ACCCF / अनुप्रयुक्त ज्ञान का पुस्तकालय

03

विवेकपूर्ण रोकथाम और सत्यापित पुनर्प्राप्ति

स्पेनिश भाषा का संस्करण · 2026

खंड

रैंसमवेयर प्रतिक्रिया मैनुअल: रोकथाम, साक्ष्य और व्यावसायिक निरंतरता

पहले क्षण, संरक्षण, उन्मूलन, पुनर्प्राप्ति और सीख

घटना को समझने, लोगों की रक्षा करने और सत्यापनयोग्य नियंत्रणों के साथ संचालन फिर शुरू करने में मदद करने वाली जानकारी को नष्ट किए बिना शीघ्र प्रतिक्रिया देना।

प्रबंधन, सुरक्षा, प्रौद्योगिकी, निरंतरता, विधि, बीमा, प्रथम उत्तरदाताओं और फोरेंसिक विशेषज्ञों के लिए। निदेश रक्षात्मक प्रशासन और संरक्षण तक सीमित हैं; इनमें मैलवेयर चलाना या हमलावरों से बातचीत करना शामिल नहीं है।

संपादकीय समन्वय: Jocsan Laguna · अमेरिकन साइबर सुरक्षा और कंप्यूटर फोरेंसिक परिषद

सामान्य तकनीकी मार्गदर्शिका और खुली शैक्षिक सामग्री। यह कानूनी सलाह, विशेषज्ञ राय या बिना प्राधिकरण सिस्टमों तक पहुँचने का निर्देश नहीं है। उदाहरण और डेटा काल्पनिक हैं; आकृतियाँ संपादकीय पुनर्निर्माण हैं।

विषय-सूची

दृश्यमान पृष्ठ-संख्याएँ PDF संस्करण से संबंधित हैं। दस्तावेज़ खोलने पर Word इस विषय-सूची को अद्यतन कर सकता है; शीर्षकों में आंतरिक नेविगेशन बना रहता है।

प्रस्तावना: संकट से कार्यविधि समाप्त नहीं होती 3

अध्याय 1. पहले पंद्रह मिनट 3

- **1.1 फ़ाइलें खोलने से पहले अभिलेख खोलें** 3
- **1.2 बंद करें, डिस्कनेक्ट करें या चालू रखें** 4

अध्याय 2. दायरा, प्रसार और प्राथमिकताएँ 5

- **2.1 दिखाई देने वाला सिस्टम ही पूरी घटना नहीं है** 5
- **2.2 शोर के आधार पर नहीं, सेवा के आधार पर प्राथमिकता** 5

अध्याय 3. रोकथाम के दौरान संरक्षण 6

- **3.1 मेमोरी, डिस्क, लॉग और स्थिति** 6
- **3.2 खाते निलंबित करने या पुनः इंस्टॉल करने से पहले लॉग** 6
- **3.3 रैंसम नोट और संपर्क चैनल के साक्ष्य** 6

अध्याय 4. जाँच: उत्पत्ति, दीर्घस्थायित्व और एक्सफ़िल्ट्रेशन 7

- **4.1 स्पष्ट अनिश्चितता के साथ कालक्रम** 7
- **4.2 प्रवेश और दीर्घस्थायित्व की परिकल्पनाएँ** 7
- **4.3 एक्सफ़िल्ट्रेशन: साक्ष्य की अनुपस्थिति और अनुपस्थिति का साक्ष्य** 8

अध्याय 5. उन्मूलन और फ़िद्या पर निर्णय 8

- **5.1 केवल लक्षण नहीं, कारण का उन्मूलन करें** 8
- **5.2 भुगतान करें या न करें: दस्तावेज़ित निर्णय, आवेग नहीं** 8
- **5.3 संचार और बाध्यताएँ** 9

अध्याय 6. पुनर्प्राप्ति और निरंतरता 9

- **6.1 पुनर्प्राप्ति बिंदु का चयन और सत्यापन** 9
- **6.2 चरणबद्ध पुनर्प्राप्ति** 10
- **6.3 जानकारी का मिलान और सीख** 10

परिशिष्ट A. कानूनी ढाँचा और क्षेत्रीय अभिलेख 11

परिशिष्ट B. प्रतिक्रिया प्रारूप 12

- **B.1 घटना का कालक्रम** 12
- **B.2 रोकथाम निर्णय मैट्रिक्स** 13
- **B.3 अधिग्रहण अभिलेख** 13
- **B.4 पुनर्प्राप्ति से बाहर निकलने के मानदंड** 13

परिशिष्ट C. अभ्यास और जाँच-सूची 14

- **C.1 काल्पनिक डेटा के साथ टेबलटॉप अभ्यास** 14
- **C.2 समापन से पहले संक्षिप्त जाँच-सूची** 14

प्रस्तावना: संकट से कार्यविधि समाप्त नहीं होती

जब फ़ाइलें खुलनी बंद हो जाती हैं और स्क्रीन पर फ़िद्या की माँग दिखाई देती है, तो पहली प्रतिक्रिया अक्सर सब कुछ बंद करना, संक्रमित दिखने वाली चीज़ें मिटाना और कोई भी बैकअप रिस्टोर करना होती है। ये कार्रवाइयाँ एक संदर्भ में नुकसान घटा सकती हैं और दूसरे में साक्ष्य नष्ट कर सकती हैं। इनसे उत्पादन में ऐसा दीर्घस्थायित्व भी लौट सकता है जिसकी किसी ने जाँच नहीं की। काम का अर्थ गति और साक्ष्य के बीच चुनाव नहीं है: नुकसान सीमित करते हुए आवश्यक चीज़ों को संरक्षित करना है, ताकि प्रत्येक निर्णय का उत्तरदायी व्यक्ति हो।

यह मैनुअल शुरुआत से दो समानांतर कार्यपंक्तियों का उपयोग करता है। पहली लोगों, सेवाओं और निरंतरता की रक्षा करती है। दूसरी स्रोतों, निर्णयों और साक्ष्य को संरक्षित करती है। दूसरी पंक्ति को किसी अत्यावश्यक सुरक्षा कार्रवाई को रोकने नहीं दिया जाता, और न ही पहली को बिना अभिलेख के यह समझने की संभावना मिटाने दिया जाता है कि क्या हुआ। प्रत्येक कार्रवाई में यह बताना होगा कि किसने उसे अधिकृत किया, किस जानकारी के आधार पर, क्या बदला और कौन-सा जोखिम उत्पन्न हुआ।

NIST SP 800-61 Rev. 3 प्रतिक्रिया को तैयारी, पहचान, प्रतिक्रिया, पुनर्प्राप्ति और निरंतर सुधार में व्यवस्थित करता है। NIST SP 800-86 संग्रह, परीक्षण, विश्लेषण और रिपोर्ट के बीच संबंध स्थापित करता है। जब दायरे, उपकरणों, परिणामों और सीमाओं का दस्तावेज़ीकरण किया जाता है, तो प्रतिक्रिया केवल बटनों की सूची नहीं रहती। एन्क्रिप्ट की गई फ़ाइल एन्क्रिप्शन सिद्ध करती है; वह अपने आप यह सिद्ध नहीं करती कि पहुँच कब शुरू हुई, एक्सफ़िल्ट्रेशन हुआ या नहीं, या यह किसने किया।[1][2]

> **मार्गदर्शक नियम**
> पहले लोगों की रक्षा करें। फिर यथासंभव कम नुकसान के साथ रोकथाम करें, नष्ट हो सकने वाली जानकारी संरक्षित करें और केवल इसलिए कि सिस्टम फिर चालू हो गया है, यह वादा न करें कि आप संक्रमण-मुक्त हैं।

