ACCCF / 应用知识库

03

卷

审慎遏制与经验证的恢复

西班牙语版 · 2026

勒索软件响应手册：遏制、证据与业务连续性

最初阶段、保全、根除、恢复与复盘

快速响应，同时不破坏有助于理解事件的信息，保护人员，并以可验证的控制措施恢复运营。

适用于管理层、安全、技术、业务连续性、法务、保险、第一响应人员和取证专家。说明仅限于防御管理和保全，不包括执行恶意软件或与攻击者谈判。

编辑统筹：Jocsan Laguna · 美国网络安全与计算机取证委员会

通用技术指南和开放教育材料。不构成法律意见、专家鉴定意见，也不构成未经授权访问系统的操作指导。示例和数据均为虚构；图示为编辑重构。

目录

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。

前言：危机不会免除方法要求 3

第1章 最初十五分钟 3

1.1 先建立案卷，再打开文件 3

1.2 关机、断网或保持运行 4

第2章 范围、传播与优先级 5

2.1 可见设备并不等于事件全貌 5

2.2 按服务而非噪声确定优先级 5

第3章 遏制期间的保全 6

3.1 内存、磁盘、日志和状态 6

3.2 停用账户或重装系统前先保留日志 6

3.3 勒索信息与联系渠道的证据 6

第4章 调查：来源、持久化与数据外泄 7

4.1 明确显示不确定性的时间线 7

4.2 入侵与持久化假设 8

4.3 数据外泄：缺乏证据与证据证明不存在 8

第5章 根除与赎金决策 9

5.1 根除原因，而不只是消除症状 9

5.2 支付或不支付：有据可查的决策，而非冲动 9

5.3 沟通与义务 9

第6章 恢复与连续性 10

6.1 选择并验证恢复点 10

6.2 分阶段恢复 10

6.3 信息核对与复盘 11

附录A 法律框架与行业记录 11

附录B 响应格式 13

B.1 事件时间线 13

B.2 遏制决策矩阵 14

B.3 取证获取记录 14

B.4 恢复退出标准 14

附录C 演练与核查清单 15

C.1 使用虚构数据的桌面演练 15

C.2 结束前的简要核查清单 15

前言：危机不会免除方法要求

当文件无法打开、屏幕要求支付赎金时，第一反应往往是关闭所有设备、删除看似受感染的内容并恢复任意备份。这些操作在某些情境下可能减少损害，在另一些情境下却会毁灭证据，还可能把未经检查的持久化机制重新带回生产环境。工作不是在速度与证据之间二选一，而是在限制损害的同时保全必要信息，并为每项决策指定负责人。

本手册从一开始就采用两条并行主线：一条保护人员、服务和业务连续性，另一条保存数据源、决策和证据。不得让第二条主线阻碍紧急安全行动，也不得让第一条主线在没有记录的情况下抹去理解事件经过的可能性。每项行动都必须说明由谁授权、依据什么信息、改变了什么，以及引入了什么风险。

NIST SP 800-61 Rev. 3 将响应组织为准备、检测、响应、恢复和持续改进。NIST SP 800-86 提供收集、检查、分析和报告之间的关系。只有记录范围、工具、结果和局限，响应才不会沦为按钮清单。文件被加密只能证明加密事实，不能单独证明访问何时开始、是否发生数据外泄或由谁实施。[1][2]

> **指导规则**
>
> 首先保护人员。随后以合理的最小损害进行遏制，保全可能消失的信息，不要仅因系统重新开机就宣称已经清除威胁。

第1章 最初十五分钟

1.1 先建立案卷，再打开文件

第一位发现问题的人应记录日期、时间和时区、看到了什么、涉及哪台设备、由谁报告，以及已经实施了哪些操作，无需作出诊断。不得使用未知程序打开勒索信息、执行附件或为了“确认真伪”而点击链接。应在不交互的情况下拍摄或记录消息，并尽可能保存原始对象。

应指定事件协调人，并在可能已受感染的系统之外建立沟通渠道。通讯录包括技术、业务连续性、法务、隐私、沟通、保险和供应商联系人。如果企业邮件可能受影响，不得用于共享指标、凭据或敏感报告。口头决策应记录时间和负责人。

