NORMA ARGENTINA

IRAM-ISO/IEC 27037

Primera edición
2022-07-04

Tecnología de la información

Técnicas de seguridad

Guías para la identificación, la recolección, la adquisición y la preservación de la evidencia digital

(ISO/IEC 27037:2012, IDT)

Information technology
Security techniques
Guidelines for identification, collection, acquisition, and preservation of digital evidence

Referencia Numérica:
IRAM-ISO/IEC 27037:2022

Prefacio

El Instituto Argentino de Normalización y Certificación (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo de Normalización de la República Argentina, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor.

IRAM es el representante de la República Argentina en la International Organization for Standardization (ISO), en la Comisión Panamericana de Normas Técnicas (COPANT) y en la Asociación MERCOSUR de Normalización (AMN), y, a través del Comité Electrotécnico Argentino, en la International Electrotechnical Commission (IEC).

Este documento es el resultado del consenso técnico entre los diversos sectores involucrados, los que a través de sus representantes han intervenido en los organismos de estudio de normas correspondientes.

Esta norma es una adopción idéntica de la ISO/IEC 27037:2012 - *Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence*.

Solo se han realizado los cambios siguientes:

Se agregaron notas IRAM en la Introducción, en 3.5, en 3.25, en el capítulo 3, en el capítulo 4, en 5.4.4 y se ha agregado un Anexo C informativo, todos con el fin de alinear la norma con el marco normativo argentino.

Se han agregado dos anexos informativos referidos a la bibliografía y la lista de integrantes del organismo de estudio correspondiente.

Prefacio ISO

La International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC) constituyen un sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para tratar temas particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC, también toman parte en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1.

Las normas internacionales se elaboran de acuerdo con las reglas dadas en la Directiva ISO/IEC, parte 2.

La tarea principal del comité técnico conjunto es la de preparar Normas Internacionales. Los Borradores de Normas Internacionales se circulan a los organismos nacionales para su votación. La publicación como Norma Internacional requiere la aprobación de, como mínimo, un 75 % de los organismos nacionales que votan.

Es importante señalar la posibilidad de que algunos elementos de esta norma internacional pueden estar sujetos a derechos de patente. ISO e IEC no son responsables de la identificación de alguno o de todos esos derechos de patentes.

La ISO/IEC 27037 fue preparada por el Comité Técnico Conjunto ISO/IEC JTC 1, *Information technology*, subcomité SC 27, *IT Security Techniques*.

Índice

Tecnología de la información
Técnicas de seguridad
Guías para la identificación, la recolección, la adquisición y la preservación de la evidencia digital

INTRODUCCIÓN

Esta norma proporciona guías para actividades específicas en el manejo de la potencial evidencia digital; estos procesos son: la identificación, la recolección, la adquisición y la preservación de la potencial evidencia digital. Estos procesos se requieren en una investigación que está diseñada para mantener la integridad de la evidencia digital - una metodología aceptable para la obtención de la evidencia digital que va a contribuir a su admisibilidad en acciones legales y disciplinarias, así como en otras instancias requeridas. Esta norma también proporciona guías generales para la recolección de evidencia no digital que puede ser de ayuda en la etapa de análisis de la potencial evidencia digital.

Esta norma tiene la intención de proporcionar guías para aquellas personas responsables de la identificación, la recolección, la adquisición y la preservación de la potencial evidencia digital. Estas personas incluyen a los **primeros intervinientes en la evidencia digital** (PIED), los **especialistas en evidencia digital** (EED), los especialistas en respuesta a incidentes y los gerentes de laboratorios forenses. Esta norma garantiza que las personas responsables gestionan la potencial evidencia digital de una manera práctica que sea aceptable a nivel mundial con el objetivo de facilitar la investigación que involucra a los dispositivos digitales y a la evidencia digital de una manera sistemática e imparcial, al mismo tiempo que preserva su integridad y autenticidad.