अध्याय 1. पहले पंद्रह मिनट

1.1 फ़ाइलें खोलने से पहले अभिलेख खोलें

समस्या का पता लगाने वाला पहला व्यक्ति तिथि, समय और समय-क्षेत्र, अपने द्वारा देखा गया दृश्य, संबंधित सिस्टम, रिपोर्ट करने वाले व्यक्ति और पहले से की गई कार्रवाइयाँ दर्ज करता है। उसे निदान करने की आवश्यकता नहीं है। उसे अज्ञात प्रोग्रामों से रैंसम नोट खोलने, संलग्नक चलाने या यह जाँचने के लिए कि यह वास्तविक है या नहीं, लिंक खोलने से बचना चाहिए। संदेश से बिना संपर्क किए उसकी फ़ोटो लें या उसे दर्ज करें और जहाँ संभव हो मूल वस्तु संरक्षित रखें।

एक घटना समन्वयक और संभावित रूप से उल्लंघित सिस्टमों से बाहर एक संचार चैनल नियुक्त करें। संपर्क सूची में तकनीकी प्रभारी, निरंतरता, विधि, गोपनीयता, संचार, बीमा और आपूर्तिकर्ताओं के संपर्क शामिल हों। यदि कॉर्पोरेट ईमेल प्रभावित हो सकता है, तो संकेतक, क्रेडेंशियल या संवेदनशील रिपोर्ट साझा करने के लिए उसका उपयोग न करें। मौखिक निर्णयों को समय और उत्तरदायी व्यक्ति के साथ दर्ज करें।

प्रारंभिक प्रश्न	त्वरित वर्गीकरण	अगला निर्णय क्या बदलता है
क्या कोई व्यक्ति या महत्वपूर्ण सेवाएँ जोखिम में हैं?	सेवा, निरंतरता और तत्काल परिणाम।	रोकथाम में जीवन और सुरक्षा को साक्ष्य से ऊपर रखा जाता है।
वास्तव में क्या देखा गया?	सर्वर, एप्लिकेशन, व्यवहार, घटनाक्रम और समय।	एक अलार्म को एक घटनाक्रम से अलग करें।

[1] NIST SP 800-61 Rev. 3 (अप्रैल 2025)। CSF 2.0 में समेकित घटना-प्रतिक्रिया सिफ़ारिशें: तैयारी, पहचान, प्रतिक्रिया, पुनर्प्राप्ति और सुधार। यह संशोधन 2 का स्थान लेता है। आधिकारिक ऑनलाइन स्रोत

[2] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. कार्यविधिगत मार्गदर्शिका; विधान या स्वीकार्यता की गारंटी नहीं। आधिकारिक ऑनलाइन स्रोत

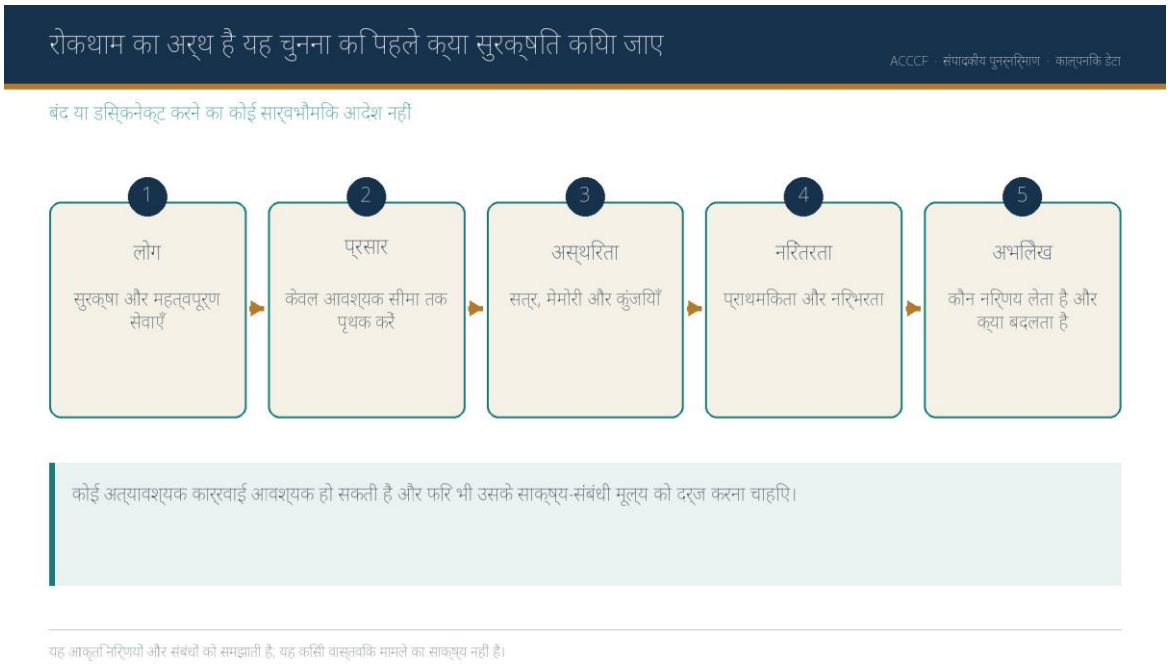
प्रारंभिक प्रश्न	त्वरित वर्गीकरण	अगला निर्णय क्या बदलता है
क्या यह जब से हो रहा है?	सिस्टम, खाते, सेवाएं और देखा गया गतिविधि।	यह अलगाव और तात्कालिकता को निर्धारित करता है।
क्या गायब हो सकता है?	मेमोरी, सत्र, लॉग, लिंक और बैकअप।	परिवर्तन से पहले संरक्षण की प्राथमिकता दें।
कौन निर्णय लेता है और सक्रिय करता है?	जिम्मेदार, प्राधिकारी, पैनल और विकल्प।	विरासत मोड़ कॉल और जवाबदेह से बचें।

1.2 बंद करें, डिस्कनेक्ट करें या चालू रखें

कोई एक सार्वभौमिक उत्तर नहीं है। सिस्टम बंद करने से प्रक्रियाएँ रुक सकती हैं, लेकिन साथ ही विश्लेषण या पुनर्प्राप्ति के लिए आवश्यक मेमोरी, सत्र और कुंजियाँ मिट सकती हैं। नेटवर्क से डिस्कनेक्ट करने से अस्थिर डेटा मिटाए बिना प्रसार और एक्सफ़िल्ट्रेशन सीमित हो सकता है, लेकिन इससे हमलावर द्वारा पहले से नियोजित व्यवहार सक्रिय हो सकता है या कोई महत्वपूर्ण सेवा बाधित हो सकती है। सिस्टम चालू रखने से निरीक्षण और लाइव अधिग्रहण संभव होता है, लेकिन डेटा में बदलाव और नुकसान का विस्तार जारी रह सकता है।

निर्णय सिस्टम की स्थिति, प्रसार, सेवा, एन्क्रिप्शन, अस्थिर डेटा, उपकरणों और प्राधिकरण पर आधारित होता है। यदि लाइव अधिग्रहण की क्षमता है, तो बंद करने से पहले उसका मूल्यांकन करें। यदि ऐसी क्षमता नहीं है, तो इस सीमा को दर्ज करें और सुरक्षा के अनुरूप सबसे कम विनाशकारी रोकथाम चुनें। प्रशिक्षित न होने पर प्रथम उत्तरदाता को मेमोरी फोरेंसिक का अनुकूलन नहीं करना चाहिए; वह स्थिति की फ़ोटो ले सकता है, प्रक्रिया के अनुसार पृथक कर सकता है और मामला आगे भेज सकता है।

