段所确定的日期视为确定日期。

---

[80]NOM-151-SCFI-2016，数据电文的保存和数字化，发布于 30-03-2017。关于记录、完整性、可访问性和电子数字指纹的要求。官方在线来源

[81]经济部。PLATIICA。NOM-151-SCFI-2016 数据电文保存和数字化条目。用于核实现行效力，并作为 DOF 文本的补充参考。官方在线来源

[82]适用于信贷机构的一般性规定，第 316 Bis、316 Bis 1、316 Bis 10 至 17 条：凭证、加密、访问、事件、异常、日志和复核。官方在线来源

[83]秘鲁。第 27269 号《数字签名和证书法》及 DS 052-2008-PCM 号条例。数字签名和数字签名文件采纳的专门制度。官方在线来源

[84]秘鲁。IOFE 条例，DS 052-2008-PCM，第 3 和 4 条：经数字签名的电子文件的要求与认可。官方在线来源

档案方面，DL 681 和 DS 001-2000-JUS 涵盖相关技术和缩微载体、真实性、完整性和保存；其范围不能与任何私人文件通用的原件规则混淆。[8586]

秘鲁议题	有用规则	操作警示
SBS 504-2021，第 12.6.g 条	为事件后的取证调查保全证据。	将其落实为有记录的程序，而不是不加区分地收集。
SBS 504-2021，第 15 条	重大事件报告和取证分析，供监管局调阅。	报告应包含执行摘要和技术细节。
SBS 504-2021，第 17.3–17.4 条	维护和保护注册、身份验证尝试和操作记录；监测交易。	这些记录对重建序列和身份验证尤其重要，但不能自动证明自然人身份。
SBS 2286-2024，新第 20.3 条	企业对某些未经认可的操作承担责任，除非其能够证明责任在用户。	这是对 504-2021 的正确修订；不得引用错误编号，也不得把旧文本当作未变版本。

表格来源：[8788]

金融比较必须反映 2024 年的这次更新。修订后的第 20.3 条涵盖某些数字渠道中未经认可且无须强化身份验证的操作，包括特定豁免情形，或用户报告凭据被窃或遗失后的操作，但能够证明责任在用户的除外。这并不等于银行总是负责，也不等于使用凭据总能证明授权。鉴定必须审查验证因素、注册、日志、警报、设备语境和序列，并将技术事实与操作发生时的现行规则联系起来。[89]

[85]秘鲁。《民事诉讼法典》第 188–197 和 245.5 条：目的、合法性、证据、举证责任、评价和通过技术手段确定日期。官方在线来源

[86]秘鲁。DL 681 和 DS 001-2000-JUS：先进技术、缩微载体、真实性、完整性和档案保存。行业范围。官方在线来源

[87]秘鲁。SBS 504-2021，第 12.6.g、15 和 17.3–17.4 条：保全、报告和取证分析，注册、身份验证和操作记录。官方在线来源

[88]秘鲁。SBS 2286-2024：修订第 20.3 条有关某些未经认可操作和责任的规定，但能够证明责任在用户的除外。官方在线来源

[89]秘鲁。SBS 2286-2024：修订第 20.3 条有关某些未经认可操作和责任的规定，但能够证明责任在用户的除外。官方在线来源

5. 智利：签名、日期与安全监管

智利国家国会图书馆汇编中的第 19.799 号现行法律规范电子文件及其效力。第 1 条规定介质等效，第 2 条定义文件和签名，第 3 条承认形式和效力并规定排除事项，第 4 条要求公共文书使用高级电子签名，第 5 条区分证明力。带高级签名的私人文件共享法律规定的完全证明制度，但除非由经认可的服务提供商提供电子日期，否则其日期不具证明力。带非高级电子签名的文件按一般规则评价。这一区分可以避免两种错误：否认简单签名的一切价值，或自动赋予其高级签名的价值。[90]

在银行领域，《规范汇编》区分第 20-10 章“信息安全与网络安全管理”和第 20-9 章“业务连续性”。第 20-7 章规范外包，要求保密、完整、可追溯和可用，并要求能够及时向主管机关提供所需日志和信息。第 20-8 章涉及运营事件信息。对本手册而言，功能等效应通过控制和可用证据表述，不能声称某一章复制了 316 Bis。确定期限或最低内容之前，应申请现行规范并确认实体适用范围。[91]

案件需要	智利功能依据	注意事项
文件和签名归属	第 19.799 号法律第 2–5 条。	区分形式识别、高级签名和证明效力。
证明私人文件的日期	第 19.799 号法律第 5.2 条。	仅凭高级签名不足以证明日期。
审查供应商/云服务和日志	RAN 20-7 和 20-10；事件适用 20-8。	不得混淆业务连续性、外包和网络安全。

表格来源：[92][93]

[90]智利。关于电子文件和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级签名、日期和证据效力。官方在线来源

[91]智利。《规范汇编》第 20-7、20-8 和 20-10 章：外包、运营事件、信息安全和网络安全。官方在线来源

[92]智利。关于电子文件和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级签名、日期和证据效力。官方在线来源

[93]智利。《规范汇编》第 20-7、20-8 和 20-10 章：外包、运营事件、信息安全和网络安全。官方在线来源

6. 阿根廷：有限推定与介质可靠性

第 25.506 号法律承认电子签名和数字签名具有不同效力。第 5 条将缺少某项数字签名要求的签名定义为电子签名；如遭否认，援引者须证明其有效性。第 7 和 8 条在法定条件下推定数字签名的作者身份和完整性，第 9 条规定有效性，第 6 条承认书面形式。第 182/2019 号法令规范保存和经认证副本。第 27.446 号法律废止了原第 25.506 号法律第 4 条并替换其他规定，因此本附录不得把历史排除条款复制为现行文本。[949596]