Esta norma también tiene la intención de informar a quienes toman decisiones y necesitan determinar la confiablidad de la evidencia digital que se les presenta. Es aplicable a las organizaciones que necesitan proteger, analizar y presentar la potencial evidencia digital y es pertinente para los organismos generadores de políticas y evaluadores de procedimientos relacionados con la evidencia digital, a menudo como parte de un conjunto más amplio de evidencias.

NOTA IRAM. En el sistema judicial de la Argentina la prueba documental informática guarda una relación de especie a género respecto de la prueba documental clásica que se integra a los restantes elementos probatorios autorizados por los distintos códigos procesales vigentes (prueba confesional, documental, de informes, testimonial, pericial y reconocimiento o inspección en el lugar del hecho).

La potencial evidencia digital a la que se refiere esta norma se puede encontrar en distintos tipos de dispositivos digitales, redes, bases de datos, etc. Se refiere a los datos que ya están en formato digital. Esta norma no pretende cubrir la conversión de datos analógicos en formato digital.

Debido a la fragilidad de la evidencia digital, es necesario llevar a cabo una metodología aceptable para garantizar la integridad y la autenticidad de la potencial evidencia digital. Esta norma no obliga a utilizar herramientas o métodos particulares. Los componentes clave que proporcionan credibilidad a la investigación son la metodología aplicada durante el proceso y las personas calificadas para realizar las tareas especificadas en ésta. Esta norma no trata la metodología para las actuaciones legales, los procedimientos disciplinarios y otras acciones relacionadas con el manejo de la potencial evidencia digital que están fuera del alcance de la identificación, la recolección, la adquisición y la preservación.

La aplicación de esta norma requiere el cumplimiento del marco normativo nacional. Se recomienda que no reemplace a los requisitos legales específicos de ninguna jurisdicción. Puede servir como guía práctica para todos los PIED o EED en investigaciones que involucren potencial evidencia digital. No está dirigida u orientada al análisis de la potencial evidencia digital y no reemplaza los requisitos legales de cada jurisdicción que entienden en el uso de la potencial evidencia digital en el proceso judicial, tales como admisibilidad, peso de la prueba, pertinencia y otras limitaciones de control legal relacionadas con la presentación de la potencial evidencia digital en procesos judicializados. La norma puede ayudar a facilitar el intercambio de potencial evidencia digital entre jurisdicciones. A fin de mantener la integridad de la evidencia digital, se requiere que los usuarios de esta norma adapten y modifiquen los procedimientos aquí descriptos de acuerdo con los requisitos legales específicos de la jurisdicción correspondiente.

A pesar de que esta norma no incluye la preparación forense, la adecuada preparación forense puede apoyar al proceso de identificación, recolección, adquisición y preservación de la evidencia digital. La preparación forense es el logro de un nivel apropiado de capacidad por parte de una organización para identificar, recolectar, adquirir, preservar, proteger y analizar la evidencia digital. A diferencia de los procesos y las actividades descriptos en esta norma, los cuales esencialmente son medidas de respuesta para investigar un incidente luego de ocurrido, la preparación forense es un proceso proactivo que intenta realizar una planificación para tales eventos.

Esta norma complementa a la IRAM-ISO/IEC 27001 y la IRAM-ISO/IEC 27002, en particular a los requisitos de control relacionados con la adquisición de potencial evidencia digital proporcionando guías adicionales para la implementación. Asimismo, esta norma tiene aplicaciones en contextos independientes de las IRAM-ISO/IEC 27001 e IRAM-ISO/IEC 27002. Se recomienda leer esta norma en conjunto con otras normas relacionadas a la evidencia digital y la investigación de los incidentes de seguridad de la información.

1 OBJETO Y CAMPO DE APLICACIÓN

Esta norma proporciona guías para actividades específicas en el manejo de la evidencia digital, es decir, la identificación, la recolección, la adquisición y la preservación de la evidencia digital que pueda llegar a tener valor probatorio. Esta norma proporciona guías a las personas con respecto a situaciones comunes que pueden encontrarse a lo largo del proceso de manejo de evidencia digital y asiste a las organizaciones en sus procesos disciplinarios y facilita el intercambio de potencial evidencia digital entre jurisdicciones.