> **अपवादात्मक निर्णय**
> यदि किसी व्यक्ति का जीवन या कोई अत्यावश्यक सेवा सिस्टम पर निर्भर है, तो सुरक्षा में देरी का कारण साक्ष्य संरक्षण को नहीं बनाया जाता। आवश्यकता, विचार किए गए विकल्पों और पहले तथा बाद में संरक्षित किए जा सकने वाले साक्ष्य को दर्ज करें।



चित्र 1. रोकथाम का अर्थ है यह चुनना कि पहले क्या सुरक्षित किया जाए। बंद या डिस्कनेक्ट करने का कोई सार्वभौमिक आदेश नहीं है। संपादकीय पुनर्संरेखण; वास्तविक साक्ष्य नहीं है।

अध्याय 2. दायरा, प्रसार और प्राथमिकताएँ

2.1 दिखाई देने वाला सिस्टम ही पूरी घटना नहीं है

एन्क्रिप्ट की गई फ़ाइलों वाला टर्मिनल किसी ऐसी शृंखला की अंतिम कड़ी हो सकता है जो कई सप्ताह पहले किसी दूसरे खाते से शुरू हुई थी। मानचित्र में पहचान, VPN, ईमेल, सर्वर, हाइपरवाइज़र, बैकअप, आपूर्तिकर्ता, काम के लिए अधिकृत निजी उपकरण, प्रशासनिक सिस्टम और क्लाउड सेवाएँ शामिल हैं। दायरे का विस्तार साक्ष्य के आधार पर किया जाता है, "सब कुछ उल्लंघित है" कहकर नहीं; इस वाक्यांश से अनावश्यक शटडाउन हो सकते हैं और प्राथमिकताएँ छिप सकती हैं।

महत्व, स्वामी, स्थिति, संभावित उल्लंघन, निर्भरता, लॉग का स्रोत और निर्णय सहित परिसंपत्तियों की एक मैट्रिक्स बनाएँ। एक सिस्टम संक्रमित हो सकता है, दूसरा केवल इसलिए अनुपलब्ध हो सकता है क्योंकि किसी स्विच को पृथक किया गया है, और तीसरा स्वस्थ होते हुए भी बंद सर्वर पर निर्भर हो सकता है। रिपोर्ट इन स्थितियों में अंतर करती है ताकि उन्हें एक ही पुष्ट संक्रमण के रूप में प्रस्तुत न किया जाए।

स्थिति	आवश्यक प्रमाण	दस्तावेज़ीकरण निर्णय
पुष्ट	परिसंपत्ति पर सत्यापनीय आर्टिफ़ैक्ट, निष्पादन, लॉग या एन्क्रिप्शन।	प्राथमिकता के अनुसार रोकथाम और सुरक्षण करें।
संदिग्ध	संबद्ध संकेतक, बिना पर्याप्त पुष्टि के।	निगरानी करना, पुनर्वा रूप से जोड़ना या अधिग्रहण करना।
निर्भरता से प्रभावित	किसी अन्य क्रिया या प्रणाली के कारण सेवा रोक दी गई।	इसे संक्रमित के रूप में लेबल किए बिना निर्भरता को पुनर्प्राप्त करना।
दायरे में कोई संकेत नहीं	क्वेरी, फ़िल्टर, जवाब और जोड़े गए खाते।	उस क्वेरी से बाहर सिस्टम को संक्रमण-मुक्त घोषित न करें।
अज्ञात	पहुँच, रिकॉर्ड या इम्पैक्ट का कमी।	उत्तरदायी व्यक्ति और निष्कर्ष को सीमा निर्धारित करें।

2.2 शोर के आधार पर नहीं, सेवा के आधार पर प्राथमिकता

निरंतरता मैट्रिक्स अत्यावश्यक प्रक्रियाओं, अधिकतम सहनीय व्यवधान समय, संचालन के लिए आवश्यक न्यूनतम डेटा, निर्भरताओं, उत्तरदायी व्यक्तियों और अस्थायी मैनुअल मार्गों की पहचान करती है। बहुत-से अलर्ट पैदा करने वाला सर्वर उस डायरेक्टरी से कम प्राथमिक हो सकता है जिस पर सभी निर्भर हैं। यह निर्णय वास्तविक प्रभाव के आधार पर होता है कि पहले क्या रिस्टोर करना है, न कि रैंसम नोट में कौन-सी फ़ाइल पहले दिखाई दी।

प्रतिक्रिया और निरंतरता टीमें एक ही कालक्रम पर काम करती हैं, लेकिन उनके डिलिवरेबल अलग होते हैं। सुरक्षा टीम को जानना होता है कि कौन-सा दीर्घस्थायित्व मौजूद है; निरंतरता टीम को यह जानना होता है कि कौन-सा संस्करण पुनर्प्राप्त किया जा सकता है और उसकी कौन-सी निर्भरताएँ हैं। मिलान से यह रोका जाता है कि कोई ऐसा सिस्टम रिस्टोर हो जो घटना के स्रोत से फिर जुड़ जाए, या अजानकारी के कारण कोई स्वस्थ सेवा बंद रहे।

> **काल्पनिक मामला**
> एक कंपनी दस्तावेज़ सर्वर पर एन्क्रिप्शन का पता लगाती है। पेरोल एन्क्रिप्ट नहीं हुआ है, लेकिन वह काम नहीं करता क्योंकि वह उसी डायरेक्टरी पर निर्भर है। टीम पेरोल को संक्रमित के रूप में चिह्नित नहीं करती: वह निर्भरता के कारण प्रभावित होना दर्ज करती है। सेवाओं को फिर जोड़ने से पहले पुनर्प्राप्ति में पहचान और लॉग को प्राथमिकता दी जाती है।

अध्याय 3. रोकथाम के दौरान संरक्षण

3.1 मेमोरी, डिस्क, लॉग और स्थिति

संरक्षण की प्राथमिकता अस्थिरता और प्रश्नों का उत्तर देने की क्षमता के आधार पर तय होती है। मेमोरी में प्रक्रियाएँ, कनेक्शन, कुंजियाँ या सत्र के अंश हो सकते हैं; डिस्क में फ़ाइलें और आर्टिफैक्ट रहते हैं; लॉग घटनाओं की व्याख्या करते हैं; कॉन्फ़िगरेशन दिखाता है कि सिस्टम कैसे जुड़ा था। हर मामले में प्रत्येक परिसंपत्ति का पूर्ण अधिग्रहण आवश्यक नहीं है। उन स्रोतों का चयन करें जो उत्पत्ति, प्रसार, दीर्घस्थायित्व, एक्सफ़िल्ट्रेशन और पुनर्प्राप्ति के बीच अंतर स्पष्ट कर सकें।

प्रत्येक अधिग्रहण में स्रोत, विधि, उपकरण और संस्करण, तिथि और समय-क्षेत्र, प्राधिकरण, कवरेज, आउटपुट, त्रुटियाँ और सत्यापन बताएँ। आउटपुट को मान्य मानने से पहले उसे खोलें। मौजूद होने पर भी जो फ़ाइल पढ़ी नहीं जा सकती, वह उपयोगी साक्ष्य नहीं है। अपूर्ण अधिग्रहण या असंगत उपकरण सहित सभी विसंगतियाँ अभिलेख में रखें। दोहराए जाने पर पहला प्रयास मिटाने के बजाय उससे संबंधित एक नई वस्तु बनाई जाती है।[3][4]

3.2 खाते निलंबित करने या पुनः इंस्टॉल करने से पहले लॉग

किसी खाते को अक्षम करने से पहले साइन-इन लॉग, फ़ैक्टर नामांकन, पुनर्प्राप्ति में बदलाव, ईमेल नियम, प्रतिनिधिकरण, टोकन और उपलब्ध प्रशासनिक गतिविधि निर्यात करें। पुनः इंस्टॉल करने से पहले इमेज, कॉन्फ़िगरेशन, लॉग, कार्य और संबंधित आर्टिफैक्ट संरक्षित करें। आपात स्थिति में ये कार्रवाइयाँ संभव न भी हों; आदर्श अनुक्रम गढ़ने के बजाय दर्ज करें कि क्या खोया और क्यों।