[1] NIST SP 800-61 Rev. 3（2025 年 4 月）。CSF 2.0 中的综合事件响应建议：准备、检测、响应、恢复和改进。取代第 2 修订版。 官方在线来源

[2] 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

初始问题	最低记录要求	它如何改变下一项决策
是否有人员或关键服务面临风险?	服务、依赖关系和直接后果。	遏制以生命和安全优先于证据。
具体观察到了什么?	消息、扩展名、行为、资产和时间。	区分警报和假设。
是否仍在传播?	设备、网段、资源和观察到的活动。	决定隔离方式和紧迫程度。
哪些信息可能消失?	内存、会话、日志、链接和备份。	变更前优先保全。
由谁决策和沟通?	协调人、授权人、渠道和代理人。	避免相互矛盾的行动和谣言。

1.2 关机、断网或保持运行

不存在通用答案。关机可以停止进程，同时也会清除分析或恢复所需的内存、会话和密钥。断网可以限制传播和数据外泄而不清除易失性信息，但也可能触发攻击者预设行为或中断关键服务。保持运行便于观察和现场获取，却可能继续修改数据并扩大损害。

决策应依据设备状态、传播情况、服务、加密、易失性数据、工具和授权。如果具备现场获取能力，应在关机前评估；如果不具备，应记录这一限制，并在保证安全的前提下选择破坏性最小的遏制方式。第一响应人员如果没有受过训练，不应临时尝试内存取证；可以拍摄状态、按程序隔离并上报。

> **例外决策**
>
> 如果生命或基本服务依赖该系统，不得以证据保全为由延迟保护。应记录必要性、考虑过的替代方案，以及行动前后能够保存的证据。



图1 遏制就是决定优先保护什么。不存在统一的关机或断网指令。编辑重构；不构成真实证据。

第2章 范围、传播与优先级

2.1 可见设备并不等于事件全貌

文件被加密的终端，可能只是数周前从另一账户开始的攻击链的最后一环。范围图应包括身份、VPN、电子邮件、服务器、虚拟机管理程序、备份、供应商、经授权用于工作的个人设备、管理系统和云服务。扩展范围必须以证据为依据，不能仅凭“一切均已失陷”这句话，否则会造成不必要的停机并掩盖优先级。

应建立资产矩阵，记录关键性、所有者、状态、可能失陷情况、依赖关系、日志来源和决策。一台设备可能已感染，另一台可能只是因交换机隔离而无法访问，还有一台虽然健康，却依赖已停止的服务器。报告必须区分这些状态，不能把它们统一表述为已确认感染。

状态	所需证据	记录在案的决策
已确认	资产中可验证的数字痕迹、执行、日志或加密。	按优先级遏制和保全。
可疑	存在相关指标，但确认不足。	监控、选择性隔离或取证获取。
因依赖关系受影响	服务因其他操作或系统而停止。	恢复依赖关系，但不将其标记为已感染。
范围内未发现迹象	查询、筛选条件、时间段和已审查的数据源。	不得在该覆盖范围之外声明未受感染。
未知	缺少访问权限、日志或清单。	分配负责人和结论边界。

2.2 按服务而非噪声确定优先级

业务连续性矩阵应识别关键流程、可容忍的最长中断时间、维持运营所需的最少数据、依赖关系、负责人和临时人工路径。产生大量警报的服务器，未必比所有人依赖的目录服务更优先。应根据实际影响决定先恢复什么，而不是根据勒索信息中最先出现的文件。

响应团队和业务连续性团队使用同一时间线，但交付物不同。安全团队需要知道存在哪些持久化机制，连续性团队需要知道哪个版本可恢复及其依赖关系。核对信息可以避免恢复一个会重新连接事件源头的系统，也可以避免因不知情而让健康服务持续停机。

虚构案例

一家公司在文档服务器上发现加密。工资系统未被加密，却因依赖同一目录服务而无法运行。团队不把工资系统标记为已感染，而是记录为依赖关系受影响。恢复工作优先处理身份和日志，再重新连接各项服务。