Esta norma da guías para los siguientes dispositivos y/o funciones que se utilizan en varias circunstancias:

- medios de almacenamiento digital utilizados en computadoras estándar como discos rígidos, disquetes, discos ópticos y magnéticos, dispositivos de datos con funciones similares,
- dispositivos móviles, asistentes digitales personales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria,
- sistemas de navegación móviles,
- cámaras digitales de foto y video (incluyendo circuitos cerrados de televisión CCTV),[1]

[1] NOTA IRAM. Los circuitos cerrados de televisión (CCTV) al momento de publicación de esta norma están siendo reemplazados por sistemas de videovigilancia (VSS).

- computadoras estándar con conexiones de red,
- redes basadas en TCP/IP y otros protocolos digitales, y
- dispositivos con funciones similares a las antes mencionadas.

NOTA 1. La lista de dispositivos antes mencionados es indicativa y no exhaustiva.

NOTA 2. Las circunstancias incluyen los dispositivos antes mencionados que existen en formas diversas. Por ejemplo, un sistema automotor puede incorporar un sistema de navegación móvil, almacenamiento de datos y un sistema sensible.

2 DOCUMENTOS NORMATIVOS PARA CONSULTA

Todo documento normativo que se menciona a continuación es indispensable para la aplicación de este documento.

Cuando en el listado se mencionan documentos normativos en los que se indica el año de publicación, significa que se debe aplicar dicha edición. En caso contrario, se debe aplicar la edición vigente, incluyendo todas sus modificaciones.

IRAM-ISO/IEC 17020, Evaluación de la conformidad. Requisitos para el funcionamiento de diferentes tipos de organismos que realizan la inspección

IRAM-ISO/IEC 17025:2005, Requisitos generales para la competencia de los laboratorios de ensayo y calibración

ISO/TR 15801, Document management - Information stored electronically - Recommendations for trustworthiness and reliability

ISO/IEC 27000, Information technology - Security techniques - Information security management systems - Overview and vocabulary

3 TÉRMINOS Y DEFINICIONES

Para los propósitos de este documento, los términos y definiciones de la ISO/IEC 27000, ISO/IEC 17020, ISO/IEC 17025 e ISO/TR 15801, así como los siguientes, aplican.

3.1
adquisición
proceso de creación de una copia de los datos dentro de un conjunto definido

NOTA. El producto de la adquisición es una copia de la potencial evidencia digital.

3.2
espacio asignado
“allocated space”
área en el medio digital, que incluye la memoria primaria, que está en uso para el almacenamiento de datos, incluyendo metadatos

3.3
recolección
proceso de recopilación de elementos físicos que contienen potencial evidencia digital

3.4
dispositivo digital
equipamiento electrónico utilizado para procesar o almacenar datos digitales

3.5
evidencia digital
información o dato, almacenado o transmitido en forma binaria, que puede utilizarse como evidencia

NOTA IRAM. A los efectos de equivalencia normalizadora la evidencia digital deviene en sinónimo de la prueba indiciaria informática, la cual una vez modelada en un documento digital (archivo) se transforma en prueba documental informática. Ver Anexo C para más información.

3.6
copia forense
imagen forense
duplicación forense
copia de la evidencia digital que se ha producido para mantener la confiabilidad de la evidencia al incluir tanto la evidencia digital como la forma de verificación cuando el método para verificarla puede estar embebido o ser independiente de las herramientas utilizadas para realizar la verificación

3.7
primer interviniente en la evidencia digital
PIED
“digital evidence first responder”
DEFR
persona que está autorizada, capacitada y calificada para actuar primero en el lugar de un incidente al realizar la recolección y la adquisición de la evidencia digital con la responsabilidad por el manejo de dicha evidencia

NOTA. Autoridad, capacitación y calificación son los requisitos esperados necesarios para producir evidencia digital confiable, pero las circunstancias particulares pueden resultar en que una persona no cumpla con los tres requisitos. En este caso, se recomienda considerar la ley local, la política organizacional y las circunstancias particulares.