दायरे पर चर्चा चलते समय रिटेंशन रोटेट हो सकता है। आपूर्तिकर्ता से अवधि, खाते, फ़ील्ड, समय-क्षेत्र, मूल प्रारूप, डेटा शब्दकोश, फ़िल्टर और सीमाएँ बताते हुए संरक्षण का अनुरोध करें। प्राप्त सामग्री को पूर्ण EML, मुख्य भाग, हेडर और संलग्नकों सहित संरक्षित करें। यदि आपूर्तिकर्ता प्रत्येक फ़ाइल का हैश देता है, तो उसकी स्थानीय जाँच करें और स्रोत में बदलाव किए बिना हर अंतर दर्ज करें।[5]

3.3 रैंसम नोट और संपर्क चैनल के साक्ष्य

रैंसम नोट को एक वस्तु के रूप में संरक्षित करें: स्क्रीनशॉट, मूल फ़ाइल यदि मौजूद हो, स्थान, नाम, देखने की तिथि, प्रारूप और सिस्टम से संबंध। इसके पाठ में एक्सफ़िल्ट्रेशन, निगरानी या पहुँच के समय के बारे में झूठे दावे हो सकते हैं। इसे हमलावर का बयान मानें, सिद्ध तथ्य नहीं। बिना कोई लेनदेन किए या निर्देशों का पालन किए भुगतान और संपर्क पहचानकर्ता दर्ज करें।

वस्तु	आवश्यक जानकारी	टाली गई त्रुटि
रैंसम नोट	मूल वस्तु, स्थान, तिथि, संबंध और सांख्यिकी सामग्री।	उसके पाठ को तकनीकी स्वीकारोक्ति मानना।
एन्क्रिप्ट की गई फ़ाइल	निर्धारित नमूना, नाम, आकार, पिछली स्थिति और संरक्षित प्रति।	कई फ़ाइलें खोलना और मूल बदल देना।
घटना संबंधी ईमेल	EML, संलग्नक, हेडर, तिथि और प्राप्तकर्ता।	संदेश को केवल एक स्क्रीनशॉट समझना।
सहायता खाता	सूचना, जानकारी, गतिविधि और निर्यात।	पहुँच साझा करना या घटना को दायरा बढ़ाना।
बैकअप	तिथि, सत्यापन, कवरेज, स्थान और पहुँच की स्थिति।	संदूषण का मूल्यांकन किए बिना उसे कनेक्ट करना।

[3] ISO/IEC 27037:2012. डिजिटल साक्ष्य की पहचान, संग्रह, अधिग्रहण और संरक्षण के दिशा-निर्देश। ISO ने इस संस्करण को प्रभावी माना है। आधिकारिक ऑनलाइन स्रोत

[4] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. कार्यविधिगत मार्गदर्शिका; विधान या स्वीकार्यता की गारंटी नहीं। आधिकारिक ऑनलाइन स्रोत

[5] RFC Editor. RFC 5322, Internet Message Format: संदेश की संरचना, हेडर और मुख्य भाग। यह ईमेल संरक्षित करने और समझने का तकनीकी संदर्भ है, मानव पहचान का स्वतः प्रमाण नहीं। आधिकारिक ऑनलाइन स्रोत

प्रयोगशाला सुरक्षा

नमूनों को निजी उपकरणों या उत्पादन नेटवर्क पर न चलाएँ। गतिशील विश्लेषण के लिए पृथक वातावरण, उद्देश्य, प्राधिकरण, नेटवर्क नियंत्रण और अभिलेख आवश्यक हैं। प्रथम प्रतिक्रिया के लिए प्रायः नमूना संरक्षित करना और मामला विशेषज्ञ को सौंपना पर्याप्त होता है।



चित्र 2. एस स्रात जा राकथाम क दारान नष्ट नहा हान चाहए। प्रत्यक आधग्रहण अपना कवरज आर सामा बताता ह। सपादकाय पुनानमाण; वास्तावक साक्ष्य नहा ह।

अध्याय 4. जाँच: उत्पत्ति, दीर्घस्थायित्व और एक्सफ़िल्ट्रेशन

4.1 स्पष्ट अनिश्चितता के साथ कालक्रम

कालक्रम में प्रत्येक मूल तिथि, समय-क्षेत्र, स्रोत, परिशुद्धता और रूपांतरण बनाए रखें। रूपांतरण समझाए बिना UTC लॉग, गलत समय वाले कंप्यूटर और स्थानीय ईमेल को इस तरह क्रमबद्ध न करें मानो वे एक ही घड़ी साझा करते हैं। पहली पहचान आवश्यक रूप से पहली पहुँच नहीं होती। किसी फ़ाइल के संशोधन की तिथि यह सिद्ध नहीं करती कि एन्क्रिप्टर कब चला; यह उसके परिणाम के लिखे जाने का संकेत दे सकती है।

देखी गई घटनाओं, किसी व्यक्ति के बयानों, गणना से प्राप्त तथ्यों और निष्कर्षों को अलग रखें। निष्कर्ष को लॉग का रूप न दें। यदि किसी चरण का स्रोत नहीं है, तो लिखें “दायरे में प्रमाणित नहीं”। लॉग की अनुपस्थिति का कारण रोटेशन, कॉन्फ़िगरेशन, फ़िल्टर या विलोपन हो सकता है; यह आवश्यक नहीं कि घटना नहीं हुई हो।

4.2 प्रवेश और दीर्घस्थायित्व की परिकल्पनाएँ

परिकल्पनाओं में चुराए गए क्रेडेंशियल, उजागर भेद्यता, दुर्भावनापूर्ण ईमेल, आपूर्तिकर्ता, बाहरी उपकरण या इनका संयोजन शामिल हो सकता है। विश्लेषण में प्रत्येक परिकल्पना की तुलना उन स्रोतों से करें जो उसे कमजोर कर सकते हैं: प्रमाणीकरण, फ़ैक्टर में बदलाव, नियम, प्रक्रियाएँ, कार्य, सेवाएँ, नए खाते, कनेक्शन और प्रशासनिक गतिविधि। चुनी गई व्याख्या वह है जो सबसे अधिक तथ्यों के अनुरूप और सबसे कम विरोधाभासों वाली हो, सबसे सनसनीखेज़ नहीं।

परिकल्पना	खोट या कमजोर करने वाले स्रोत	निष्कर्ष का खतरा
उल्लंघित पद खाता।	जासूसी सत्र, प्रमाणीकरण कारक, उपकरण, पुनर्प्राप्ति और अनुमानित भौगोलिक स्थिति।	इस्तेमाल किया गया खाता किसी व्यक्ति की पहचान नहीं करता है।

परिकल्पना	सूट या कमजोर करने वाला स्रोत	निष्कर्ष का सीमा
सांयोगिक मंथन	सत्करण, एक्सपोज़र, लॉग, निर्धारित परीक्षण और पैच की तिथि।	मंथन की उपस्थिति उसके शोषण का प्रमाण नहीं है।
दुर्भावनापूर्ण मेल	EMR, सेलनिक, खोलने और निष्पादन का टेलीमेट्री।	प्राप्त निष्पादन का प्रमाण नहीं है।
उल्लंघित जीवंतता	दूरस्थ पहुंच, मूनकाई, परिवर्तन और समय-सीमा।	अनुबंधक समय प्रवेश-मार्ग सिद्ध नहीं करता।
दायित्वाधित्व	खाते, कोष, सेवाएं, फुटेज, नियम और आर्टिफैक्ट।	केवल दिखाई देने वाली फ़ाइलों को उन्मूलन न करें।

