ACCCF / अनुप्रयुक्त ज्ञान का पुस्तकालय

05

उपकरण, एप्लिकेशन, खाते और अधिग्रहण

स्पेनिश भाषा का संस्करण · 2026

खंड

मोबाइल फ़ोन और इंस्टेंट मैसेजिंग फोरेंसिक मैनुअल

प्राप्ति, पृथक्करण, अधिग्रहण, विश्लेषण, संदर्भ और उत्तरदायी अट्रिब्यूशन

मोबाइल संचारों की इस तरह जाँच करना कि स्क्रीनशॉट को स्रोत, निष्कर्षण को पूर्ण अधिग्रहण और खाते को उसका उपयोग करने वाले व्यक्ति से भ्रमित न किया जाए।

फोरेंसिक विशेषज्ञों, प्रथम उत्तरदाताओं, वकीलों, जाँचकर्ताओं और कस्टडी प्रशासकों के लिए। प्रक्रिया उपकरण, सिस्टम, एप्लिकेशन, संस्करण, एन्क्रिप्शन और प्राधिकरण पर निर्भर करती है; इसमें लॉक बायपास करने या दूसरों के खातों तक पहुँचने के तरीके नहीं दिए गए हैं।

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।

सामग्री

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: फ़ोन अपने आप नहीं बोलता 3

अध्याय 1. उपकरण की प्राप्ति और स्थिति 3

1.1 कार्यवाही-विवरण जिसे कोई दूसरा व्यक्ति पुनः बना सके 3

1.2 हानि और परिवर्तन के जोखिम 4

अध्याय 2. परतों के अनुसार स्रोत 4

2.1 डिवाइस, एप्लिकेशन और संबंधित डेटा 4

2.2 खाता, सत्र और लिंक किए गए उपकरण 4

2.3 आपूर्तिकर्ता और अन्य प्रतिभागी 5

अध्याय 3. पृथक्करण, विद्युत आपूर्ति और स्थानांतरण 5

3.1 वास्तविक और सत्यापित पृथक्करण 5

3.2 पैकेजिंग, स्थानांतरण और कस्टडी 6

अध्याय 4. अधिग्रहण की विधियाँ 6

4.1 मैनुअल दस्तावेज़ीकरण और स्क्रीनशॉट 6

4.2 एप्लिकेशन निर्यात और बैकअप 6

4.3 लॉजिकल, उन्नत और आपूर्तिकर्ता निष्कर्षण 7

4.4 उपकरण और आउटपुट का सत्यापन 7

अध्याय 5. वार्तालाप और सामग्री की जाँच 8

5.1 केवल वाक्यांश नहीं, थ्रेड पुनर्निर्मित करें 8

5.2 संपादित, हटाए और अग्रेषित संदेश 8

5.3 संलग्नक, थंबनेल और मेटाडेटा 8

अध्याय 6. अट्रिब्यूशन और संचार 9

6.1 खाता, उपकरण और व्यक्ति 9

6.2 कालक्रम और स्वतंत्र पुष्टि 9

6.3 स्पष्ट दायरे वाली रिपोर्ट 9

परिशिष्ट A. परिचालन प्रारूप 10

A.1 उपकरण की प्राप्ति 10

A.2 खातों और स्रोतों की सूची 10

A.3 अधिग्रहण अभिलेख 11

A.4 अट्रिब्यूशन मैट्रिक्स 11

परिशिष्ट B. कानूनी ढाँचा और अंतिम जाँच 11

प्रस्तावना: फ़ोन अपने आप नहीं बोलता

मोबाइल फ़ोन में वार्तालाप, फ़ाइलें, सेंसर, खाते और गतिविधि के अवशेष होते हैं, लेकिन वह क्लाउड या दूसरे प्रतिभागियों की केवल एक खिड़की भी हो सकता है। पहला प्रश्न यह नहीं कि कौन-सा प्रोग्राम उसे खोलेगा, बल्कि यह है कि कौन-सा कथन प्रमाणित करना है और कौन-से स्रोत उसका उत्तर दे सकते हैं। यदि जानना है कि संदेश किसने लिखा, तो स्क्रीन की फ़ोटो पर्याप्त नहीं है: सत्र, उपकरण, प्रमाणीकरण कारक, सामग्री और संदर्भ चाहिए।

मोबाइल विश्लेषण सिस्टम, एप्लिकेशन, संस्करण, एन्क्रिप्शन और उपकरण की स्थिति के अनुसार बदलता है। एक निष्कर्षण उपलब्ध डेटाबेस प्राप्त कर सकता है; दूसरा केवल दिखाई देने वाली फ़ाइलों या किसी निर्यात तक सीमित हो सकता है। “फोरेंसिक” शब्द वास्तविक कवरेज नहीं बदलता। रिपोर्ट में बताएँ कि क्या किया गया, क्या मिला और क्या बाहर रहा; हटाए गए संदेशों की पुनर्प्राप्ति या सार्वभौमिक पहुँच का वादा न करें।

NIST SP 800-101 Rev. 1 मोबाइल उपकरणों के संरक्षण, अधिग्रहण, परीक्षण, विश्लेषण और रिपोर्टिंग को व्यवस्थित करता है, जिसमें सत्यापन और दस्तावेज़ीकरण पर ध्यान दिया गया है। यह कार्यविधि की मार्गदर्शिका है, प्रत्येक उपकरण की क्षमताओं की अद्यतन सूची नहीं। उन क्षमताओं की जाँच विशिष्ट मॉडल और संस्करण पर परीक्षण डेटा और सत्यापनीय परिणामों से करें।[1]

> **पहला नियम**
> जिज्ञासावश चालू, ब्राउज़, रीसेट या कनेक्ट न करें। स्थिति और प्राधिकरण दर्ज करें, सहायक उपकरण संरक्षित करें और कुछ बदलने से पहले तय करें कि कौन-सी जानकारी नष्ट हो सकती है।