3.8
especialista en evidencia digital
EED
“digital evidence specialist”
DES
persona que puede llevar a cabo las tareas de un PIED y que tiene conocimiento especializado, capacidad y aptitud para manejar un amplio rango de temas técnicos

NOTA. Un EED puede tener capacidades adicionales específicas como, por ejemplo, la adquisición en redes, la adquisición de RAM, conocimiento de software de sistemas operativos o unidad central (“*mainframe*”).

3.9
medio de almacenamiento digital
dispositivo en el cual se graban datos digitales

[Adaptado de la ISO/IEC 10027:1990]

3.10
depósito de preservación de la evidencia
entorno seguro o ubicación en la cual se almacena la evidencia recolectada o adquirida

NOTA. Se recomienda no exponer un depósito de preservación de la evidencia a campos magnéticos, polvo, vibraciones, humedad o cualquier otro elemento ambiental (tales como temperatura o humedad extremas) que pueda dañar la potencial evidencia digital dentro del depósito.

3.11
valor del digesto matemático
valor de "*hash*"
secuencia de bits que es la salida de una función de digesto matemático

[ISO/IEC 10118-1:2000]

3.12
identificación
proceso que involucra la búsqueda, el reconocimiento y la documentación de la potencial evidencia digital

3.13
obtención de una copia forense
proceso para la creación de una copia bit a bit de un medio de almacenamiento digital

NOTA. A la copia bit a bit también se la conoce como copia física.

EJEMPLO. Cuando se obtiene una copia forense de un disco rígido, el PIED también copia datos que han sido borrados.

3.14
periférico
dispositivo conectado a un dispositivo digital con el fin de expandir sus funcionalidades

3.15
preservación
proceso para mantener y salvaguardar la integridad y/o la condición original de la potencial evidencia digital

3.16
confiabilidad
propiedad de resultados y comportamiento esperados coherentes

[ISO/IEC 27000:2009]

3.17
repetibilidad
propiedad de un proceso para obtener los mismos resultados de un ensayo en el mismo entorno de ensayo (iguales computadoras, discos rígidos, modos de operación, etc.)

3.18
reproducibilidad
propiedad de un proceso para obtener los mismos resultados de un ensayo en diferentes entornos de ensayo (distintas computadoras, discos rígidos, operadores, etc.)

3.19
adulteración
“spoliation”
acto de realizar o permitir cambios a la potencial evidencia digital lo cual disminuye su valor probatorio

3.20
fecha y hora del sistema
fecha y hora generadas por el reloj del sistema y utilizadas por el sistema operativo, no el tiempo computado por el sistema operativo

3.21
adulteración intencional
“tampering”
acto deliberado de hacer o permitir cambios a la evidencia digital (es decir, adulteración intencional o deliberada)

3.22
marca de tiempo
“timestamp”
parámetro de la variable tiempo que indica un punto en el tiempo con respecto a una referencia común de fecha y hora

[ISO/IEC 11770-1:1996]

3.23
espacio no asignado
“unallocated space”
área del medio digital, incluyendo la memoria principal, que no ha sido asignada por el sistema operativo, y que está disponible para el almacenamiento de datos, incluyendo los metadatos

3.24
validación
confirmación, a través del aporte de pruebas objetivas, del cumplimiento de los requisitos especificados para una aplicación o un uso previsto

[ISO/IEC 27004:2009]

3.25
función de verificación
función que se utiliza para verificar que dos conjuntos de datos son idénticos

NOTA 1. Dos conjuntos no idénticos de datos no deberían producir una coincidencia idéntica al utilizar una función de verificación.

NOTA 2. Las funciones de verificación normalmente se implementan utilizando funciones de digesto matemático, tales como MD5, SHA1, etc. pero se pueden utilizar otros métodos.