《民商法典》提供通用证据规则。第 318 条允许提交以任何方式创建或传输的通信，但对机密通信设有限制。第 319 条要求评价私人文书时权衡一致性、技术清晰度、惯例、先前关系以及介质和技术程序的可靠性。本手册可以将这些标准转化为具体问题：哪个系统生成记录、谁管理密钥、可以实施哪些更改、如何导出、序列是否一致，以及是否存在独立印证。密码学完整性推定本身不能回答这些语境问题。[97]

BCRA 监管	功能	与墨西哥的差异
A 7783 号通告	交易记录以数字格式至少保存 90 天；特定消息服务须实时记录；监测。	期限和范围各不相同；不得用墨西哥的 180 天替代。
A 8280 号通告	网络事件响应与恢复；遏制、恢复和解决后五天内提交最终报告。	起算取决于规范描述的事件，与 CNBV 通知并不相同。

表格来源：[9899]

[94]阿根廷。第 25.506 号《数字签名法》，第 1 和 5–9 条：数字文件、援引遭否认电子签名时的举证责任，以及有限范围的推定。官方在线来源

[95]阿根廷。第 27.446 号法律：废止原第 25.506 号法律第 4 条并替换其他规定。不得将历史文本作为现行引用。官方在线来源

[96]阿根廷。第 182/2019 号法令：在规定期限和条件下进行数字保存和制作经认证副本。官方在线来源

[97]阿根廷。《民商法典》第 318–319 条：允许以任何方式通信，并评价介质和技术程序的可靠性。官方在线来源

[98]阿根廷。BCRA A 7783 号通告：数字交易记录至少保存 90 天，并监测安全事件。官方在线来源

[99]阿根廷。BCRA A 8280 号通告：网络事件响应与恢复；遏制、恢复和解决后五天内提交最终报告。官方在线来源

7. 哥伦比亚：数据电文、保存与回执

1999 年第 527 号法律与墨西哥模式具有非常清晰的功能对应关系。第 5 条防止因电子形式而否定效力；第 6 条涵盖书面形式和可访问性；第 7 条规定以可靠且适当的方法签署；第 8–9 条涉及原件和完整性；第 10–11 条涉及可采性和评价；第 12–13 条涉及自行或通过第三方保存；第 16–25 条涉及归属、发送、接收、回执、副本、时间和地点。第 28 条规定数字签名属性。第 12 条要求保存能够确定来源、目的地、日期和时间的信息，导出和保管格式必须纳入这一要素。[100]

CPACA 为行政行为提供规则。第 57–58 条要求电子行为和档案的真实性、完整性和可用性；第 61 条要求对所收文件进行控制，并记录日期、时间、安全和回执；第 62 条规定发送/接收证明和服务故障记录。这些规定不替代第 527 号法律，而是适用于行政程序。金融领域找到了 2020 年第 033 号外部通函，作为安全和网络安全指令文件，但所取得的来源无法可靠确定其全部操作条款编号。为保持严谨，本矩阵未赋予其未经阅读的期限或文字要求。[101][102]

应用	文件规则	建议的最低记录
原始消息	第 527 号法律第 8–9 条。	原生格式对象、完整性、生成过程和展示方式。
保存	第 527 号法律第 12–13 条。	格式、来源、目的地、日期、时间、保管人和相关第三方。
行政接收	CPACA 61–62。	登记编号、回执、日期/时间，以及任何故障的可验证记录。
金融网络安全	SFC 发布的 2020 年 CE 033。	施加具体义务前，确认条款编号和官方版本。

[100]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。官方在线来源

[101]哥伦比亚。CPACA 第 57–58、61 和 62 条：电子行为和档案的真实性、完整性、回执和服务故障记录。官方在线来源

[102]哥伦比亚。金融监管局。2020 年第 033 号外部通函，确认为安全和网络安全指令；施加具体义务前必须核实条款编号。官方在线来源

8. 厄瓜多尔：文件等效与支付系统

《电子商务、电子签名和数据电文法》（第 67 号法律）明确规定了核心功能。第 2 条承认数据电文依法律及条例具有同等法律价值；第 6 条涵盖可访问的书面信息；第 7 条涉及原件和完整性；第 8 条涉及保存格式、可访问性、来源、目的地、日期、时间和完整性；第 10 条涉及来源和身份及其推定与例外；第 11 条涉及发送和接收；第 13–14 条涉及电子签名的定义和效力。其条例进一步规定附件纳入、非实体化、完整性和验证。第 10 条的推定并不允许自动识别操作设备的自然人，仍需分析验证、通知和接收方的审慎程度。[103][104]

在金融领域，2025 年 8 月 18 日《官方公报》第 104 号增刊发布的 JPRM-2025-006-M 号决议规范支付系统。第 77–79 条涉及运营、有效性、清算和结算；第 82 条要求分别列示钱包资金和交易，并保持持续可用；后续条款规定参与者和监督。该文件有助于理解支付系统的记录和确认，但不能证明其与 CNBV 具有相同的日志、保存和事件义务。本手册必须将这一等效标为行业性和部分等效，并在推断责任之前申请实体和渠道的适用制度。[105]

需要	厄瓜多尔依据	局限
保存消息和元数据	第 67 号法律第 8 条。	如果丢失格式和来源数据，仅供查看的 PDF 并不足够。
消息归属	第 67 号法律第 10、13–14 条。	签名和来源本身不能识别自然人，也不能证明全部事实。
重建电子支付	JPRM-2025-006-M 号决议。	支付系统制度，并非 CNBV 全部义务的通用等效制度。