अध्याय 1. उपकरण की प्राप्ति और स्थिति

1.1 कार्यवाही-विवरण जिसे कोई दूसरा व्यक्ति पुनः बना सके

कार्यवाही-विवरण में प्रकार, ब्रांड, मॉडल, दृश्यमान पहचानकर्ता, भौतिक स्थिति, चालू/बंद स्थिति, लॉक, बैटरी, दिखाई देने वाला नेटवर्क, तिथि और समय-क्षेत्र, लोग, सहायक उपकरण और पिछली कार्रवाइयाँ दर्ज हों। सामान्य विवरण में पासवर्ड न लिखें। अनलॉक का प्राधिकरण होने पर उसका अस्तित्व और उसे सुरक्षित रूप से उपलब्ध कराने की विधि दर्ज करें। पुराने लेबल संरक्षित रखें और नए पहचानकर्ता से जोड़ें।

जब संभव हो, दिखाई देने वाली स्क्रीन की फ़ोटो बिना इंटरैक्ट किए लें: समय, नेटवर्क आइकन, बैटरी, सूचनाएँ और स्थिति। फ़ोटो उस क्षण की स्थिति दिखाती है, पूरी सामग्री नहीं। यदि किसी ने पहले एप्लिकेशन खोले या निष्कर्षण का प्रयास किया है, तो दर्ज करें। अपूर्ण प्राप्ति को दस्तावेज़ित करें; इसे ऐसे न लिखें मानो वस्तु बिना किसी बदलाव के प्राप्त हुई हो।

फ़ील्ड	काल्पनिक उदाहरण	किस निर्णय में मदद करता है
उपकरण	फ़ोन DEMO-MBL-003, मॉडल और सीरियल दृश्यमान।	पहचान और कार्यवाही-विवरण से तुलना करें।
स्थिति	चालू, लॉक, 43 %, मोबाइल नेटवर्क दृश्यमान।	संरक्षण और पृथक्करण की प्राथमिकता दें।
सहायक उपकरण	केबल, चार्जर, SIM और कवर अलग-अलग लेबल किए गए।	पहुँच-मार्ग और संदर्भ संरक्षित रखें।
बताया गया इतिहास	खाता खोलने से सत्यापन से पहले वार्तालाप निर्यात करने का प्रयास किया।	पिछली कार्रवाइयों को विश्लेषण से अलग रखें।

[1] NIST SP 800-101 Rev. 1, मोबाइल उपकरणों के फोरेंसिक विश्लेषण की मार्गदर्शिका: संरक्षण, अधिग्रहण, परीक्षण, विश्लेषण, सत्यापन और रिपोर्टिंग। प्रौद्योगिकी और वास्तविक क्षमताओं की जाँच वर्तमान मोबाइल डिवाइस और चुने गए टूल पर करनी चाहिए। आधिकारिक ऑनलाइन स्रोत

फ़ाइंड	काल्पनिक उदाहरण	किस निर्णय में मदद करता है
प्राथिकरण	एक वार्तालाप और निर्दिष्ट खाता की समीक्षा।	तात्कर पढ़ा और जम्प एप्लिकेशन तक पहुंच सीमित करें।
निर्णय	स्थिति संरक्षित करें और विशेषज्ञ से संपर्क करें।	अनधिकृत परिवर्तन से बचें।

1.2 हानि और परिवर्तन के जोखिम

एक उपकरण संदेश प्राप्त कर सकता है, सिंक्रनाइज़ हो सकता है, दूर से मिटाया जा सकता है, निष्क्रियता पर लॉक हो सकता है या उसकी बैटरी समाप्त हो सकती है। इसमें ऐसे सत्र और कुंजियाँ भी हो सकती हैं जो बंद करने पर नष्ट हो जाती हैं। पहचानें कि कौन-सा जोखिम अधिक अत्यावश्यक है और उससे निपटने के लिए क्या तकनीकी ज्ञान उपलब्ध है। बंद करना हमेशा संरक्षण नहीं है; चालू रखना हमेशा विश्लेषण नहीं है। अभिलेख में चुने गए विकल्प का कारण बताएँ।

यदि वार्तालाप किसी दूसरे प्रतिभागी या आपूर्तिकर्ता के पास उपलब्ध है, तो उपकरण में हस्तक्षेप करने से पहले वह स्रोत माँगना कम आक्रामक हो सकता है। यदि प्राथमिकता अस्थिर गतिविधि या एन्क्रिप्शन कुंजी है, तो अधिकृत लाइव अधिग्रहण आवश्यक हो सकता है। ऑकहम के रेज़र का सिद्धांत सबसे अधिक अंतर स्पष्ट करने वाले और सबसे कम परिवर्तन करने वाले स्रोत को चुनता है, सबसे परिष्कृत उपकरण को नहीं।

> **कब रुकना है**
> प्राधिकरण की कमी, विलोपन का जोखिम, असत्यापित उपकरण, न समझा गया एन्क्रिप्शन या किसी व्यक्ति को खतरा होने पर रुकें और मामला विशेषज्ञ को सौंपें। क्या मिलता है यह देखने के लिए ब्राउज़ करने से साक्ष्य बदल सकता है और बिना अनुमति दायरा बढ़ सकता है।

अध्याय 2. परतों के अनुसार स्रोत

2.1 डिवाइस, एप्लिकेशन और संबंधित डेटा

उपकरण की मेमोरी में एप्लिकेशन डेटाबेस, फ़ाइलें, थंबनेल, लॉग, संरक्षित क्रेडेंशियल, कैश और सेंसर डेटा हो सकते हैं। उनकी उपलब्धता स्थिति और पहुँच पर निर्भर करती है। सिंक्रनाइज़ेशन होने पर चित्रों का फ़ोल्डर पूरी फ़ोटो लाइब्रेरी के बराबर नहीं है। स्थानीय रूप से हटाया गया संदेश किसी दूसरे प्रतिभागी या प्रति में रह सकता है और अपुनर्प्राप्य भी हो सकता है। विश्लेषण इनमें से किसी भी चरम स्थिति की गारंटी नहीं देता।