NOTA IRAM. Se recomienda utilizar algoritmos que no sean obsoletos ni que hayan sido vulnerados o como mínimo aplicarlos de manera conjunta en forma tal que resulten aptos para garantizar la integridad del conjunto de datos a los que se los aplica. Una lista de algoritmos no obsoletos se puede encontrar en el SD12 del ISO/IEC JTC 1/SC 27 que se puede descargar de https://www.din.de/en/meta/jtc1sc27/downloads.

3.26
dato volátil
dato que es especialmente propenso a cambiar y que puede modificarse fácilmente

NOTA. Un cambio puede ser desconectar la energía eléctrica o pasar a través de un campo magnético. Un dato volátil también incluye datos que cambian cuando cambia el sistema. Los datos almacenados en la RAM o direcciones de IP dinámicas son ejemplos.

NOTA IRAM. La definición siguiente se considera necesaria para el uso de esta norma.

examen
conjunto de procesos aplicados para identificar y recuperar potencial evidencia digital pertinente de una o más fuentes

[ISO/IEC 27042:2015, 3.7]

4 ABREVIATURAS

Para los fines de este documento, se aplican las abreviaturas siguientes:

AVI	interfaz de audio y video “Audio Video Interleave”
CCTV	circuito cerrado de televisión
CD	disco compacto “Compact Disk”
ADN	ácido desoxirribonucléico
PIED	primer interviniente en la evidencia digital
EED	especialista en evidencia digital
DVD	disco de video digital “Digital Video/Versatile Disk”
ESN	número de serie electrónico “Electronic Serial Number”
GPS	sistema de posicionamiento global “Global Positioning System”
GSM	sistema global para las comunicaciones móviles “Global System for Mobile Communication”
IMEI	identidad internacional del equipamiento móvil “International Mobile Equipment Identity”
IP	protocolo de internet “Internet Protocol”
ISIRT	equipo de respuesta a incidentes de seguridad de la información “Information Security Incident Response Team”
LAN	red de área local “Local Area Network”
MD5	algoritmo de digesto de mensaje 5 “Message-Digest Algorithm 5”
MP3	formato de audio. MPEG capa de audio 3 “MPEG Audio Layer 3”
MPEG	formato de video. grupo de expertos en imágenes en movimiento “Moving Picture Experts Group”

NAS almacenamiento conectado a la red “Network Attached Storage”

PDA asistente digital personal “Personal Digital Assistant”

PED dispositivo electrónico personal “Personal Electronic Device”

PIN número de identificación personal “Personal Identification Number”

PUK clave de desbloqueo del PIN “PIN Unlock Key”

RAID matriz redundante de discos independientes “Redundant Array of Independent Disks”

RAM memoria de acceso aleatorio “Random Access Memory”

RFID identificación por radiofrecuencia “Radio Frequency Identification”

SAN red de área de almacenamiento “Storage Area Network”

SHA algoritmo seguro de digesto matemático “Secure Hash Algorithm”

SIM módulo de identidad del suscriptor “Subscriber Identity Module”

USB bus universal en serie “Universal Serial Bus”

UPS suministro de energía eléctrica sin interrupciones “Universal Power Supply”

USIM módulo de identidad universal del suscriptor “Universal Subscriber Identity Module”

UV ultravioleta

Wi-Fi fidelidad inalámbrica “Wireless Fidelity”

NOTA IRAM. La abreviatura siguiente se utiliza en esta norma.

TCP protocolo de control de transmisión “Transmission Control Protocol”

5 GENERALIDADES

5.1 Contexto para la recolección de evidencia digital

Las evidencias digitales se pueden usar en distintos escenarios, cada uno de los cuales tiene un equilibrio diferente entre la calidad de la evidencia, el cumplimiento de los plazos requeridos para el análisis, la restauración del servicio y el costo de la recolección de evidencias digitales. Las organizaciones, por lo tanto, requieren tener un proceso de priorización que identifique las necesidades y sopese la calidad de las evidencias, el cumplimiento de los plazos requeridos y la restauración del servicio antes de ocupar los recursos del PIED. Un proceso de priorización implica llevar a cabo una evaluación del material disponible para determinar el posible valor probatorio y el orden en el que se recomienda recolectar, adquirir o preservar las potenciales evidencias digitales. La priorización se lleva a cabo para minimizar el riesgo de adulterar las potenciales evidencias digitales y maximizar el valor probatorio de las potenciales evidencias digitales recolectadas.