第3章 遏制期间的保全

3.1 内存、磁盘、日志和状态

保全应根据易失性和回答问题的能力确定优先级。内存可能包含进程、连接、密钥或会话片段；磁盘保存文件和数字痕迹；日志解释事件；配置显示系统如何连接。并非所有案件都需要对每个资产进行完整获取。应选择能够区分来源、传播、持久化、数据外泄和恢复可能性的材料。

每次取证获取都应记录数据源、方法、工具和版本、日期和时区、授权、覆盖范围、输出、错误和验证。输出必须先打开验证，才能视为有效。文件存在却无法读取，就不是有用的证据。案卷应保留异常情况，包括获取不完整或工具不兼容。重复获取会生成新的关联对象，不会删除首次尝试。[3][4]

3.2 停用账户或重装系统前先保留日志

停用账户之前，应导出登录、验证因素注册、恢复方式变更、邮件规则、委派、令牌和可用的管理活动记录。重装之前，应保全镜像、配置、日志、任务和相关数字痕迹。这些操作在紧急情况下可能无法完成，应记录失去了什么及原因，而不是编造理想顺序。

讨论范围时，日志可能正在滚动覆盖。应要求供应商保全，并注明时间段、账户、字段、时区、原生格式、字段字典、筛选条件和局限。交付应保存完整 EML、正文、邮件头和附件。如果供应商为每个文件声明哈希值，应在本地验证并记录任何差异，不得修改数据源。[5]

3.3 勒索信息与联系渠道的证据

勒索信息应作为对象保存：截图、原始文件（如有）、位置、名称、观察日期、格式及其与设备的关系。其中关于数据外泄、监控或访问时间的陈述可能虚假，应将其视为攻击者的声明，而不是已证实的事实。支付和联系标识符应记录，但不得据此交易或遵循其指令。

[3] 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

[4] 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

[5] RFC Editor. RFC 5322, Internet Message Format：消息结构、邮件头和正文。这是保存和理解电子邮件的技术参考，并不能自动证明人的身份。 官方在线来源

对象	必要记录	可避免的错误
勒索信息	原始对象、位置、日期、关联关系和原文内容。	把其中的文字当作技术供述。
加密文件	受控样本、名称、大小、先前状态和保存的副本。	打开大量文件并改变现场。
事件邮件	EML、附件、邮件头、日期和接收方。	只保存消息截图。
支持账户	角色、权限、活动和导出。	共享访问权限或扩大事件范围。
备份	日期、版本、覆盖范围、位置和访问状态。	未评估污染情况就接入。

实验室安全

样本不得在个人设备或生产网络中运行。动态分析需要隔离环境、明确目标、授权、网络控制和记录。第一响应通常只需保全并上报。



图2 遏制时不应消失的数据源。每次取证获取都声明覆盖范围和局限。编辑重构；不构成真实证据。

第4章 调查：来源、持久化与数据外泄

4.1 明确显示不确定性的时间线

时间线应保留每个原始日期、时区、来源、精度和转换。UTC 日志、时钟有偏差的计算机和本地邮件，不能在不解释转换的情况下按同一时钟排序。首次检测不一定是首次访问。文件的修改日期不能证明加密器何时运行，它可能只反映结果被写入的时间。

应区分观察到的事件、人员陈述、计算结果和推定，不能把推定伪装成日志。如果某个阶段没有数据源，应写“范围内未证实”。日志缺失可能源于滚动覆盖、配置、筛选或删除，不一定意味着事件没有发生。

4.2 入侵与持久化假设

假设可以包括凭据被窃、暴露的漏洞、恶意邮件、供应商、外部设备或多种因素组合。分析应将每项假设与可能削弱它的数据源比较：身份验证、验证因素变化、规则、进程、计划任务、服务、新账户、连接和管理活动。应选择与最多事实相符、矛盾最少的解释，而不是最耸人听闻的解释。