सहायक उपकरण महत्वपूर्ण हैं: SIM या eSIM, मेमोरी, चार्जर, केबल, एडाप्टर, कवर, दस्तावेज़ और सिंक्रनाइज़ किए गए अन्य उपकरण। घड़ी, टैबलेट या कंप्यूटर में अलग जानकारी वाली सूचनाएँ या सत्र हो सकते हैं। इनकी सूची बनाएँ, लेकिन प्राधिकरण अपने आप न बढ़ाएँ: किसी वस्तु के जुड़ा होने का अर्थ यह नहीं कि उसकी सारी सामग्री कार्य-दायरे में है।

2.2 खाता, सत्र और लिंक किए गए उपकरण

एप्लिकेशन कई सत्रों, डेस्कटॉप क्लाइंट, बैकअप तथा ईमेल या ऑपरेटर से पुनर्प्राप्ति की अनुमति दे सकता है। उपलब्ध होने पर लिंक किए गए उपकरणों की सूची, जोड़ने और हटाने के अभिलेख, प्रमाणीकरण कारक, तिथियाँ, पुनर्प्राप्ति में बदलाव और सत्र गतिविधि माँगें। खाते का नाम तार्किक संबंध दर्शाता है; भौतिक पहचान के लिए अधिक तत्व चाहिए।

IP पता नेटवर्क का संकेत दे सकता है, लेकिन पता या व्यक्ति नहीं बताता। फ़ोन नंबर पुनः आवंटित हो सकता है या संबंधित अवधि में किसी दूसरे व्यक्ति से जुड़ा हो सकता है। IMEI अपने संदर्भ में उपकरण या कॉन्फ़िगरेशन पहचानता है, आवश्यक रूप से फ़ोन धारक को नहीं। अट्रिब्यूशन अभिसरण और वैकल्पिक व्याख्याओं से बनता है: उधार, साझा उपयोग, दूरस्थ पहुँच, सत्र की चोरी या किसी दूसरे व्यक्ति द्वारा प्रशासन।

2.3 आपूर्तिकर्ता और अन्य प्रतिभागी

आपूर्तिकर्ता के पास एन्क्रिप्ट की गई सामग्री के बिना मेटाडेटा, कनेक्शन लॉग या खाता जानकारी हो सकती है। दूसरे प्रतिभागियों के पास संदेश का अलग प्रतिनिधित्व और मूल संलग्नक हो सकते हैं। अनुरोध में खाता, अवधि, फ़ील्ड, नेटिव प्रारूप, समय-क्षेत्र और प्रक्रिया बताएँ। केवल माँगने पर प्लेटफ़ॉर्म सामग्री देगा, ऐसा वादा न करें; उसकी क्षमता और प्रतिक्रिया दर्ज करें।

मेक्सिको में दूरसंचार और रेडियो प्रसारण संबंधी कानून, 2025 में उसके अंतर्गत आने वालों और प्राधिकरणों के लिए डेटा संरक्षण तथा सौंपने के नियम हैं। विश्लेषण में जाँचें कि अनुरोध उस व्यवस्था में आता है या नहीं और अभिलेख दूरसंचार, एप्लिकेशन या किसी दूसरे आपूर्तिकर्ता का है। मैसेजिंग प्लेटफ़ॉर्म की सारी जानकारी को टेलीफ़ोन अभिलेख न मानें।[2]

> **स्वतंत्र स्रोत**
> किसी स्क्रीनशॉट और उसी का प्रिंट दो स्वतंत्र साक्ष्य नहीं हैं। दूसरे व्यक्ति को मिला संदेश, एप्लिकेशन निर्यात और सत्र अभिलेख के स्रोत तथा त्रुटियाँ अलग हो सकती हैं।



चित्र 1. फ़ोन एक परत है, पूरा मामला नहीं। बातचीत अलग-अलग वस्तुओं में मौजूद हो सकती है। संपादकीय पुनर्सृजन; वास्तविक साक्ष्य नहीं है।

अध्याय 3. पृथक्करण, विद्युत आपूर्ति और स्थानांतरण

3.1 वास्तविक और सत्यापित पृथक्करण

पृथक्करण का उद्देश्य दूरस्थ परिवर्तनों और नए संचारों को नियंत्रित करना है। सेल्यूलर, Wi-Fi, Bluetooth, NFC, केबल और सिंक्रनाइज़ेशन का मूल्यांकन करें। एयरप्लेन मोड चालू करने के लिए उपकरण को छूना पड़ता है और लॉग बदल सकते हैं; बंद करने से सत्र नष्ट हो सकते हैं; पृथक्करण कंटेनर सत्यापित न हो या उपकरण फिर जुड़ने का प्रयास करे तो अप्रभावी हो सकता है। क्या किया गया और उसका क्या प्रभाव हुआ, दर्ज करें।

एंटीस्टैटिक बैग डिस्चार्ज से बचाता है, आवश्यक रूप से रेडियोफ़्रीक्वेंसी से नहीं। उसे फैराडे कहने से उसका कार्य नहीं बदलता। पृथक्करण समाधान की जाँच सुरक्षित तरीकों और समान परिस्थितियों में करें: सिग्नल के प्रकार, सील, सामग्री, दूरी और उपकरण की स्थिति। जाँच का अर्थ बिना अनुमति किसी व्यक्ति के नंबर पर कॉल करना नहीं है; परीक्षण उपकरण उपयोग करें।