4.3 एक्सफ़िल्ट्रेशन: साक्ष्य की अनुपस्थिति और अनुपस्थिति का साक्ष्य

एक्सफ़िल्ट्रेशन का मूल्यांकन करने के लिए कनेक्शन, गंतव्य, डेटा की मात्रा, संपीड़न, क्लाउड सिंक्रनाइज़ेशन, ईमेल, नियम, स्थानांतरण सेवाएँ, प्रॉक्सी लॉग और उपलब्ध होने पर DNS की समीक्षा करें; हमलावर के बयानों को एक अलग परिकल्पना मानें। अधिक मात्रा बैकअप या वैध गतिविधि का भी हो सकती है; ट्रैफ़िक न मिलने का अर्थ लॉग की अनुपस्थिति, जाँचा न गया एन्क्रिप्शन या कवरेज से बाहर कोई चैनल भी हो सकता है।

निष्कर्ष में अंतर करें: स्थानांतरण का साक्ष्य, संगत संकेत, अपर्याप्त डेटा या परिभाषित कवरेज के भीतर देखी गई अनुपस्थिति। केवल इसलिए कि फ़ायरवॉल में एक्सफ़िल्ट्रेशन नहीं दिखता, “कोई एक्सफ़िल्ट्रेशन नहीं हुआ” न कहें। “हम आपका डेटा प्रकाशित करेंगे” को भी डेटा बाहर जाने का प्रमाण न मानें। यदि प्रकाशित कोई नमूना मिले, तो उसे फैलाए या अनावश्यक जानकारी डाउनलोड किए बिना दस्तावेज़ित करें।

> **प्रमाण-समर्थित प्रस्तुति**
> “इन तिथियों के बीच और इन फ़ील्ड वाले प्रॉक्सी लॉग में घटना से जुड़ा कोई स्थानांतरण नहीं देखा गया। कवरेज में जाँचे न गए एन्क्रिप्टेड चैनल, अन्य आपूर्तिकर्ता या पिछली अवधियाँ शामिल नहीं हैं; इसलिए एक्सफ़िल्ट्रेशन की पूर्ण अनुपस्थिति का दावा नहीं किया जा सकता।”

अध्याय 5. उन्मूलन और फ़िद्या पर निर्णय

5.1 केवल लक्षण नहीं, कारण का उन्मूलन करें

उन्मूलन में खाते, पुनर्प्राप्ति के तरीके, नियम, दूरस्थ पहुँच, दीर्घस्थायित्व, भेद्यताएँ, रहस्य और आपूर्तिकर्ता पहुँच-मार्ग शामिल हैं। यदि टोकन, सत्र या कुंजियाँ बनी रहती हैं तो केवल पासवर्ड बदलना पर्याप्त नहीं है। एन्क्रिप्टर हटाने से प्रवेश-बिंदु नहीं हटता। उपायों को स्रोतों और परीक्षणों से सत्यापित करें और संचालन पर उनके प्रभाव दर्ज करें।

यदि कारण ज्ञात नहीं है, तो यह स्पष्ट करें। संगठन उसी सिस्टम को “साफ़” करने के बजाय विश्वसनीय वातावरण से पुनर्निर्माण चुन सकता है। निर्णय जोखिम और साक्ष्य पर आधारित हो, बचत के दिखावे पर नहीं। पुनः इंस्टॉल किए गए सिस्टम में नया कॉन्फ़िगरेशन, क्रेडेंशियल और निगरानी दी जाती है; उसे उसी स्थिति में नहीं लौटाया जाता जिसने घटना को संभव बनाया था।

5.2 भुगतान करें या न करें: दस्तावेज़ित निर्णय, आवेग नहीं

भुगतान का निर्णय संगठन और उसके कानूनी सलाहकारों, बीमाकर्ताओं तथा सक्षम प्राधिकरणों का है। इसमें वैधता, सैंक्शन, धन का स्रोत और गंतव्य, निरंतरता की क्षमता, लोगों की सुरक्षा, फिर से जबरन वसूली की संभावना और पुनर्प्राप्ति की गारंटी न होने पर विचार होना चाहिए। यह मैनुअल भुगतान या हमलावर से संपर्क की सिफ़ारिश नहीं करता; यह ऐसी संरचना देता है कि दबाव में निर्णय किसी एक व्यक्ति पर निर्भर न रहे।

कारक	जिस प्रश्न का उत्तर देना है	निर्णय को आकार देने वाले साक्ष्य
पवता	क्या कोई लागू निषेध, सफ़ारी या प्रतिषेध है?	अधीनस्थ कानून, विश्लेषण और अनुमोदन चैनल।
निरंतरता	क्या कोई दूसरा व्यवहार मौजूद है और उसे कितना समय लगता है?	बेसलाइन परीक्षण, विकल्प और व्यवधान की लागत।
पुनर्प्राप्ति	क्या वादा किया जाता है और क्या साबित किया जा सकता है?	कोई लिखित गारंटी नहीं, तकनीकी मूल्यांकन और सीमाएं।
मानव जोखिम	क्या कोई अतिरिक्त खतरा या संवेदनशील डेटा है?	सुरक्षा और प्रभावित लोगों की रक्षा की प्राथमिकता।
पुनरावृत्ति	क्या प्रोत्साहन या एक्सपोज़र शेष रहता है?	दस्तावेज़ीकृत जोखिम और जोड़ की पहचान।
प्राधिकरण	कौन निर्णय ले सकता है और लिख कर सकता है?	गणपूर्ति, जोखिम और एकमात्र अधिकृत चैनल।

5.3 संचार और बाध्यताएँ

अधिसूचना के मूल्यांकन में ग्राहकों, डेटा विषयों, नियामकों, बीमाकर्ताओं, भागीदारों और प्राधिकरण को अलग-अलग देखें। प्रत्येक क्षेत्राधिकार और अनुबंध की सीमा-रेखाएँ और समय-सीमाएँ अलग होती हैं। तकनीकी जानकारी इस तरह तैयार करें कि तथ्य, अनिश्चितता और उपाय समझाए जा सकें, लेकिन नुकसान बढ़ाने वाले विवरण उजागर न हों। सार्वजनिक संचार संरक्षण से आगे न बढ़े और किसी संदेह को कारण की घोषणा न बना दे।

मेक्सिको में, लागू प्रावधानों के अंतर्गत ऋण संस्थानों की घटनाओं की जाँच और सूचना, अभिलेख तथा संरक्षण से जुड़ी विशिष्ट बाध्यताएँ हैं; पेरू में SBS पर्यवेक्षित संस्थाओं से संरक्षण और फोरेंसिक विश्लेषण अपेक्षित करता है; अर्जेंटीना में Comunicación A 8280 अपने व्यवस्था-ढाँचे में प्रतिक्रिया और अंतिम रिपोर्ट पर चर्चा करता है। इन समय-सीमाओं को हर संगठन या दूसरे देश पर लागू न करें।[678]

निश्चितता न गढ़

कार्यकारी रिपोर्ट में बताया जा सकता है कि क्या ज्ञात है, क्या किया जा रहा है और क्या अभी निर्धारित करना बाकी है। उसे आतंक और कृत्रिम निश्चितता के बीच चुनाव नहीं करना है। उसे प्रमाण-समर्थित कालक्रम और स्पष्ट उत्तरदायी व्यक्ति चाहिए।