[103]厄瓜多尔。《电子商务、电子签名和数据电文法》，第 67 号法律，第 2、6–8、10–16 条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。官方在线来源

[104]厄瓜多尔。《电子商务、电子签名和数据电文法》条例：附件纳入、非实体化、完整性和验证。司法机构发布的官方来源。官方在线来源

[105]厄瓜多尔。JPRM-2025-006-M 号决议，《官方公报》第 104 号增刊，18-08-2025：支付系统的运营、有效性、清算、结算和资金可用性。官方在线来源

9. 西班牙与欧盟：不歧视、信任服务与程序

西班牙需要结合欧盟法律和程序法。eIDAS 第 25 条禁止仅因签名是电子形式或不属于合格签名而否定其效力或可采性；合格电子签名具有与手写签名同等的效力；第 26 条规定高级电子签名要求；第 46 条禁止因文件格式而否定其效力和可采性。第 6/2020 号法律规范特定电子信任服务，并废止第 59/2003 号法律和 LSSI 第 25 条。因此，将旧《电子签名法》作为现行法律引用属于更新错误。功能等效集中于不歧视、签名级别和信任服务，而不是照搬墨西哥的结构。[106][107]

2026 年 10 月 7 日更新的 LEC 合并文本区分真实性和证据评价。第 326 条规范私人文件及其质疑；第 3 和 4 款涉及电子文件以及非合格和合格信任服务，并在规定情形下设置推定。第 384 条规范用于归档、了解或复制数据的措施：各方参与的检查、记录和保管，以及按合理审查原则进行评价。该法律本身允许质疑真实性、完整性、日期和时间的准确性或其他特征。因此，提交电子文件并不会终结技术争论，而是提供可验证、可质证的对象，使争论得以展开。[108]

支付服务	西班牙规则	技术应用
RD-ley 19/2018，第 45 条	对未经授权操作的返还，须符合规定条件和例外，包括以书面形式通报有理由怀疑的欺诈。	区分法律上的未授权与仅对设备或凭据存在分歧。
第 66 条	风险管理框架、控制措施和事件管理/分类程序；至少每年评估一次。	申请相关评估和控制记录，不得假设其证明某次具体操作。

[106]《（UE）910/2014 号 eIDAS 条例》，第 25–26 和 46 条：不得因电子签名和文件的格式而加以歧视，高级电子签名及合格电子签名的效力。官方在线来源

[107]西班牙。第 6/2020 号《电子信任服务法》：废止第 59/2003 号法律和 LSSI 第 25 条；不得将旧制度作为现行引用。官方在线来源

[108]西班牙。《民事诉讼法》第 326 和 384 条：私人文件、质疑、用于归档、了解或复制数据的措施、检查、保管和合理审查。官方在线来源

支付服务	西班牙规则	技术应用
第 67 条	严重事件须立即通知西班牙银行；影响或可能影响用户利益时，不得不当拖延向用户提供信息。	保存检测、分类、通知和缓解措施的时间线。

表格来源：[109]

10. 金融日志与事件的功能比较

下表避免一种常见简化：把任何网络安全规范都当作第 316 Bis 及后续条文的“等效规定”。实际上存在多种功能：出具凭证、通知用户、控制访问、记录身份验证、保存日志、调查事件、向监管机关报告，以及分配未经认可操作的责任。一个法域可能通过不同法律文件分别覆盖这些功能。鉴定必须先列出所需数据，再定位其法律依据，不能一开始就笼统申请“所有现存日志”。

此处刻意只列出少数与所读文本直接相关的期限。不会把墨西哥的 180 天套用于阿根廷，也不会把 CNBV 的五个自然日套用于秘鲁或西班牙。未核实的期限不作编造。为了证据保存，本手册可以建议立即保全副本并向保管人申请数据，无需等到最低保存期限届满，因为法定保存不能保证无限期可用，也不能保证覆盖所有相关事件。

墨西哥

法域	规则、范围和局限
日志/身份验证	CNBV 316 Bis 11 和 15：访问和日志。
事件	316 Bis 12：调查和通知。
未经认可的操作	316 Bis 14：异常和未经认可的操作。

[109]西班牙。第 19/2018 号皇家法令，第 45、66 和 67 条：未经授权操作的返还、风险管理和严重事件立即通知。官方在线来源

法域	规则、范围和局限
已核实的期限和范围	316 Bis 15 的日志为 180 天；316 Bis 14 为五年；316 Bis 12 的通知为五个自然日，分别适用于各自范围。

表格来源：[110]

秘鲁

法域	规则、范围和局限
日志/身份验证	SBS 504-2021 第 17.3–17.4 条：注册、尝试和操作；监测。
事件	第 12.6.g 和 15 条：保全、报告和取证分析。
未经认可的操作	SBS 2286-2024 修订第 20.3 条；除能证明责任在用户外，企业承担责任。
已核实的期限和范围	不得外推单一期限；应阅读适用规则和修订。

表格来源：[111]

智利

法域	规则、范围和局限
日志/身份验证	RAN 20-10；外包和日志适用 20-7。
事件	RAN 20-8。
未经认可的操作	需要产品和渠道的具体规范。

[110]适用于信贷机构的一般性规定，第 316 Bis、316 Bis 1、316 Bis 10 至 17 条：凭证、加密、访问、事件、异常、日志和复核。官方在线来源

[111]秘鲁。SBS 2286-2024：修订第 20.3 条有关某些未经认可操作和责任的规定，但能够证明责任在用户的除外。官方在线来源

法域	规则、范围和局限
已核实的期限和范围	不得采用未经核实的期限。

表格来源： [112]