5.2 Principios de las evidencias digitales

En la mayoría de las jurisdicciones y las organizaciones, las evidencias digitales se rigen por tres principios fundamentales: la pertinencia, la confiabilidad y la suficiencia[2]. Estos tres principios son importantes en todas las investigaciones, no solo en aquellas en las que la evidencia digital necesite ser admisible en un juicio. La evidencia digital es pertinente cuando sirve para demostrar o descartar un elemento del caso específico que se investiga. Aunque la definición detallada de *confiable* varía entre las jurisdicciones, el significado general del principio *para garantizar que la evidencia digital es lo que aparenta ser* está ampliamente extendido. No siempre es necesario que el PIED recolecte todos los datos o realice una copia completa de la evidencia digital original. En muchas jurisdicciones, el concepto de suficiencia significa que el PIED necesita recolectar la potencial evidencia digital suficiente para permitir que los elementos de la cuestión puedan ser examinados o investigados adecuadamente. La comprensión de este concepto es importante para el PIED para priorizar el esfuerzo correctamente cuando el tiempo o el costo es una preocupación.

NOTA. Se recomienda que el PIED garantice que la recolección de las potenciales evidencias digitales se realice de acuerdo con el marco normativo de la jurisdicción local, como lo requieran las circunstancias específicas.

Se recomienda que todos los procesos a usar por los PIED y los EED se validen antes de su uso. Si la validación se realiza externamente, se recomienda que el PIED o el EED verifiquen que la validación es apropiada para su uso específico en los procesos y el entorno y las circunstancias en las cuales los procesos se van a utilizar. Se recomienda que los PIED o los EED también:

a) documenten todas las acciones;

b) determinen y apliquen un método para establecer la exactitud y la confiabilidad de las copias de las potenciales evidencias digitales, en comparación con la fuente original; y

c) adviertan que el acto de preservar las potenciales evidencias digitales a veces puede ser invasivo.

5.3 Requisitos para el manejo de la evidencia digital

5.3.1 Generalidades

Los principios establecidos en 5.2 pueden cumplirse de la manera siguiente:

- pertinencia: se recomienda que sea posible demostrar que el material adquirido sea pertinente a la investigación, es decir, que contiene información que aporta valor a la investigación de un incidente específico y que existe una razón fundada para haberlo adquirido. A través de la auditoría y la justificación, se recomienda que el PIED sea capaz de describir los procedimientos seguidos y explicar cómo se tomó la decisión para realizar la adquisición de cada elemento;

- confiabilidad: se recomienda que todos los procesos utilizados en el manejo de potenciales evidencias digitales sean auditables y repetibles. Se recomienda que los resultados de la aplicación de estos procesos sean reproducibles;

- suficiencia: Se recomienda que los PIED reúnan suficiente material para permitir que se realice una investigación apropiada. Se recomienda que los PIED sean capaces, a través de la auditoría y la justificación, de indicar cuánto material, en total, fue considerado y los procedimientos utilizados para decidir cuánto y qué material fue adquirido.

NOTA. Se permite reunir el material a través de actividades de adquisición, de recolección o de ambas.

[2] NOTA IRAM. En el anexo C se puede encontrar la explicación sobre los principios de criminalística en nuestro marco legal.

Existen cuatro aspectos claves en el manejo de las evidencias digitales: que sean *auditables*, justificables y, repetibles o reproducibles en función de las circunstancias particulares.

5.3.2 Auditable

Se recomienda que un evaluador independiente u otras partes interesadas autorizadas puedan evaluar las actividades realizadas por un PIED y un EED. Esto va a ser posible gracias a la documentación apropiada de todas las acciones realizadas. Se recomienda que los PIED y los EED sean capaces de justificar el proceso de toma de decisiones en la selección de un determinado curso de acción. Se recomienda que los procesos realizados por un PIED y un EED estén disponibles para una evaluación independiente con el fin de determinar si se siguió un método científico, técnica o procedimiento apropiado.