अध्याय 6. पुनर्प्राप्ति और निरंतरता

6.1 पुनर्प्राप्ति बिंदु का चयन और सत्यापन

सबसे नए बैकअप में दीर्घस्थायित्व या क्षतिग्रस्त फ़ाइलें हो सकती हैं; सबसे पुराने बैकअप से वैध संचालनों का डेटा छूट सकता है। तिथि, कवरेज, अखंडता, पहुँच, इतिहास और संगतता की तुलना करें। मूल बैकअप संरक्षित रखें और पृथक वातावरण में नियंत्रित प्रति पर काम करें। कुंजियाँ अलग चैनल से दें और उन्हें कार्यवाही-विवरण में न लिखें।

सत्यापन में जाँचें कि प्रति खुलती है, अपेक्षित वस्तुएँ रखती है, माउंट हो सकती है, संस्करणों में सुसंगतता है और उल्लंघन के ज्ञात संकेतक नहीं दिखाती। इससे यह सिद्ध नहीं होता कि वह पूरी तरह संक्रमण-मुक्त है; यह सिद्ध होता है कि उसने निर्धारित परीक्षण पास किए। यदि प्रति में त्रुटियाँ हैं, तो तय करें कि वे उद्देश्य को प्रभावित करती हैं या नहीं और उनका विवरण संरक्षित रखें।

[6]ऋण संस्थानों पर लागू सामान्य प्रावधान, अनुच्छेद 316 Bis, 316 Bis 1, 316 Bis 10 से 17: प्रमाण-पत्र, एन्क्रिप्शन, पहुँच, घटनाएँ, विसंगतियाँ, लॉग और समीक्षाएँ। आधिकारिक ऑनलाइन स्रोत

[7]पेरू। SBS 504-2021, अनुच्छेद 12.6.g, 15 और 17.3–17.4: संरक्षण, रिपोर्टिंग और फोरेंसिक विश्लेषण, नामांकन, प्रमाणीकरण और संचालन के अभिलेख। आधिकारिक ऑनलाइन स्रोत

[8]अर्जेंटीना। BCRA Comunicación A 8280: साइबर-घटनाओं पर प्रतिक्रिया और पुनर्प्राप्ति; रोकथाम, पुनर्प्राप्ति और समाधान के बाद पाँच कैलेंडर दिनों के भीतर अंतिम रिपोर्ट। आधिकारिक ऑनलाइन स्रोत

6.2 चरणबद्ध पुनर्प्राप्ति

पृथक वातावरण में न्यूनतम सेवाओं से शुरुआत करें और काल्पनिक डेटा या परीक्षण खातों का उपयोग करें। फिर पहचान, अनुमतियाँ, एप्लिकेशन, एकीकरण, पढ़ना और लिखना, निर्यात तथा निगरानी परखें। तभी क्रमिक विस्तार की अनुमति दें। पहली पुनर्प्राप्ति की प्रयोगशाला के रूप में उत्पादन नेटवर्क का उपयोग न करें।

चरण	स्वीकृति मानदंड	साक्ष्य
न्यूनतम बुनियादी ढाँचा	सत्यापित घटक और सॉफ़्टवेयर, कोई ज्ञात दोषग्रस्त नहीं।	इन्वेंटरी और कॉन्फ़िगरेशन।
डेटा	पठनीय फ़ाइलें, सही फ़ॉर्मेट और संस्करण।	नमूना, मानिफ़ेस्ट और गणना।
एप्लिकेशन	ऐप्स और अनुमतियाँ काल्पनिक खातों से काम करती हैं।	परीक्षण मामले और परिणाम।
एकीकरण	आवश्यक निर्भरताएँ अनुपातित माँग के बिना उत्तर देती हैं।	लॉग और कनेक्शन।
निरीक्षण	निर्धारित अवधि में कोई असामान्य गतिविधि नहीं दिखाई देती है।	अलर्ट, क्वेरी और समीक्षा।
बाहर निकलना	प्रभारी दल औपचारिक और अगला समाधान स्वीकार करता है।	बाहर निकलने का प्रमाण-पत्र और निगरानी।

6.3 जानकारी का मिलान और सीख

अंतिम पूर्ण बैकअप और पहचान के बीच किए गए संचालनों का पुनर्निर्माण आवश्यक हो सकता है। बाहरी अभिलेख, रसीदें, ईमेल, संदेश और तीसरे पक्ष के दस्तावेज़ों का मिलान स्रोत में बदलाव किए बिना करें। अंतर दर्ज करें; उन्हें वास्तविक डेटा का रूप दिए गए अनुमानों से न भरें।

सीखा गया सबक प्रक्रिया बदलता है: नए रिटेंशन नियम, फ़िशिंग-प्रतिरोधी प्रमाणीकरण, सेगमेंटेशन, अपरिवर्तनीय प्रतियाँ, रिस्टोर परीक्षण, संपर्क सूची, विशेषाधिकारों की सीमा या अभ्यास। यदि घटना एक प्रस्तुति के साथ समाप्त होती है लेकिन कोई व्यवहार नहीं बदलता, तो अगला संकट उसी क्रम को दोहराएगा।

> **समापन मानदंड**
> पुनर्प्राप्ति का अर्थ है यह साक्ष्य रखते हुए फिर संचालन शुरू करना कि नियंत्रण काम करते हैं और जो अभी अज्ञात है उसकी ईमानदार व्याख्या करना। समापन में लोग, सिस्टम, डेटा, आपूर्तिकर्ता और बाद की समीक्षा शामिल हैं।



चित्र 3. रिस्टोर करने का अर्थ विश्वास की पुनर्प्राप्ति नहीं है। बहाल किए जाने की जाँच चरणों और स्वीकृत मानदंडों से की जाती है। संपादकीय पुनर्निर्माण; वास्तविक साक्ष्य नहीं है।

परिशिष्ट A. कानूनी ढाँचा और क्षेत्रीय अभिलेख

घटना में इलेक्ट्रॉनिक साक्ष्य, डेटा संरक्षण, अनुबंध, वित्तीय बाध्यताएँ और निरंतरता नियम शामिल हो सकते हैं। इन पहलुओं का अलग-अलग विश्लेषण करें। कोई क्षेत्रीय नियम सार्वभौमिक बाध्यता नहीं बनाता और रिटेंशन की अवधि सब कुछ अनिश्चित काल तक रखने का अधिकार नहीं देती। 10 नवंबर 2026 तक दस्तावेज़ समीक्षा; वास्तविक अभिलेख के लिए प्रभावी वैधता, लागू व्यक्ति, विषय और चैनल सत्यापित करना आवश्यक है।

क्षेत्राधिकार	कार्यात्मक स्रोत	उपयोग की सीमा
मेक्सिको	CCom. 89–94 और 1205, CFPC 210-A / CNPCF 348–350 संक्रमण के अनुसार; CNBV 316 Bis श्रृंखला, शामिल संस्थाओं के लिए; LFPDPPP व्यक्तिगत डेटा के लिए।	इलेक्ट्रॉनिक दस्तावेज़, प्रक्रिया, बीमा और गोपनीयता को अलग रखें। CNPCF की घोषणा जाँचें।
स्पेन	Reglamento IOFE, CPC 188–197, SBS 504-2021 और 2286-2024, पर्यवेक्षित संस्थाओं के लिए।	Ley 27/209 का पूरा दस्तावेज़ व्यवस्था न मानें और CNBV की समय-सीमाएँ नकल न करें।
चिली	Ley 19.799, RAN 20-7, 20-8, 20-10, सेवा और सेवा के अनुसार।	निरंतरता, आउटसोर्सिंग और घटनाओं को अलग न करें।
अर्जेंटीना	Ley 25.506, CCyC 318–319, BCRA A 7783 और A 8280।	अपना समय-सीमाएँ और लागू व्यक्ति, प्रमाणीकरण प्राधिकरण के समान नहीं है।
कोलंबिया	Ley 527, प्रशासनिक कार्यवाहियों के लिए CPACA, SFC विनियमन के विशिष्ट खंड की पुष्टि अभी करनी है।	न पढ़ पारंपरे से घटनाओं की आवश्यकताएँ न गढ़।
इक्वाडोर	Ley 67, LOPDP, जहाँ लागू हो, मुकदमा प्रमाण की व्यवस्था।	आपसूचना और संरक्षण डेटा प्रासंगिक और क्षेत्र पर निर्भर करते हैं।
स्पेन / यूरोपीय संघ	eIDAS, LEC 326 और 384, RGPD, मुकदमा सेवाओं के लिए RD-ley 19/2018।	दस्तावेज़, प्रक्रिया, गोपनीयता और अनधिकृत संचालन को अलग रखें।