阿根廷

法域	规则、范围和局限
日志/身份验证	BCRA A 7783：交易和安全事件。
事件	BCRA A 8280：响应、恢复和最终报告。
未经认可的操作	适用渠道和用户规范；不得仅凭身份验证推断。
已核实的期限和范围	A 7783 要求数字日志至少保存 90 天；A 8280 规定情形下须在五天内提交最终报告。

表格来源： [113]

哥伦比亚

法域	规则、范围和局限
日志/身份验证	第 527 号法律用于一般保存；SFC 用于监管。
事件	2020 年 CE 033 被确认为该领域的指令。
未经认可的操作	本次复核未证实存在充分的文字规则。
已核实的期限和范围	使用期限或必填字段前，确认条款编号和官方文本。

[112]智利。《规范汇编》第 20-7、20-8 和 20-10 章：外包、运营事件、信息安全和网络安全。官方在线来源

[113]阿根廷。BCRA A 7783 号通告：数字交易记录至少保存 90 天，并监测安全事件。官方在线来源

表格来源：[114]

厄瓜多尔

法域	规则、范围和局限
日志/身份验证	第 67.8 条适用于消息；JPRM-2025-006-M 适用于支付系统。
事件	未证实与 CNBV 完全等效。
未经认可的操作	需要实体和渠道的具体制度。
已核实的期限和范围	不得编造日志或事件期限。

表格来源：[115]

西班牙

法域	规则、范围和局限
日志/身份验证	RD-ley 19/2018，第 66 条：风险和控制措施。
事件	第 67 条：严重事件和用户通知。
未经认可的操作	第 45 条：在特定条件和例外下返还。
已核实的期限和范围	严重事件：立即；风险评估至少每年一次；统计数据至少每年一次。

表格来源：[116]

---

[114]哥伦比亚。金融监管局。2020 年第 033 号外部通函，确认为安全和网络安全指令；施加具体义务前必须核实条款编号。官方在线来源

[115]厄瓜多尔。JPRM-2025-006-M 号决议，《官方公报》第 104 号增刊，18-08-2025：支付系统的运营、有效性、清算、结算和资金可用性。官方在线来源

[116]西班牙。第 19/2018 号皇家法令，第 45、66 和 67 条：未经授权操作的返还、风险管理和严重事件立即通知。官方在线来源

11. 国际方法标准

ISO/IEC 27037:2012 为潜在数字证据的识别、收集、取证获取和保全提供指导。ISO 官方页面显示，该版本于 2018 年经审查确认并仍然有效。其定义有助于明确识别、保全、逐位镜像、可重复性和可复现性。该标准用于构建程序和控制，不能仅因使用了特定工具就宣布文件真实或可采，也不能替代各法域规则或司法评价。[117]

NIST SP 800-86 将流程组织为收集、检查、分析和报告，并把文件、操作系统、流量和应用程序与事件响应联系起来。该指南明确说明它不是通用程序或法律意见。对本手册而言，它用于组织数据源和文档；对法律附录而言，其性质是技术指南。良好做法是将每个阶段与工作证据对应起来：识别数据源和授权、有记录的取证获取、验证、发现、其他假设和限定性结论。目标不是制造确定性，而是展示做了什么、哪些可以重复、哪些仍未证明。[118]

手册阶段	方法参考	应达到的证据质量
识别	ISO/IEC 27037	数据源、保管人、状态、授权、改动风险和优先级。
取证获取	ISO/IEC 27037 和 NIST SP 800-86	方法、工具/版本、日期和时区、适用时的哈希值、异常情况，以及原始材料/副本关系。
检查与分析	NIST SP 800-86	工作副本、假设、测试、未发现结果和可复现性。
报告	NIST SP 800-86 和当地程序规范	事实、方法、发现、局限、附录和质证可能性。

[117]ISO/IEC 27037:2012。数字证据识别、收集、取证获取和保全指南。该版本经 ISO 确认现行有效。官方在线来源

[118]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. 方法指南，并非法律，也不保证证据可采性。官方在线来源

12. 使用矩阵并避免虚假等效的规则

第一条规则是引用功能 + 法律文件 + 条文 + 适用范围 + 版本，而不是所谓的“等效法律”。第二条是保留差异：简单、高级、数字或合格签名；电子原件与打印副本；完整性推定与作者身份证明；档案保存与取证保管；身份验证记录与同意；可采性与证明力。第三条是记录查询日期，并在案卷需要时核查后续修订。第四条是不得用银行规范为超出其主体范围的任何私人调查提供依据，也不得用行政规则解决所有民事或刑事程序。

第二项核查是实质核查。关闭本手册附录前，必须确认每个链接都能打开来源、条文确实存在于下载文本中；不得把第 27269 号法律中不存在的一般制度归于秘鲁；秘鲁的修订必须是 SBS 2286-2024；阿根廷不得把第 27.446 号法律废止的条文当作现行；西班牙不得把第 59/2003 号法律当作现行。墨西哥的过渡必须区分 CNPCF 汇编、延长至 2030 年的提案和实际颁布的法令。圣路易斯波托西州的人工智能规范应作为独立案卷记录，因为它包含修订和后续废止，而不是一项保管规则。

编辑控制	验收问题	不合格时的行动
身份	法律文件和条文是否逐字出现在来源中?	撤回引文或标记为未验证。
功能	该规范是否确实规定了所述功能?	重新归类为部分/行业性，并说明局限。
现行效力	版本和修订是否适用于该事实?	记录日期并在官方公报中进行专项复核。
范围	主体、渠道和程序是否均在其范围内?	不得扩展规则；应申请特别制度。
效力	是否区分采纳、真实性、证明力和举证责任?	删除自动推定并改写结论。
技术验证	格式是否允许核验规范要求?	保存原生文件、语境、元数据和导出过程。