假设	能够证实或削弱假设的数据源	结论边界
合法账户失陷	异常会话、验证因素、设备、恢复和大致地理位置。	账户被使用并不能识别使用人。
公开漏洞	版本、暴露情况、日志、受控测试和补丁日期。	存在漏洞不等于已被利用。
恶意邮件	EML、附件、打开和执行遥测数据。	收到邮件不等于执行了其中内容。
供应商失陷	远程访问、角色、变更和时间关联。	合同关系不能证明攻击途径。
持久化	账户、计划任务、服务、密钥、规则和数字痕迹。	不能只清除可见文件。

4.3 数据外泄：缺乏证据与证据证明不存在

评估数据外泄时，应检查连接、目的地、数据量、压缩、云端同步、电子邮件、规则、传输服务、代理日志、可用时的 DNS，并将攻击者声明作为单独假设。数据量大可能只是备份或合法活动；没有流量可能意味着缺少日志、加密流量未检查，或相关渠道未纳入。

结论应区分：存在传输证据、存在相容迹象、数据不足，或在明确覆盖范围内未观察到。不能仅因防火墙未显示就断言“没有数据外泄”，也不能把“我们会公开你的数据”当作数据已经外泄的证据。如果发现已发布的样本，应记录，但不得传播或下载不必要的信息。

> **可辩护的表述**
>
> “在这些日期和这些字段范围内的代理日志中，未观察到与事件相关的传输。覆盖范围不包括未检查的加密渠道、其他供应商或更早时期，因此不能断言完全不存在数据外泄。”

第5章 根除与赎金决策

5.1 根除原因，而不只是消除症状

根除范围包括账户、恢复方法、规则、远程访问、持久化机制、漏洞、秘密信息和供应商路径。如果令牌、会话或密钥仍然存在，仅更改密码并不足够。删除加密器并不能消除入口点。措施必须通过数据源和测试验证，并记录对运营的影响。

如果原因未知，应予声明。组织可以选择从可信环境重建，而不是在同一系统上“清理”。决策应基于风险和证据，而不是看似节省成本。重装的系统必须采用新配置、新凭据和监控，不能恢复到导致事件发生的状态。

5.2 支付或不支付：有据可查的决策，而非冲动

是否支付赎金，应由组织及其法律顾问、保险机构和主管机关决定。必须考虑合法性、制裁、资金来源和去向、持续运营能力、人员保护、再次遭到勒索的可能性，以及无法保证恢复的事实。本手册不建议支付赎金或与攻击者联系，只提供决策结构，避免由一个人在压力下独自决定。

因素	必须回答的问题	用于决策的证据
合法性	是否存在适用的禁令、制裁或限制？	最新的法律分析和审批渠道。
业务连续性	是否有其他可行路径，需要多长时间？	备份测试、替代方案和中断成本。
恢复	对方承诺了什么，又能验证什么？	不采信口头保证；进行技术评估并说明局限。
人员风险	是否存在额外威胁或敏感数据？	优先考虑安全和受影响人员保护。
重复风险	会留下什么激励或暴露风险？	记录风险和后续计划。
授权	由谁决策和沟通？	法定人数、记录和唯一授权渠道。

5.3 沟通与义务

通知评估应区分客户、数据主体、监管机关、保险机构、合作伙伴和主管机关。每个法域和合同都有不同的门槛和期限。技术信息的准备应能够解释事实、不确定性和措施，同时避免披露会扩大损害的细节。公共沟通不得先于证据保全，也不得把怀疑直接宣布为确定原因。

在墨西哥，信贷机构在适用规定下承担特定的事件调查、通知、记录和保存义务；在秘鲁，SBS 要求受监管实体进行保全和取证分析；在阿根廷，A 8280 号通告在其制度内规定响应和最终报告。这些期限不能套用到所有组织或其他国家。[6][7][8]

> **不得编造确定性**
>
> 执行报告可以说明已经知道什么、正在采取什么措施，以及哪些事项仍待确定。无需在恐慌和刻意镇定之间选择，只需要可辩护的时间线和明确的负责人。

第6章 恢复与连续性

6.1 选择并验证恢复点

最新备份可能含有持久化机制或损坏文件，较旧备份又可能缺少合法操作。应比较日期、覆盖范围、完整性、访问、历史和兼容性。原始备份应保存，工作则在隔离环境中使用受控副本。密钥应通过单独渠道交付，不得写入记录。