[2] दूरसंचार और रेडियो प्रसारण संबंधी कानून, 16-07-2025 को प्रकाशित। अनुच्छेद 182 और 183: आवश्यकताएँ और डेटा संरक्षण, वास्तविक समय में जाँच तथा संबंधित चरण के अनुसार 48 घंटे के भीतर डिलीवरी। आधिकारिक ऑनलाइन स्रोत

विकल्प	मुख्य जोखिम	आवश्यक जाँच
एयरप्लेन मोड	इंटरफ़ेस, लॉग में बदलाव और रोष फनफ्रेम।	स्क्रीन, फ़ोरग्राउंड, समय और सत्यापित फनफ्रेम।
बंद करना	मनोरंजन, सत्र का इम्प्रेशन का कारण पहुँच का मुफ़्तसाम।	जीवंत, स्थिति और जीवग्रहण क्षमता।
RF फटनर	जबरदस्ती या जस्टत्यापित पृथक्करण।	परिदृश्य, साल, समग्र और पारास्थातिय।
कनेक्ट रखना	सिंक्रनाइज़ेशन, सर्वर या दूरस्थ विलोपन।	जीवंतता, नियंत्रण और निरीक्षण।
विद्युत आपूर्ति	गंभीर, गतिविधि या स्थिति में परिवर्तन।	पावर, कंपन और उद्देश्य दस्तावेज़ित।

3.2 पैकेजिंग, स्थानांतरण और कस्टडी

पैकेजिंग भौतिक और तार्किक कार्य के अनुसार चुनें: वह धक्के, स्थिर विद्युत, नमी और पहुँच से बचाए तथा अपनाया गया पृथक्करण बनाए रखे। सहायक उपकरण भी पैक करके उनका संबंध दर्ज करें। सील में पहचानकर्ता, तिथि और उत्तरदायी व्यक्ति हों; हर खोलने या बदलाव को दर्ज करें। जब बैटरी और कनेक्टिविटी से डेटा बदल सकता है, तो सक्रिय उपकरण को उनके नियंत्रण के बिना स्थानांतरित न करें।

कस्टडी शृंखला दर्ज करती है कि कौन सौंपता है, कौन प्राप्त करता है, किस उद्देश्य से, कहाँ, किस स्थिति में और किस सत्यापन के साथ। इलेक्ट्रॉनिक स्थानांतरण में संबंधित वस्तु की अनुमतियाँ, चैनल, संस्करण, डाउनलोड और हैश दर्ज करें। निष्कर्षण समीक्षक के साथ साझा करने पर नियंत्रित प्रति दें और दायरे से बाहर के तीसरे पक्ष के डेटा को प्रतिबंधित करें।

> **व्यावहारिक नियम**
> पैकेजिंग किसी खराब निर्णय को ठीक नहीं करती, लेकिन नए परिवर्तन रोकती है। सील भी यह सिद्ध नहीं करती कि सामग्री सत्य है: वह दस्तावेज़ित अनुक्रम में बंद रखने की स्थिति दर्शाती है।

अध्याय 4. अधिग्रहण की विधियाँ

4.1 मैनुअल दस्तावेज़ीकरण और स्क्रीनशॉट

जब प्रश्न किसी वार्तालाप तक सीमित हो या दूसरे स्रोत उपलब्ध न हों, तो मैनुअल समीक्षा उपयोगी हो सकती है। एप्लिकेशन, संस्करण, उपकरण, तिथि और समय-क्षेत्र, ऑपरेटर, देखने का क्रम और दिखाई देने वाली सामग्री दर्ज करें। स्क्रीन रिकॉर्डिंग दृश्य निरंतरता देती है, लेकिन फिर भी इंटरफ़ेस में दिखाई देने वाली सामग्री का चयन ही रहती है। यह पूरे डेटाबेस या अदृश्य घटनाओं को सिद्ध नहीं करती।

स्क्रीनशॉट लेने से पहले दायरा तय करें और दूसरी चैट, फ़ोटो या सूचनाएँ उजागर होने से बचाएँ। एप्लिकेशन से निर्यात करने पर प्रारूप, फ़िल्टर, संलग्नक, मूल नाम और तिथि संरक्षित रखें। फ़ाइल की गणना नई वस्तु के रूप में करें और उसे उपकरण से जोड़ें। स्रोत को संरक्षित करने से पहले उसका नाम न बदलें।

4.2 एप्लिकेशन निर्यात और बैकअप

चैट निर्यात में एप्लिकेशन द्वारा चुनी गई संरचना के साथ पाठ और संलग्नक हो सकते हैं। जाँचें कि उसमें संपादित और हटाए गए संदेश, प्रतिक्रियाएँ, उद्धरण, उत्तर या संदर्भ शामिल हैं या नहीं, तथा तिथियाँ और प्रतिभागी कैसे दर्शाए जाते हैं। बैकअप में अलग स्नैपशॉट हो सकता है और वह किसी अलग कुंजी से एन्क्रिप्ट हो सकता है। उपलब्ध क्षमता दर्ज करें, लेकिन उसे भौतिक निष्कर्षण के बराबर न बताएँ।

वार्तालाप संरक्षित करना उद्देश्य हो, तो निर्यात के साथ संदर्भ का स्क्रीनशॉट और दूसरे प्रतिभागियों के स्रोत भी रखें। शामिल नहीं की गई घटनाओं का विश्लेषण उद्देश्य हो, तो अधिकृत निष्कर्षण का मूल्यांकन करें। दो निर्यातों के बीच अंतर फ़िल्टर या संस्करणों से हो सकता है, अपने आप हेरफेर से नहीं। दोनों वस्तुओं को संबंधित पहचानकर्ताओं के साथ संरक्षित रखें।