操作结论：本手册需要的不是一张相似措辞对照表，而是一份指导，用不同规则处理同一问题。有用的功能等效必须能够帮助决定保全什么、申请什么、核验什么和声明哪些局限。凡不能以来源和已核实范围支撑的，都应排除或明确标为未证实。

研究范围

法律声明：本文件是通用研究和编辑设计材料，不构成法律意见、专家鉴定意见或对具体案件的看法。适用于案卷时，必须核查事实发生时的现行规范、法域、事项、渠道和相应程序规则。

A.13 实际应用：先选择制度，再作结论

案卷可以涉及多个国家，但并非所有规范都适用于所有事实。一个在墨西哥管理的账户、一家位于智利的供应商和一笔在西班牙受到质疑的操作，要求分别分析事实发生地、受监管主体、渠道、合同、程序和时间版本。第一步不是翻译第 210-A 条，而是确定需要哪种功能：保存消息、证明归属、取得日志、重建身份验证或审查事件义务。然后再定位在该主体和程序中承担该功能的规范。

步骤	应用问题	记录在案的结果
界定	分析的是哪种事实、主体、渠道和程序?	法域和范围图。
定位	哪项规范在该事项中承担该功能?	法律文件、条文、版本和官方来源。
分类	等效属于直接、部分还是行业性?	明确局限和补充规范。
保全	哪个对象可以用于核验要求?	原生文件、语境、元数据、导出和保管。

步骤	应用问题	记录在案的结果
结论	哪些效力得到证明，哪些没有？	限定性断言，不照搬他人的推定。

A.14 墨西哥调查期间的数据保护

取证保管不是数据保护的一般例外。处理必须保持目的明确、比例适当、安全和保密；不能仅因方便就共享完整案卷。应区分工作版本和传播版本、限制访问，并避免保留与委托无关的第三方数据。重大数据泄露必须按照法律规定的审慎义务处理，包括通知受影响人员，使其能够维护权利。根据 2025 年 3 月开始的过渡，现行联邦主管机关是反腐败与善治部。[119][120]

比较规则

有用的法律等效最终必须形成可验证的决策：保全什么、申请什么、核验什么、不作什么断言。如果分析没有改变其中任何答案，引文就只是装饰。

[119]《联邦私人持有个人数据保护法》，新法于 20-03-2025 发布，并于 14-11-2025 修订。第 5–9、18–20 和 31 条：原则、安全、保密、数据泄露和期限。官方在线来源

[120]反腐败与善治部。第 011 号公告，21-03-2025：个人数据保护职能由 INAI 移交至该部。官方在线来源

附录B 范围与授权表

本表应在访问数据源前填写，用于防止委托因冲动而扩大，或把技术能力误当成许可。如果对象、期间或目的发生变化，应创建新版本并保留旧版本。任何不可用字段都必须说明原因及能够解决该问题的人。

B.1 格式内容

字段	必需内容	完整虚构示例
标识符	不含客户姓名或敏感数据的案件编号。	EXP-DEMO-2026-001。
目的	预期用途：业务连续性、内部调查、司法鉴定或诉讼程序。	确定争议销售的记录、传输和结算。
分别记录各方说法	各方的主张，不将其表述为已证实的事实。	商家：销售未获付款。支付处理方：未收到交易。
时间段	开始、结束、时区和所需精度。	2026 年 11 月 1 至 3 日，当地时间 −06:00。
纳入的数据源	经授权的系统、文件、账户和设备。	三个参考编号对应的汇款批次、支付处理方报告和银行入账记录。
排除事项	不审查哪些内容以及原因。	与案件参考编号无关的个人设备和电子邮件。
授权	授权人、授权文书、允许的操作和有效期。	获授权的代表；有记录的管理性查询和导出。

字段	必需内容	完整虚构示例
风险	易失性、隐私、业务连续性、第三方和不可逆节点。	日志滚动覆盖和无关购买者的个人数据。
交付物	产品、格式、接收方、渠道和复核。	技术报告、清单文件和导出文件；加密交付给负责人。
变更控制	版本、日期、申请人、授权人及其对数据源的影响。	A01：增加支付处理方的字段字典，不扩大设备范围。

初始条件

在范围、授权和排除事项得到回答之前，不执行取证获取。如果紧急情况迫使行动，应记录例外决策、其依据和已实施操作的局限。

附录C 接收与初步保全记录

接收记录应在收到对象时填写，而不是在分析结束后填写。观察结果与交付人的陈述应分别记录。照片应与标识符关联，但不能替代文字描述。如果不知道某项先前操作，应写明“情况不明”及解释，不得用令人安心的推测代替。

C.1 物理接收记录示例

字段	虚构记录
案件和证据	EXP-DEMO-2026-001 · ED-20261109-DEMO-SSD-003-R00。
对象	2.5 英寸 SATA SSD，标称容量 512 GB；可见序列号 DEMO-003。
交付	保管人 A，获授权的行政负责人；2026 年 11 月 9 日 14:32 −06:00。
接收	分析师 B，指定的专业人员；接收实验室。
观察到的状态	已关机并断开连接；外壳无可见变形；连接器无明显残留物。
配件	SATA 数据线和电源登记为关联对象 ACC-003-01 和 ACC-003-02。
所声明的历史	该驱动器由系统人员拆下；不知道事件后是否曾连接。
照片	FOT-003-01 整体；FOT-003-02 序列号；FOT-003-03 连接器和配件。
包装和封条	防静电袋置于硬质容器内；SL-DEMO-003 封条完好。