验证包括：副本可以打开、包含预期对象、可以挂载、版本一致，并且不显示已知失陷指标。这不能证明副本完全干净，只能证明它通过了既定测试。如果副本有错误，应判断这些错误是否影响目标，并保留详细记录。

6.2 分阶段恢复

先在隔离环境中以虚构数据或测试账户恢复最低服务，然后测试身份、权限、应用程序、集成、读写、导出和监控。只有通过这些测试，才允许逐步扩大范围。生产网络不得用作首次恢复实验室。

阶段	验收标准	证据
最低基础设施	组件和版本均已验证，无已知持久化机制。	清单和配置。
数据	文件可读、覆盖范围和关联关系正确。	样本、清单文件和数量。
应用程序	功能和权限使用虚构账户正常运行。	测试用例和结果。
集成	获授权的依赖项能够响应，且不存在非预期路径。	日志和连接。
观察	在规定期间内未出现异常活动。	警报、查询和局限。

[6]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

[7]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

[8]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

阶段	验收标准	证据
退出	负责人接受剩余风险并安排后续复核。	退出记录和监控。

6.3 信息核对与复盘

可能需要重建最近一次完整备份到检测之间产生的操作。应核对外部日志、凭证、电子邮件、消息和第三方文档，同时不得改动数据源。差异应记录，不得用伪装成真实数据的估算填补。

经验教训必须改变程序：新的保存规则、抗网络钓鱼身份验证、分段、不可变副本、恢复测试、目录、权限限制或演练。如果事件以一场展示结束，却没有任何行为改变，下一次危机将重复同样的顺序。

> **结束标准**
>
> 恢复意味着在证据表明控制措施有效运行的情况下恢复运营，并诚实说明仍未知的事项。结束工作应涵盖人员、系统、数据、供应商和后续复核。



图3 恢复系统不等于恢复信任。退出应分阶段并按照验收标准验证。编辑重构；不构成真实证据。

附录A 法律框架与行业记录

事件可能涉及电子证据、数据保护、合同、金融义务和业务连续性规则，这些功能必须分别分析。行业规范不会产生普遍义务，保存期限也不授权无限期保留一切。文献复核截至 2026 年 11 月 10 日；真实案卷需要核实现行效力、主体、事项和渠道。

法域	功能依据	使用限制
墨西哥	CCom 89–94 和 1205；CFPC 210-A / CNPCF 348–350，视过渡情况而定；CNBV 316 Bis 系列适用于相关实体；LFPDPPP 适用于个人数据。	区分电子文件、程序、银行和隐私。核查 CNPCF 的适用宣告。
秘鲁	IOFE 条例；CPC 188–197；适用于受监管实体的 SBS 504-2021 和 2286-2024。	不得把完整文件制度归于第 27269 号法律，也不得照搬 CNBV 期限。
智利	第 19.799 号法律；RAN 20-7、20-8、20-10，视实体和服务而定。	不得混淆业务连续性、外包和事件。
阿根廷	第 25.506 号法律；CCyC 318–319；BCRA A 7783 和 A 8280。	期限和主体各不相同；身份验证不等于授权。
哥伦比亚	第 527 号法律；行政行为适用 CPACA；SFC 规范的具体条款编号待确认。	不得编造来自未阅读通函的事件要求。
厄瓜多尔	第 67 号法律；LOPDP；适用时的支付系统制度。	通知和保存取决于处理和行业。
西班牙 / 欧盟	eIDAS；LEC 326 和 384；RGPD；支付服务适用 RD-ley 19/2018。	区分文件、程序、隐私和未经授权的操作。

表格来源： 910111213141516171819202122232425262 7

申请日志时，应明确功能、时间段、参考编号、字段、格式、时区和交付方式。目标不是索取所有服务器，而是获取能够回答具体问题的事件。保管链应记录由谁交付、由谁接收、包含什么对象、如何验证，以及存在哪些局限。