*तालिका के स्रोत:*9101112131415161718192021222324252627

लॉग के अनुरोध में कार्य, अवधि, संदर्भ, फ़ील्ड, प्रारूप, समय-क्षेत्र और डिलीवरी की विधि बताएँ। उद्देश्य सभी सर्वर माँगना नहीं, बल्कि वे घटनाएँ प्राप्त करना है जो ठोस प्रश्नों का उत्तर दे सकें। कस्टडी शृंखला में यह अभिलेख रहता है कि कौन सौंपता है, कौन प्राप्त करता है, उसमें कौन-सी वस्तु है, उसकी जाँच कैसे होती है और कौन-सी सीमाएँ हैं।

परिशिष्ट B. प्रतिक्रिया प्रारूप

B.1 घटना का कालक्रम

फ़ील्ड	जानकारी जो भरनी है	निर्देश
घटना	देखा गया, बताया गया, गणना किया गया या निकाला गया निष्कर्ष।	तथ्यों में मिलाएँ।
मूल समय और समय-क्षेत्र	मूल पाठ, रूपांतरण और स्रोतकर्ता।	स्रोत को अधिलेखित न करें।
परिसंपत्ति और स्रोत	वस्तु, प्रणाली, पहचानकर्ता और स्थान।	मानफ़ेस्ट तथा ट्रेसाबिलिटी।
कार्रवाई और उत्तरदायी व्यक्ति	क्या हुआ, किसने फ़ैसला किया और किसने उसे निष्पादित किया।	प्राधिकरण और साक्ष्य।
परिणाम	आउटपुट, त्रुटियाँ और स्थिति में बदलाव।	विसंगतियों में छिपाएँ।

[9]मेक्सिको का वाणिज्य संहिता, अनुच्छेद 89–94 और 1205: तटस्थता, अट्रिब्यूशन, लिखित रूप, मूल रूप, अखंडता, पहुँच-योग्यता और डेटा संदेशों की स्वीकार्यता। आधिकारिक संकलन। आधिकारिक ऑनलाइन स्रोत

[10]संघीय नागरिक प्रक्रिया संहिता, अनुच्छेद 210-A: विधि की विश्वसनीयता, अट्रिब्यूशन, पहुँच-योग्यता और इलेक्ट्रॉनिक जानकारी की अखंडता। 07-06-2023 के अध्यादेश से निरस्त संहिता, क्रमिक संक्रमण व्यवस्था के अधीन। आधिकारिक ऑनलाइन स्रोत

[11]राष्ट्रीय नागरिक और पारिवारिक प्रक्रिया संहिता, अनुच्छेद 348–350। 15-01-2026 के संशोधन सहित संकलन। इसका क्रमिक कार्यान्वयन घोषणापत्रों पर निर्भर है। आधिकारिक ऑनलाइन स्रोत

[12]ऋण संस्थानों पर लागू सामान्य प्रावधान, अनुच्छेद 316 Bis, 316 Bis 1, 316 Bis 10 से 17: प्रमाण-पत्र, एन्क्रिप्शन, पहुँच, घटनाएँ, विसंगतियाँ, लॉग और समीक्षाएँ। आधिकारिक ऑनलाइन स्रोत

[13]पेरू। IOFE का विनियम, DS 052-2008-PCM, अनुच्छेद 3 और 4: डिजिटल हस्ताक्षर वाले इलेक्ट्रॉनिक दस्तावेज़ों की अपेक्षा और स्वीकार्यता। आधिकारिक ऑनलाइन स्रोत

[14]पेरू। नागरिक प्रक्रिया संहिता, अनुच्छेद 188–197 और 245.5: उद्देश्य, वैधता, साधन, प्रमाण-भार, मूल्यांकन और तकनीकी साधनों से तिथि। आधिकारिक ऑनलाइन स्रोत

[15]पेरू। SBS 504-2021, अनुच्छेद 12.6.g, 15 और 17.3–17.4: संरक्षण, रिपोर्टिंग और फोरेंसिक विश्लेषण, नामांकन, प्रमाणीकरण और संचालन के अभिलेख। आधिकारिक ऑनलाइन स्रोत

[16]चिली। इलेक्ट्रॉनिक दस्तावेज़ों और इलेक्ट्रॉनिक हस्ताक्षर संबंधी Ley 19.799, अनुच्छेद 1–5: समतुल्यता, लिखित रूप, साधारण/उन्नत हस्ताक्षर, तिथि और प्रमाण-मूल्य। आधिकारिक ऑनलाइन स्रोत

[17]चिली. मानकों का अद्यतन संकलन, अध्याय 20-7, 20-8 और 20-10: आउटसोर्सिंग, परिचालन घटनाएं, सूचना सुरक्षा और साइबर सुरक्षा। आधिकारिक ऑनलाइन स्रोत

[18]अर्जेंटीना। डिजिटल हस्ताक्षर संबंधी Ley 25.506, अनुच्छेद 1 और 5–9: डिजिटल दस्तावेज़, अज्ञात इलेक्ट्रॉनिक हस्ताक्षर का आह्वान करने पर प्रमाण-भार और सीमांकित धारणाएँ। आधिकारिक ऑनलाइन स्रोत

[19]अर्जेंटीना। नागरिक और वाणिज्यिक संहिता, अनुच्छेद 318–319: किसी भी माध्यम से पत्राचार तथा तकनीकी माध्यमों और प्रक्रियाओं की विश्वसनीयता का मूल्यांकन। आधिकारिक ऑनलाइन स्रोत

[20]अर्जेंटीना। BCRA Comunicación A 8280: साइबर-घटनाओं पर प्रतिक्रिया और पुनर्प्राप्ति; रोकथाम, पुनर्प्राप्ति और समाधान के बाद पाँच कैलेंडर दिनों के भीतर अंतिम रिपोर्ट। आधिकारिक ऑनलाइन स्रोत

[21]कोलंबिया। Ley 527 (1999), अनुच्छेद 5–13, 16–25 और 28: डेटा संदेश, लिखित रूप, मूल रूप, अखंडता, स्वीकार्यता, संरक्षण, प्रेषण, प्राप्ति और डिजिटल हस्ताक्षर। आधिकारिक ऑनलाइन स्रोत

[22]इक्वाडोर। इलेक्ट्रॉनिक वाणिज्य, इलेक्ट्रॉनिक हस्ताक्षर और डेटा संदेश संबंधी Ley 67, अनुच्छेद 2, 6–8, 10–16: समतुल्यता, लिखित रूप, मूल रूप, संरक्षण, उत्पत्ति, प्रेषण, प्राप्ति और इलेक्ट्रॉनिक हस्ताक्षर। आधिकारिक ऑनलाइन स्रोत

[23]इक्वाडोर। व्यक्तिगत डेटा संरक्षण का संगठित कानून, Registro Oficial Suplemento 459, 26-05-2021। अनुच्छेद 10, 37–44: सिद्धांत, सुरक्षा उपाय, डिज़ाइन से संरक्षण, जोखिम और घटनाओं की स्थिति में डेटा प्रोसेसिंग। आधिकारिक ऑनलाइन स्रोत