4.3 लॉजिकल, उन्नत और आपूर्तिकर्ता निष्कर्षण

लॉजिकल निष्कर्षण संगत उपकरण से उपलब्ध फ़ाइलें या डेटाबेस प्राप्त करता है। उपकरण और विधि अनुमति देने पर उन्नत अधिग्रहण का कवरेज अधिक हो सकता है, लेकिन उसके लिए प्रशिक्षण, प्राधिकरण और सत्यापन आवश्यक हैं। यदि केवल कुछ विभाजन या एप्लिकेशन कवर हुए हों, तो रिपोर्ट में सामान्य "पूर्ण निष्कर्षण" लेबल न लगाएँ। त्रुटियाँ, डिक्रिप्ट न की गई वस्तुएँ और अपवाद संरक्षित रखें।

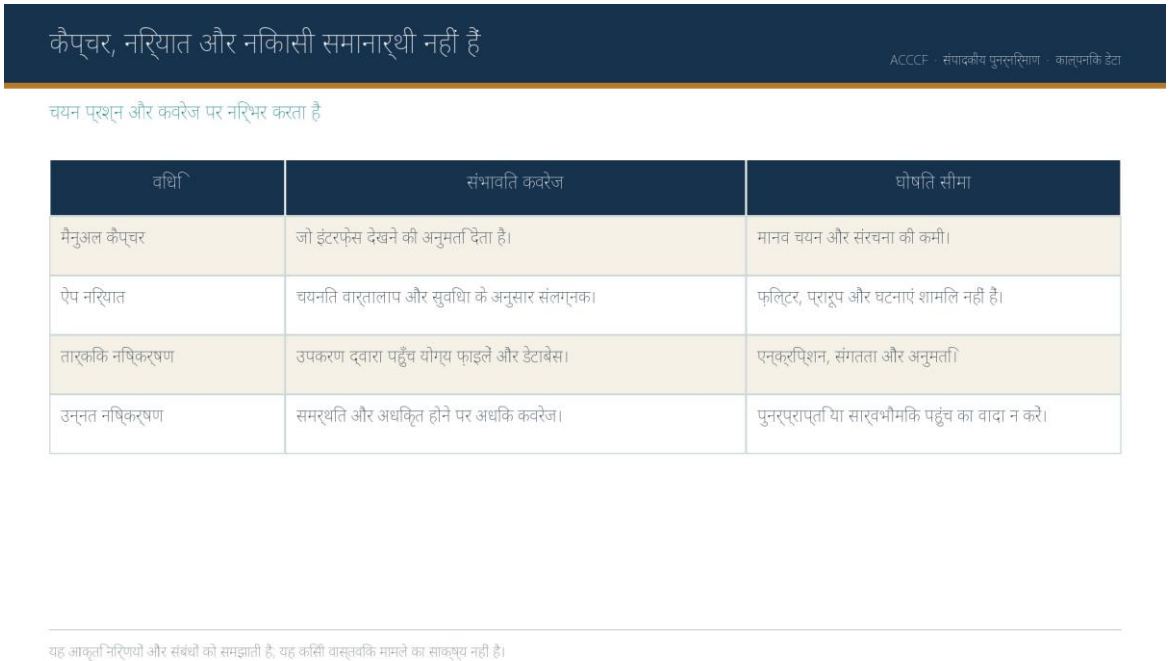
आपूर्तिकर्ता अधिग्रहण से ऐसी खाता जानकारी या अभिलेख मिल सकते हैं जो फ़ोन में नहीं हैं। फ़ील्ड, समय-क्षेत्र, नेटिव प्रारूप, प्रक्रिया और डेटा शब्दकोश माँगें। प्राप्त फ़ाइल को EML और उपलब्ध होने पर अखंडता के घोषणापत्र से जोड़ें। आपूर्तिकर्ता के पास एन्क्रिप्ट की गई सामग्री नहीं हो सकती या उसका रिटेंशन नियम अलग हो सकता है; उत्तर को सार्वभौमिक टेलीफ़ोन अभिलेख के रूप में प्रस्तुत न करें।[34]

4.4 उपकरण और आउटपुट का सत्यापन

काल्पनिक उपकरण या ज्ञात डेटा वाले समुच्चय से जाँचें कि उपकरण अपेक्षित वस्तुएँ बनाता है, तिथियों, प्रतिभागियों और संलग्नकों की सही व्याख्या करता है तथा दस्तावेज़ित सीमा से बाहर स्रोत में बदलाव नहीं करता। नाम, संस्करण, वातावरण, लाइसेंस, कॉन्फ़िगरेशन और परिणाम दर्ज करें। अद्यतन से व्यवहार बदल सकता है और नया सत्यापन आवश्यक होता है।

आउटपुट खोलें और चुने गए दृश्यमान स्रोत से तुलना करें: नियंत्रण वार्तालाप, फ़ाइल, तिथि या अनुक्रम। डिकोड न की गई वस्तुओं को चिह्नित करें, छिपाएँ नहीं। यदि दूसरा उपकरण अलग प्रतिनिधित्व देता है, तो अंतर दर्ज करें और मूल्यांकन करें कि कौन-सा प्रतिनिधित्व प्रश्न का बेहतर उत्तर देता है। उपकरण गवाह नहीं बनता; वह विधि का घटक है।

> **स्वीकृति मानदंड**
> अधिग्रहण तब पूरा माना जाता है जब आउटपुट खोला जा सके, उपकरण से जोड़ा जा सके, उसका कवरेज बताया जा सके, विसंगतियाँ संरक्षित हों और अनुरूप समीक्षा संभव हो। प्रोग्राम "100 %" दिखा देने पर यह पूरा नहीं माना जाता।



चित्र 2. स्क्रीनशॉट, निर्यात और निष्कर्षण समानार्थी नहीं हैं। चयन प्रश्न और कवरेज पर निर्भर करता है। संपादकीय पुनर्निर्माण; वास्तविक साक्ष्य नहीं है।