附录B 响应格式

B.1 事件时间线

字段	必需记录	控制
事件	观察到、陈述、计算或推定。	不得混淆类别。
原始日期和时区	原文、转换和精度。	不得覆盖数据源。
资产和数据源	对象、系统、标识符和位置。	可追溯至清单文件。
行动和负责人	发生了什么、由谁决定、由谁执行。	授权和证据。

[9]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

[10]《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

[11]《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

[12]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

[13]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

[14]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

[15]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

[16]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

[17]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

[18]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

[19]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

[20]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

[21]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

[22]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

[23]厄瓜多尔。《个人数据保护基本法》，26-05-2021《官方公报》第 459 号增刊。第 10、37–44 条：原则、安全措施、设计保护、风险和事件处理。 官方在线来源

[24]《（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

[25]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

[26]欧盟。（UE）2016/679 号条例，第 5、25、28 和 32–34 条：原则、设计保护、受托处理方、安全及数据安全泄露的通知/告知。西班牙还要求审查适用的国家和行业法律。 官方在线来源

[27]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

字段	必需记录	控制
结果	输出、错误和状态变化。	不得隐瞒异常情况。
下一项核验	待解问题和负责人。	避免过早结束。

B.2 遏制决策矩阵

虚构决策表

事件：DEMO-RANSOM-2026-001
资产和服务：[标识符、功能、依赖关系]
观察到的状态：[屏幕、进程、网络、加密]
评估的选项：[关机、隔离网络、保持运行、停用账户]
人员和业务连续性风险：[优先级]
易失性和面临风险的证据：[内存、日志、会话]
决策和授权：[行动、人员、日期和时区]
事先保全：[对象、方法和输出]
产生的变化：[最终状态和附带影响]
待解决事项：[无法保全或确认的内容]
复核：[负责人和下一次评估时间]

B.3 取证获取记录

技术清单文件

数据源/获取 ID：DEMO-SRV-001 / A01
授权和范围：[文件和排除事项]
初始状态：[照片和观察]
目标和覆盖范围：[内存、镜像、逻辑、导出]
工具和验证：[版本、环境和测试]
开始/结束及所在时区：[原始值]
输出：[文件、格式和大小]
完整性：[算法和具体对象]
异常情况：[错误和缺失的覆盖范围]
验证：[打开、关联和复核]
保管：[保存、访问和移交]

B.4 恢复退出标准

核验	是 / 否 / 不适用	证据和备注
使用前已保全备份	[ ]	标识符和保管情况。
数据可读且覆盖范围一致	[ ]	样本和数量。
账户和验证因素已重建	[ ]	不存在旧会话。
持久化已评估	[ ]	数据源和局限。
功能和集成已测试	[ ]	虚构用例。
监控和负责人已指定	[ ]	警报和复核。

核验	是 / 否 / 不适用	证据和备注
沟通已执行	[ ]	版本和接收方。
剩余风险已接受	[ ]	负责人签字和日期。

附录C 演练与核查清单

C.1 使用虚构数据的桌面演练

模拟一家企业，拥有三台服务器、两个管理账户、夜间备份和一家电子邮件供应商。08:12 报告文档被加密；08:16 另一台设备出现相同扩展名；08:20 在一个账户中发现转发规则。团队必须决定隔离方式、首次获取、供应商联络、数据评估和恢复路径，且不得执行任何文件。

评估依据是决策和记录的质量：如果团队未保全就恢复，将失去解释转发规则的机会；如果在导出前停用账户，必须记录该局限；如果让关键服务没有替代方案，必须说明理由。最后应复核决策，而不是奖励最快的行动。

C.2 结束前的简要核查清单

问题	预期结果
人员是否得到保护？	优先事项和基本服务已得到处理。
优先易失性证据是否已保全？	对象、方法和局限均有记录。
是否评估了来源、持久化和数据外泄？	假设和数据源，不使用绝对表述。
赎金和沟通决策是否获得授权？	法定人数、依据和版本。
恢复是否经过测试？	数据、功能、访问和观察。
为下一次作了哪些改变？	实际控制、负责人和验证。

结语

冷静不是声称一切正常，而是清楚正在做什么、依据什么证据、由谁决策，以及哪些事项仍待核验。