字段	虚构记录
初始决策	保全、验证写保护器并准备经授权的物理取证获取。
备注	接收期间未开机或查看；记录中未写任何密码。

C.2 文件或消息的接收

电子接收时，物理状态字段应替换为渠道、账户、自称的发件人、URL 或消息、权限、原始名称、大小和下载日期。文件必须先保存，再重命名或转换。如果来自邮件，应保存 EML，并分别计算消息和附件的哈希值。如果来自链接，应记录访问人及当时可用的版本。

控制	虚构示例
渠道和消息	2026 年 11 月 9 日 15:02 −06:00 收到供应商邮件。
完整对象	entrega_001.eml 已保存，包含正文、邮件头和两个附件。
附件	registros.csv 和 diccionario.pdf；清单文件中保留原始名称。
供应商声明	正文声明使用 SHA-256 算法，并列出每个附件的值。
验证	有记录的本地计算：registros.csv 一致；diccionario.pdf 不一致。
处理	不编辑任何附件；请求澄清并再次交付 PDF。
局限	CSV 一致只能证明与交付文件相同，不能证明内容真实性或覆盖完整。

附录D 取证获取记录

记录必须说明复制了什么、覆盖范围如何以及在何种条件下完成。工具不能只作为可信品牌引用，还应附版本、配置、验证和结果。错误与输出一并保存。如果重复取证获取，应创建新标识符并说明相互关系。

D.1 完整示例

字段	虚构记录
案件和取证获取	EXP-DEMO-2026-001 · ED-20261109-DEMO-SSD-003-A01。
相关数据源	ED-20261109-DEMO-SSD-003-R00，已在接收记录中识别。
目标和覆盖范围	制作完整介质的物理镜像，包括未分配空间，供后续检查。
授权	A01 表；范围仅限于收到的 SSD 和所界定的事件。
连接	数据源连接写保护器，写保护器再连接工作站；型号和端口已记入日志。
工具	经验证可用于测试镜像的工具；名称、版本和配置已记入技术记录。
日期和时区	开始 2026-11-09T15:21:08−06:00；结束 2026-11-09T16:47:52−06:00。
输出	ssd003_A01.e01 和日志文件；工作副本与保存的原始材料分开。
完整性	算法 SHA-256；受控清单文件中与镜像文件关联的值。

字段	虚构记录
异常情况	记录了十二个不可读扇区；不隐藏错误信息，也不声称取证获取完美。
验证	输出可以打开，大小与介质一致，验证值相符。
结束	原始材料使用新标识符重新封存；旧封条和拆封情况已记入保管记录。

验收标准

文件存在并不足够。必须能够打开、与数据源关联、说明覆盖范围并保留异常情况。如果某一阶段无法核验，应先记录再继续。

附录E 保管链与移交

日志记录的是事件，而不只是移交。拆封、制作副本、下载文件或查阅容器，也可能改变责任人和需要验证的内容。每一行都关联对象、负责人、目的、位置、封条和完整性。密钥不得写入此表。

E.1 事件序列示例

事件	负责人和目的	验证和结果
接收 09-11 14:32 −06	保管人 A 将 SSD-003 交给分析师 B 进行保全。	序列号和照片一致；SL-003 封条完好。
拆封 09-11 15:18 −06	分析师 B 打开容器，实施经授权的取证获取。	保留旧封条和拆封原因；对象未更换。
取证获取 09-11 15:21 −06	分析师 B 在经验证的工作站上生成 A01。	输出、异常情况和哈希值记录在 D 表中。
重新封存 09-11 16:55 −06	分析师 B 将数据源放回容器。	新封条 SL-003-B；原始材料与工作副本分开。
移交 10-11 09:10 −06	保管人 C 通过加密渠道将 A01 副本交给复核人 D。	接收方、权限、下载和哈希验证均已确认。
查阅 10-11 11:42 −06	复核人 D 打开副本以复核假设矩阵。	访问已登记；原始材料未修改。

E.2 电子移交

通过链接移交应包括发送人、接收方、权限、到期日期、版本、密钥交付渠道和下载核验。不能仅因系统显示“已发送”就推定已接收。接收方应确认对象身份、大小，并在适用时核对哈希值。如果链接被替换，应保留两次交付的历史。

附录F 通过供应商申请与取证获取

本格式用于避免笼统申请“全部信息”却只收到缺乏语境的表格。申请应明确问题、字段和交付方式。授权通过安全渠道发送；示例不含真实数据。如果供应商无法满足某项要求，必须在答复中声明，使该局限随证据一并保留。

F.1 申请模板

虚构的记录申请与可验证交付

主题：EXP-DEMO-2026-001 • 2026 年 11 月 1 至 3 日的记录

通过获授权的安全渠道，我申请案卷中参考编号所关联的事件，时间范围为 2026-11-01T00:00:00−06:00 至 2026-11-03T23:59:59−06:00。请说明系统使用的时区、夏令时和转换规则。

请在可用时提供：日期/时间、事件类型、方向、时长、标识符、基站小区、技术、结果和空字段说明。包括原生 CSV/XLSX 格式、供查阅的 PDF 副本、字段字典、提取过程和日期、筛选条件、覆盖范围及保存期限限制。