[3] 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

[4] NIST SP 800-101 Rev. 1. मोबाइल उपकरणों के फोरेंसिक विश्लेषण की मार्गदर्शिका: संरक्षण, अधिग्रहण, परीक्षण, विश्लेषण, सत्यापन और रिपोर्टिंग। प्रौद्योगिकी और वास्तविक क्षमताओं की जाँच वर्तमान मोबाइल डिवाइस और चुने गए टूल पर करनी चाहिए। आधिकारिक ऑनलाइन स्रोत

अध्याय 5. वार्तालाप और सामग्री की जाँच

5.1 केवल वाक्यांश नहीं, थ्रेड पुनर्निर्मित करें

स्रोत में उपलब्ध होने पर प्रतिभागियों, पहचानकर्ताओं, उद्धृत संदेशों, उत्तरों, संलग्नकों, प्रतिक्रियाओं, संपादन, विलोपन तथा भेजने, प्राप्त करने और पढ़ने की तिथियों का विश्लेषण करें। स्क्रीनशॉट में वह संदेश छिप सकता है जिसका उत्तर दिया जा रहा था। अनुक्रम स्रोत के पहचानकर्ताओं से दस्तावेज़ित करें, गढ़ी हुई संख्या से नहीं जो असिद्ध निरंतरता का आशय दे।

वार्तालाप की तुलना संदर्भ से करें: कॉल, फ़ाइलें, संपर्क, एप्लिकेशन गतिविधि, अनुमानित स्थान, ईमेल और गवाही। किसी वाक्यांश की व्याख्या के लिए भाषा, संबंध, घटनाएँ और अनुक्रम चाहिए। उद्धृत संदेश खो जाने पर “हाँ” किसी दूसरे प्रश्न का उत्तर हो सकता है। विश्लेषण में कल्पना से अर्थ पूरा न करें।

5.2 संपादित, हटाए और अग्रेषित संदेश

“संपादित” लेबल दिखाई देने वाली स्थिति बताता है, पिछली सामग्री नहीं। “हटाया गया” लेबल यह सिद्ध नहीं करता कि सभी निशान मिट गए हैं या उद्देश्य छिपाना था। अग्रेषण से स्रोत की एक अलग परत जुड़ सकती है। उपलब्ध अभिलेख, प्रतियाँ, दूसरे प्रतिभागी और बैकअप जाँचें, लेकिन पिछला पाठ पुनर्प्राप्त करने का वादा न करें।

अवलोकन	इसका क्या अर्थ हो सकता है	आपको निष्कर्ष निकालने के लिए क्या चाहिए
संपादित	एप्लिकेशन में बाद का परिवर्तन।	पिछली सामग्री वाले संस्करण, जो अभिलेख या प्रति मांगी।
सभी के लिए हटाया गया	क्लाइंट में हटाने का दिखना।	हटाने का कवरेज और उपलब्ध प्रतियाँ।
अग्रेषित	किसी अन्य स्रोत से प्रसारित सामग्री।	मूल स्रोत और प्रारंभिक तिथि, यदि उपलब्ध हो।
बिना संलग्न फ़ाइल	संलग्नक डाउनलोड नहीं हुआ, समाप्त हो गया या शामिल नहीं है।	अभिलेख, लिंक, दूसरे प्रतिभागी या प्रति।
अलग संस्करण	संपर्क-छवि, चैट, स्क्रीनशॉट या संपादन।	मूल नाम और स्रोत की फ़ोरेंसिक परीक्षा।

5.3 संलग्नक, थंबनेल और मेटाडेटा

संलग्नक को अलग संरक्षित करके संदेश से जोड़ें। उसका थंबनेल किसी अलग संस्करण का हो सकता है; डाउनलोड करने पर नाम बदल सकता है। आंतरिक मेटाडेटा, सामग्री, आकार, प्रारूप और सिस्टम तिथि की जाँच करें, लेकिन इन फ़ील्ड को उत्पत्ति का स्वतः प्रमाण न बनाएँ। दूसरे प्रतिभागी की प्रति में बेहतर गुणवत्ता या अतिरिक्त जानकारी हो सकती है।

दस्तावेज़, चित्र या ऑडियो के लिए मौलिकता और सामग्री का विशिष्ट विश्लेषण आवश्यक हो सकता है। मोबाइल फोरेंसिक परीक्षण यह दिखाती है कि फ़ाइल किसी संदेश या फ़ोल्डर से जुड़ी मिली, न कि उसका दृश्य सत्य है या लेखक प्रेषक है। इस अंतर से अच्छे अधिग्रहण को सामग्री पर अत्यधिक निष्कर्ष का आधार बनने से रोका जाता है।

> **काल्पनिक मामला**
> किसी वार्तालाप में धमकी के बाद हटाया गया संदेश है। दूसरे प्रतिभागी के पास बाद का संदेश सुरक्षित है, जो उसी लेखक का स्पष्टीकरण था। बचाव और आरोप दोनों को दोनों संदेशों का विश्लेषण करना चाहिए। संदर्भ की पुनर्प्राप्ति निर्दोषता या दोष सिद्ध नहीं करती; इससे किसी अलग वाक्यांश को पूरा संचार मानकर व्याख्या करने से बचा जाता है।

अध्याय 6. अट्रिब्यूशन और संचार

6.1 खाता, उपकरण और व्यक्ति

अट्रिब्यूशन को प्रश्नों में बाँटें: किस खाते ने संदेश बनाया या प्राप्त किया, किस उपकरण पर सत्र था, कौन उसे अनलॉक कर सकता था, प्रमाणीकरण कारक किसके नियंत्रण में थे, किस दूसरे व्यक्ति की पहुँच थी और अनुक्रम कौन-सी गतिविधि दिखाता है। लाइन का अनुबंधिक स्वामित्व संदर्भ दे सकता है, लेकिन उस समय के उपयोग को अपने आप सिद्ध नहीं करता।