[24]Reglamento (UE) 910/2014 eIDAS, अनुच्छेद 25–26 और 46: प्रारूप के आधार पर इलेक्ट्रॉनिक हस्ताक्षरों और दस्तावेज़ों के साथ भेदभाव न करना, उन्नत हस्ताक्षर और योग्य हस्ताक्षर के प्रभाव। आधिकारिक ऑनलाइन स्रोत

[25]स्पेन। नागरिक विचारण संहिता, अनुच्छेद 326 और 384: निजी दस्तावेज़, चुनौती, डेटा संग्रहित करने, जानने या पुनः उत्पन्न करने के साधन, परीक्षण, कस्टडी और विवेकपूर्ण मूल्यांकन। आधिकारिक ऑनलाइन स्रोत

[26]यूरोपीय संघ। Reglamento (UE) 2016/679, अनुच्छेद 5, 25, 28 और 32–34: सिद्धांत, डिज़ाइन से संरक्षण, प्रोसेसर, सुरक्षा तथा सुरक्षा उल्लंघनों की अधिसूचना/सूचना। स्पेन में लागू राष्ट्रीय और क्षेत्रीय विधान की भी समीक्षा आवश्यक है। आधिकारिक ऑनलाइन स्रोत

[27]स्पेन। Real Decreto-ley 19/2018, अनुच्छेद 45, 66 और 67: अनधिकृत लेनदेन की प्रतिपूर्ति, जोखिम प्रबंधन और गंभीर घटनाओं की तत्काल अधिसूचना। आधिकारिक ऑनलाइन स्रोत

फ़ील्ड	जानकारी जो नोट करें	निर्देश
जगह। जोड़ें	खुला प्रश्न और उत्तरदायी व्यक्ति।	समय से पहले समापन से बचें।

B.2 रोकथाम निर्णय मैट्रिक्स

निर्णय का काल्पनिक पत्रक

घटना: DEMO-RANSOM-2026-001
परिसंपत्ति और सेवा: [पहचानकर्ता, कार्य, निर्भरताएँ]
देखी गई स्थिति: [स्क्रीन, प्रक्रियाएँ, नेटवर्क, एन्क्रिप्शन]
मूल्यांकन किए गए विकल्प: [बंद करें, नेटवर्क को अलग करें, बनाए रखें, खाता निलंबित करें]
लोगों और निरंतरता के लिए जोखिम: [प्राथमिकता]
अस्थिरता और जोखिम में साक्ष्य: [मेमोरी, लॉग, सत्र]
निर्णय और प्राधिकरण: [कार्रवाई, व्यक्ति, तिथि और समय-क्षेत्र]
पूर्व संरक्षण: [वस्तु, विधि और आउटपुट]
हुआ परिवर्तन: [अंतिम स्थिति और पार्श्व-प्रभाव]
लंबित: [क्या संरक्षित या पुष्ट नहीं किया जा सका]
समीक्षा: [उत्तरदायी व्यक्ति और अगले मूल्यांकन का समय]

B.3 अधिग्रहण अभिलेख

तकनीकी मानिफ़ेस्ट

स्रोत / अधिग्रहण ID: DEMO-SRV-001 / A01
प्राधिकरण और दायरा: [दस्तावेज़ और अपवाद]
प्रारंभिक स्थिति: [फ़ोटो और अवलोकन]
उद्देश्य और कवरेज: [मेमोरी, इमेज, लॉजिकल, निर्यात]
उपकरण और सत्यापन: [संस्करण, वातावरण और परीक्षण]
समय-क्षेत्र सहित प्रारंभ / समाप्ति: [मूल मान]
आउटपुट: [फ़ाइलें, प्रारूप और आकार]
अखंडता: [एल्गोरिदम और सटीक वस्तु]
विसंगतियाँ: [त्रुटियाँ और छूटा हुआ कवरेज]
सत्यापन: [खोलना, संबंध और समीक्षा]
कस्टडी: [सुरक्षित रखरखाव, पहुँच और स्थानांतरण]

B.4 पुनर्प्राप्ति से बाहर निकलने के मानदंड

जाँच	हाँ / नहीं / लागू नहीं	साक्ष्य और अवलोकन
उपयोग से पहले बैकअप सत्यापित	[ ]	पहचानकर्ता और फ़ाइलें।
पहचान डेटा और सुसंगत कवरेज	[ ]	नमूना और गणना।
पुनर्स्थापित खाते और प्रमाणीकरण कारक	[ ]	कोई पुराना सत्र नहीं।
कार्यक्षमता की मूल्यांकन	[ ]	खाते और सामाने।
परीक्षण किए गए फ़ंक्शन और एकीकरण	[ ]	काल्पनिक मामले।
निगरानी और उत्तरदायी व्यक्ति नियुक्त	[ ]	जगह और जोड़।
सभी पूरे किए गए	[ ]	सत्यापन और प्रासंगिकता।
अवशिष्ट जोखिम स्वीकार किया गया	[ ]	उत्तरदायी व्यक्ति के हस्ताक्षर और तिथि।

परिशिष्ट C. अभ्यास और जाँच-सूची

C.1 काल्पनिक डेटा के साथ टेबलटॉप अभ्यास

तीन सर्वर, दो प्रशासनिक खाते, रात्रिकालीन बैकअप और एक ईमेल आपूर्तिकर्ता वाली कंपनी का अभ्यास करें। 08:12 पर दस्तावेज़ों में एन्क्रिप्शन की सूचना मिलती है; 08:16 पर दूसरे सिस्टम में वही एक्सटेंशन दिखाई देता है; 08:20 पर एक खाते में अग्रेषण का नियम मिलता है। टीम को कोई फ़ाइल चलाए बिना पृथक्करण, प्रारंभिक अधिग्रहण, आपूर्तिकर्ता से संपर्क, डेटा मूल्यांकन और पुनर्प्राप्ति का मार्ग तय करना है।

मूल्यांकन निर्णयों और अभिलेखों की गुणवत्ता पर आधारित है: यदि टीम संरक्षण किए बिना रिस्टोर करती है, तो अग्रेषण की व्याख्या करने का अवसर खो देती है; यदि निर्यात से पहले खाता निलंबित करती है, तो उस सीमा को दर्ज करती है; यदि किसी महत्वपूर्ण सेवा को बिना विकल्प छोड़ती है, तो उसे औचित्य देना होगा। अंत में सबसे तेज़ कार्रवाई को पुरस्कृत करने के बजाय निर्णयों की समीक्षा करें।

C.2 समापन से पहले संक्षिप्त जाँच-सूची

प्रश्न	अपेक्षित परिणाम
क्या लॉग सुरक्षित हैं?	प्राथमिकताओं और अपेक्षाओं को ध्यान रखा गया।
क्या प्राथमिक आरंभ साक्ष्य संरक्षित किया गया?	वस्तुएँ, विधियाँ और सीमाएँ दर्ज हैं।
क्या उत्पत्ति, दायरा-निर्धारण और एक्सफ़िल्ट्रेशन का मूल्यांकन किया गया?	परिकल्पनाएँ और खोज, बिना निरपेक्ष दावों के।
क्या फ़ैसले और सुधार के निर्णय अधिकृत थे?	गणपूर्ति, जोखिम और सत्करण।
क्या पुनर्प्राप्ति का परीक्षण किया गया?	डेटा, फ़ंक्शन, पहुँच और निरंतरता।
जगहें और क्या बदल गया?	वास्तविक नियंत्रण, उत्तरदायी व्यक्ति और सत्यापन।

समापन

शांति का अर्थ यह कहना नहीं है कि सब ठीक है। इसका अर्थ है यह जानना कि क्या किया जा रहा है, किस साक्ष्य के साथ, कौन निर्णय लेता है और कौन-सी जाँच अभी बाकी है।