请在答复正文中注明每个文件的算法和哈希值。交付应保存为 EML 格式，包含正文、邮件头和附件。不得在该邮件中发送密钥或凭据。

获授权的技术负责人 • EXP-DEMO-2026-001

F.2 导出或 API 记录

字段	虚构示例
账户和角色	DEMO 管理账户；只读和导出角色。

字段	虚构示例
系统和版本	供应商门户；记录界面版本或日期。
查询	时间段、参考编号和事件类型；筛选条件保存在日志中。
时区和格式	声明为 UTC；原生 CSV 和字段字典。
API（如适用）	端点、版本、参数、分页和限制；报告中不含秘密信息。
结果	两个文件，记录行数和导出错误。
交付	完整 EML、URL 或受控渠道和下载日期。
验证	每个对象的哈希值及其与供应商声明的关系。
覆盖范围和局限	可用保存期限、缺失数据和未覆盖期间。

附录G 对象清单与清单文件

清单文件用于关联对象，避免文件夹变成没有来源的文件集合。每一行对应一个文件、镜像、导出文件、可视化内容或报告。路径和大小有助于识别，哈希值控制该具体对象。公开版本应省略敏感数据，同时保留完整的工作版本。

G.1 清单文件示例

标识符	关系和对象	控制
DEMO-EML-001-R00	收到的原始邮件；正文、邮件头和附件。	名称、大小、接收日期和受控记录中的 SHA-256。
DEMO-CSV-001-R00	从 EML 中提取的附件 registros.csv，未作修改。	与正文中声明的哈希值一致；18,420 行。
DEMO-PDF-001-R00	首次交付的附件 diccionario.pdf。	哈希值不一致；保留以供比较和澄清。
DEMO-PDF-001-R01	第二次交付的字段字典；不同的关联对象。	新的日期和哈希值；不得悄然替代 R00。
DEMO-CSV-001-W01	供查询的 CSV 工作副本。	派生自 R00；分析更改另行保存。
DEMO-INF-001-V10	报告 1.0 版及所引用附录。	加密交付；记录分发哈希值和接收方。

命名规则

操作名称不会删除原始名称。清单文件保留收到的名称并添加内部标识符，使整理绝不意味着改动数据源。

附录H 时间线与时区

时间线应区分数据源表述与分析师所作转换，绝不能以“已纠正”的日期替代原始值。精度应按可用粒度表达：日、分钟、秒或时间窗口。如果同步未获证实，应将其记录为局限，而不是把时间变成虚假的确定性。

H.1 时间线示例

数据源和原始值	规范化	允许的解读
服务器：2026-11-03 20:14:07 UTC	2026-11-03 14:14:07 −06:00；秒级精度。	在服务器上观察到的事件；未证明自然人作者身份。
邮件：2026 年 11 月 03 日 14:20:11 −06:00	不转换；邮件头保存在 EML 中。	晚六分钟接收；时间接近不能证明因果关系。
照片：2026:11:03 14:16:00	未声明时区；设备时钟待核实。	只有确认时区和时钟才能相容；不得作为确定事件排序。
证言：“饭后”	大致时间窗口；不指定确切时间。	由人员陈述的语境，不是技术记录。
导出：11 月 1 至 3 日	覆盖范围有限；该期间之外未查询。	不能断言范围之外没有事件。

H.2 矛盾日期处理规则

首先核查事件是否属于同一对象和含义，然后核查时区、时钟、转换、格式和导出过程，最后才评估是否遭到操控。矛盾应连同两个值及可能解释一并保留。有用的时间线应显示疑问所在，而不是用整齐的单元格掩盖它。

附录I 假设与印证矩阵

矩阵应在撰写结论前建立，并且必须包含能够削弱每项假设的核验，而不能只列出有利数据。如果两个数据源来自同一文件，应标明其依赖关系；把它们算作独立印证会人为夸大证据分量。

I.1 完整示例

要素	虚构展开
陈述	该文件于 11 月 3 日在前员工账户中首次创建。
假设 A	由指定账户在该日期新创建。
假设 B	事后复制或修改先前文件。
假设 C	他人使用该账户或会话失控。
数据源	原生文件、云端历史、会话、第二验证因素和先前备份。
核验	比较版本、应用程序作者、会话和设备；检查先前序列。
发现	10 月 28 日的先前版本和来自未登记设备的会话。
影响	削弱了新创建和自动归属于账户持有人的假设。
局限	尚不能识别谁控制设备，也不能确定其意图。
后续行动	在授权范围内申请设备注册和活动记录。
临时结论	可见日期不能证明初始创建；账户本身不能识别个人。

决策不带自我偏见
如果发现与初始假设相矛盾，应改变假设或结论，不得改动对象，也不得为了维持便利说法而省略发现。

附录J 合成内容审查

目标不是获得一个“人工智能”百分比，而是记录来源、转换和发布。生成、编辑、转码和重新录制是不同事件。如果使用检测器，应记录名称、版本、配置和局限。无论结果为肯定还是否定，都不能替代文件和语境。

J.1 应用格式

字段	虚构示例
收到的对象	video_publicado.mp4；链接、账户、日期和保存的副本。
先前来源	生成文件未知；向持有人和平台申请。
历史	发布、下载和转换分别记录为独立事件。
声明的工具	发布者未声明；不得推定使用了某个具体工具。
技术分析	编码、帧、音频、连续性和可用元数据。
检测器	结果仅供参考；记录版本和局限，不自动给出定论。
印证	申请相机原始文件、编辑历史和早期发布记录。
法律语境	分别审查同意、身份、用途、行为、日期和现行规范。
允许的结论	该文件呈现与编辑相符的转换；来源和作者未获证实。
可能改变结果的数据源	具有可验证历史的原始文件或生成服务的日志。