उधार, साझा उपयोग, प्रतिनिधिकरण, क्रेडेंशियल की चोरी, पहले से सक्रिय सत्र, दूरस्थ पहुँच और तीसरे पक्ष के प्रशासन पर विचार करें। अट्रिब्यूशन अपर्याप्त बताने के लिए बचाव पक्ष को इनमें से कोई वैकल्पिक व्याख्या सिद्ध करने की आवश्यकता नहीं है; आरोप पक्ष को उसे साक्ष्य से खारिज करने वाला आधार-वाक्य चाहिए। मजबूत अभिसरण होने पर उसका दायरा बताएँ, निरपेक्ष निश्चितता का दावा न करें।

6.2 कालक्रम और स्वतंत्र पुष्टि

प्रत्येक तिथि का मूल मान, समय-क्षेत्र और परिशुद्धता संरक्षित रखें। भेजना, प्राप्त करना, पढ़ना, संपादन और स्क्रीनशॉट अलग घटनाएँ हैं। निर्यात की तिथि संदेश की तिथि नहीं होती। सूचना का समय किसी दूसरी परत पर निर्भर हो सकता है। अंतर को जालसाज़ी बताने से पहले डेटा शब्दकोश और घड़ी के साथ उसका विश्लेषण करें।

स्वतंत्र पुष्टि दूसरे प्रतिभागी, सत्र अभिलेख, प्रति, रसीद, कैमरा या सेंसर के अनुक्रम से मिल सकती है। स्क्रीनशॉट की संख्या को स्वतंत्र स्रोतों की गिनती न मानें। प्रश्न यह है कि प्रत्येक स्रोत में कौन-सी त्रुटि हो सकती है और उनका अभिसरण वैकल्पिक व्याख्याएँ खारिज करने देता है या नहीं।

6.3 स्पष्ट दायरे वाली रिपोर्ट

स्तर	प्रमाण-समर्थित प्रस्तुति	क्या दावा न करें
पर्याप्त	पे पहचानकर्ता और सहायक उपकरण वाला उपकरण प्राप्त हुआ।	"यह आरोपी का फ़ोन था", केवल दिखावे के आधार पर।
आंशिक	उपकरण में बताए गए पैमाने में पे फ़ाइल और डेटाबेस प्राप्त किए।	जो कुछ भी गायब था, उसे निकाल लिया गया।
सीमित	खाते में सबसे इस तारीख और इन प्रति मांगने के लिए दर्ज है।	"खाता वास्तव में इसे लिखा", उपयोग का साक्ष्य न होने पर।
विश्लेषण	खाते इस अनुक्रम के साथ मेल है और इन समानता को प्रदर्शित करते हैं।	कोई दूसरी व्याख्या नहीं है।
अनुपस्थित	कैमरा और फ़ोल्डर में घटना नहीं देखा गया।	यह कभी मौजूद नहीं था।

विश्लेषण का समापन

किसी व्यक्ति की पहचान केवल एक लेबल से नहीं निकाली जाती। जब स्वतंत्र स्रोत अट्रिब्यूशन का विरोध कर सकते थे लेकिन नहीं करते, तो वह मजबूत होता है; जब उनमें से कोई दूसरी संभावना दिखाता है, तो कमजोर होता है।



चित्र 3. खात स व्याक्त तक: आधार-वाक्य अनुपलब्ध ह। आट्रब्यूशन विशेषणा स नहा, स्वतत्रता स मजबूत हाता ह। सपादकाय पुनानमाण; वास्तावक साक्ष्य नहा है।

परिशिष्ट A. परिचालन प्रारूप

A.1 उपकरण की प्राप्ति

काल्पनिक कार्यवाही-विवरण

मामला: EXP-DEMO-2026-005
उपकरण / ID: DEMO-MBL-003
ब्रांड, मॉडल और दृश्यमान पहचानकर्ता: [अभिलेख]
स्थिति: [चालू/बंद, लॉक, बैटरी, नेटवर्क, क्षति]
सहायक उपकरण: [केबल, SIM, मेमोरी, कवर, अन्य]
डिलीवरी / प्राप्ति: [भूमिकाएँ, तिथि, समय-क्षेत्र, स्थान]
पिछली कार्रवाइयाँ: [देखी गई और बताई गई, अलग-अलग]
प्राधिकरण: [एप्लिकेशन, खाते, अवधि, अपवाद]
जोखिम: [अस्थिरता, विलोपन, बैटरी, गोपनीयता]
प्रारंभिक निर्णय: [पृथक्करण, विद्युत आपूर्ति, मामला आगे भेजना]
फ़ोटो और सील: [पहचानकर्ता और संबंध]
टिप्पणियाँ: [कुंजियाँ या अनावश्यक डेटा शामिल न करें]

A.2 खातों और स्रोतों की सूची

परत	खाता / स्रोत	उपलब्धता और प्राधिकरण	नोट
उपकरण	[प्रदाता/सेवा]	[स्थिति, पहुँच और धारक]	[प्रारूप, कवरेज]
खाता	[पहचानकर्ता]	[सत्र, प्रमाणीकरण कारक और अनुमति]	[सत्र पहले द्वारा उपयोग]
प्रति भाग	[जोड़ीकृत सेवक]	[उपलब्ध खाते]	[अलग प्रतिलिपियाँ]
जटिलता	[सेवा और फ़र्स्ट प्रभाव]	[अनुरोध और उत्तर]	[समझ या रिटेंशन]
बैकअप	[तिथि और स्थान]	[कुंजी और पहुँच]	[सेवरेंट और कवरेज]

A.3 अधिग्रहण अभिलेख

आउटपुट लॉग

स्रोत और प्राधिकरण: DEMO-MBL-003 / [दायरा]
विधि: [मैनुअल, निर्यात, लॉजिकल, उन्नत, आपूर्तिकर्ता]
उपकरण, सिस्टम और एप्लिकेशन: [संस्करण]
उपकरण, संस्करण और सत्यापन: [काल्पनिक परीक्षण]
प्रारंभ / समाप्ति तिथि और समय-क्षेत्र: [मूल मान]
उपकरण पर कार्रवाइयाँ: [इंटरैक्शन और बदलाव]
प्राप्त वस्तुएँ: [फ़ाइलें, डेटाबेस, निर्यात]
फ़िल्टर और कवरेज: [अवधि, खाते, अपवाद]
हैश और मैनिफ़ेस्ट: [प्रति वस्तु]
विसंगतियाँ: [त्रुटियाँ, डिकोड न किया गया, अनुपस्थितियाँ]
सत्यापन: [खोलना, नमूना और समीक्षा]
बाद की कस्टडी: [कार्य-प्रति और पहुँच]

A.4 अट्रिब्यूशन मैट्रिक्स

कथन	अनुकूल स्रोत	वैकल्पिक व्याख्या	सीमित परिणाम
खाता न बदला गया	[आधिकारिक]	[दूसरा सेट सक्रिय]	[ ]
उपकरण सक्रिय था	[स्क्रीन, लॉग]	[घड़ी गलत तिथि पर सेट]	[ ]
व्यक्ति ने इसका इस्तेमाल किया	[प्रमाणीकरण कारक, सेशन]	[उधार, चोरी, प्रतिरूपण]	[ ]
पाठ्यांश पूरा है	[निर्यात]	[फ़िल्टर और जम्प चरण]	[ ]
फ़ाइल घटना से संबंधित है	[सेशन, मेटाडेटा]	[आयोजन या पहले का सेशन]	[ ]

परिशिष्ट B. कानूनी ढाँचा और अंतिम जाँच

इलेक्ट्रॉनिक दस्तावेज़ की मान्यता का अर्थ यह नहीं कि हर स्क्रीनशॉट प्रामाणिक है या खाता किसी व्यक्ति की पहचान करता है। मेक्सिको में CCom 89–94 और 1205, संक्रमण के अनुसार CFPC/CNPCF व्यवस्था और संबंधित क्षेत्र के लिए LMTR की समीक्षा करें। पेरू में हस्ताक्षर, प्रक्रिया और अभिलेखन अलग देखें; चिली हस्ताक्षर और तिथि में अंतर करता है; अर्जेंटीना विश्वसनीयता का मूल्यांकन करता है; कोलंबिया और इक्वाडोर संरक्षण के विवरण देते हैं; स्पेन eIDAS और LEC को साथ रखता है। अनुप्रयोग की जाँच संस्करण, विषय और क्षेत्राधिकार के साथ करें।[567891011121314]

[5]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

[6]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

[7]दूरसंचार और रेडियो प्रसारण संबंधी कानून, 16-07-2025 को प्रकाशित। अनुच्छेद 182 और 183: आवश्यकताएँ और डेटा संरक्षण, वास्तविक समय में जाँच तथा संबंधित चरण के अनुसार 48 घंटे के भीतर डिलीवरी। आधिकारिक ऑनलाइन स्रोत

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

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

[10]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

[11]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

[12]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

[13]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

[14]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

डेटा संरक्षण पूरी प्रक्रिया में साथ रहता है: एप्लिकेशन, अवधि, खाते और तीसरे पक्ष के डेटा सीमित करें; कार्य और डिलीवरी संस्करण अलग रखें; प्राधिकरण और पहुँच का साक्ष्य संरक्षित करें। रिपोर्ट में पासवर्ड, निजी कुंजियाँ, पूरे नंबर या दूसरी हानि सुविधाजनक बनाने वाली जानकारी प्रकाशित न करें।[15][16][17]

जाँच का क्षेत्र	स्वीकृति प्रश्न
पहचान	क्या उपकरण, सहायक उपकरण और फ़ोरेंसिक-वातावरण मेल खाते हैं?
स्थिति	क्या पृथक्करण और विद्युत जोखिम का निर्णय दस्तावेज़ित है?
फ़ोरेंसिक	क्या निष्कर्षण में फ़िल्टर, सीमाएँ और त्रुटियाँ बताई गई हैं?
सबूत	क्या पोर्टलिंग में ब्रेक, संलग्नक और जन्य परत संरक्षित हैं?
जाँचकर्ता	क्या खाते, उपकरण और व्याख्या अलग-अलग रखे गए हैं?
गोपनीयता	क्या फ़ोन-दायरे से बाहर का डेटा बाहर रखा गया?
समीक्षा	क्या कोई दूसरा व्यक्ति परिणाम खोजकर उसकी जाँच कर सकता है?

सारांश

फ़ोन तथ्यों का निर्णायक हिस्सा रख सकता है। विधि तय करती है कि उस हिस्से को स्क्रीन को आरोप में बदले बिना समझा जा सके या नहीं।

[15] मेक्सिको। निजी व्यक्तियों के कब्ज़े में व्यक्तिगत डेटा के संरक्षण संबंधी संघीय कानून, 20-03-2025 को प्रकाशित पाठ और 14-11-2025 का संशोधन। अनुच्छेद 5–9, 18–20 और 31: सिद्धांत, सुरक्षा, गोपनीयता, उल्लंघन और अधिकारों के निपटान। वर्तमान संघीय प्राधिकरण भ्रष्टाचार-विरोध एवं सुशासन सचिवालय है। आधिकारिक ऑनलाइन स्रोत

[16] 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

[17] 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