附录K 报告结构和结论

模板用于组织内容，但不能替代推理。报告每章都应回答读者的问题，并引用具体附录。个人数据仅限于必要范围。执行报告和技术报告可以分开，以便管理层阅读和专业复核，同时保持相互关联。

K.1 建议顺序

部分	回答的问题	最低内容要求
委托和范围	请求了什么，哪些内容被排除？	问题、目的、法域、期间和排除事项。
授权和角色	由谁授权、由谁执行？	授权、职能、沟通和已申报的冲突。
数据源	收到或获取了哪些对象？	清单文件、标识符、状态、表现形式和缺失项。
方法	如何检查，覆盖范围如何？	工具、版本、参数、日期、查询和异常情况。
发现	观察到了什么？	肯定、否定和无法定论的结果，并注明对应对象。
分析	比较了哪些解释？	假设、印证、矛盾和已避免的错误推论。
结论	在范围内可以作出什么断言？	逐项回答、断言程度和依据。
局限	哪些事项未得到证明？	缺失数据源、覆盖范围、时钟、格式、错误和访问。

部分	回答的问题	最低内容要求
附录和交付	如何复核?	记录、取证获取、清单文件、时间线、查询和版本控制。

K.2 完整结论示例

虚构结论

作为 DEMO-EML-001-R00 邮件附件收到的 registros.csv，其 SHA-256 与供应商在邮件正文中声明的值一致。这证明收到的附件与该声明所指文件相同。导出文件包含 18,420 行，涵盖 2026 年 11 月 1 至 3 日；根据交付的字段字典，时间以 UTC 表示。在该覆盖范围内，未观察到与所查询的三个参考编号相关的事件。该结果不能证明此期间之外、其他渠道或未交付记录中不存在操作，也不能识别可能实施这些操作的人。

上述结论不需要“确凿地”这样的措辞，也不需要承诺诉讼成功。其力量在于每个组成部分都可定位：消息、文件、哈希值、行数、期间、参考编号和局限。如果另一方找到其他数据源，可以在不破坏先前工作的情况下扩展分析。

附录L 操作核查清单

清单用于输出控制，不能替代专业判断。每项肯定回答都需要可定位的证据。“不适用”必须说明理由。如果某项控制未通过，应记录由谁决定继续、为何继续以及附带何种局限。这些问题可以打印并适配程序，但不得被用来事后声明未实际执行的操作。

L.1 接收与取证获取

控制	预期证据	不合格时
范围和授权是否有记录?	签署的表格或可验证的授权。	停止并澄清；如有例外，予以记录。
对象是否有标识符和状态?	接收记录、序列号、照片和配件。	解决身份问题或声明局限之前，不得分析。
数据源和副本是否分开?	原始材料/派生对象的关系和位置。	制作受控副本，不改写接收记录。
方法和覆盖范围是否清楚?	取证获取记录、筛选条件和格式。	按实际执行的操作补齐日志。
输出能否打开并验证?	打开测试、清单文件和相关哈希值。	作为新对象重复，并保留异常情况。
是否记录错误和排除事项?	异常情况、筛选条件、缺失字段和原因。	不得声称全面；限制结论。

L.2 分析、报告与交付

控制	复核问题	要求的结果
可追溯性	每项结论是否都能追溯到发现和数据源?	路径完整，附录一致。
时间线	是否保留原始值、时区和精度?	转换有说明，不确定性可见。
假设	是否寻找与初始说法相矛盾的内容?	其他解释、否定和无法定论的结果。
语言	完整性、作者身份和内容真实性是否分开?	不使用绝对表述或错误推论。
质证	是否有他人尝试查找错误?	意见、答复和变更均有记录。
现行效力	规范是否对应主体、事项和日期?	官方来源、版本、功能和适用范围。
交付	能否打开、阅读并包含所引用附录?	交付包已验证，渠道和接收均已确认。
隐私	传播版本是否避免不必要的暴露?	访问、最小化和受控版本。

附录M 版本、来源和经验教训控制

版本控制应区分历史案卷和现行程序。过去的记录不得为了显得更新而修改；法律或工具变化时，指南则应修订。每项变更都注明原因、来源、负责人、日期和影响。未经验证的来源不得呈现为已验证。

M.1 法律和技术记录

要素	应记录的内容	示例
法律文件或工具	完整名称、事项、法域或版本。	CNPCF 第 348–350 条；经验证的工具和版本。
来源和查询	官方 URL、日期、汇编和负责人。	众议院门户，查询过程有记录。
发现的变更	修订、废止、宣告或行为变化。	提案与法令分开；新的导出版本。
功能影响	哪项要求或决策发生变化，影响谁。	更新过渡制度或字段字典。
编辑处理	修改的章节、表格或格式。	替换现行文本并保留历史。
复核	人员、日期、验证和按风险安排的下一次复核。	在来源中核对条文，并用虚构示例测试。

M.2 将经验转化为改进

字段	虚构示例
异常事件	收到一份没有时区和字段字典的导出文件。

字段	虚构示例
影响	无法构建可靠时间线，也无法解释空字段。
原因	此前申请只要求“完整报告”，没有规定格式或语境。
个案纠正	申请重新交付，同时保留首次交付及其局限。
预防性变更	附录F 要求提供时区、字段字典、筛选条件、原生格式、哈希值和 EML。
验证	与虚构供应商演练：所有字段均已提供且能够打开。
负责人和版本	方法复核人；F 格式从 1.0 更新为 1.1，并记录日期和原因。

连续性规则

新版本不掩盖旧版本。它使人了解曾经相信什么、发生了什么变化、依据什么来源，以及对未来案件有何影响，同时不改动已结案的案卷。