5.3.3 Repetible

La repetibilidad se establece cuando se producen los mismos resultados de un ensayo en las condiciones siguientes:

- utilizando el mismo procedimiento y método de medición;
- utilizando los mismos instrumentos y bajo las mismas condiciones; y
- se puede repetir en cualquier momento después del ensayo original.

Se recomienda que un PIED con las calificaciones y la experiencia adecuadas sea capaz de realizar todos los procesos descritos en la documentación y llegar a los mismos resultados, sin orientación o interpretación. Se recomienda que el PIED sea consciente de que puede haber circunstancias en las que no sea posible repetir el ensayo, por ejemplo, cuando un disco rígido original ha sido copiado y reutilizado, o cuando un elemento involucra a la memoria volátil. En este caso, se recomienda que el PIED asegure que el proceso de adquisición es confiable. Para lograr la repetibilidad, se recomienda realizar el control de la calidad y la documentación del proceso.[3]

5.3.4 Reproducible

La reproducibilidad se establece cuando se producen los mismos resultados de un ensayo en las condiciones siguientes:

- utilizando el mismo método de medición;
- utilizando diferentes instrumentos y bajo diferentes condiciones; y
- se puede reproducir en cualquier momento después del ensayo original.

Las necesidades para reproducir resultados varían según las jurisdicciones y las circunstancias, por lo que el PIED, o la persona a cargo de la reproducción, necesita ser informada acerca de las condiciones aplicables.

5.3.5 Justificable

Se recomienda que el PIED pueda justificar todas las acciones y los métodos utilizados en el manejo de las potenciales evidencias digitales. La justificación puede lograrse mediante la demostración de que la decisión fue la mejor elección para obtener todas las potenciales evidencias digitales. Otro PIED o EED también puede demostrar esto reproduciéndolo satisfactoriamente o validando las acciones y los métodos utilizados.

[3] NOTA IRAM. Estas son condiciones necesarias, pero no suficientes para lograr la repetibilidad.

Lo mejor para la organización es emplear un PIED o un EED que posea los conocimientos básicos y las competencias indicadas en el anexo A de esta norma. Esto garantiza que se siguen los procesos y los procedimientos correctos al manejar las potenciales evidencias digitales, para garantizar la eventual preservación de la evidencia digital que pueda tener valor probatorio. Esto también garantiza que las organizaciones son capaces de utilizar la potencial evidencia digital, por ejemplo, en sus procedimientos disciplinarios o para facilitar el intercambio de potenciales evidencias digitales entre jurisdicciones.

NOTA. Las competencias indicadas en el anexo A se limitan a la función del PIED que está alineada con el rol del EED tal como se define en 3.8.

5.4 Proceso de manejo de evidencias digitales

5.4.1 Generalidades

Aunque el proceso de manejo de evidencia digital completo incluye otras actividades (es decir, la presentación, la disposición final, etc.), el objeto y campo de aplicación de esta norma solo se refiere al proceso inicial de manejo que consiste en la identificación, la recolección, la adquisición y la preservación de la potencial evidencia digital.

La evidencia digital por su naturaleza puede ser frágil. Se la puede alterar, adulterar intencionalmente o destruir debido a un manejo o examen inadecuados. Se recomienda que quienes manejen la evidencia digital sean competentes para identificar y gestionar tanto los riesgos como las consecuencias de los potenciales cursos de acción cuando se tratan las evidencias digitales. La impericia para manejar dispositivos digitales de manera apropiada puede hacer que las potenciales evidencias digitales, contenidas en dichos dispositivos digitales, sean inservibles.

Se recomienda que los PIED y los EED sigan procedimientos documentados para garantizar que se mantengan la integridad y la confiabilidad de la potencial evidencia digital. Se recomienda que los procedimientos incluyan las pautas de manejo para las fuentes de potencial evidencia digital e incluyan los principios fundamentales siguientes:

- minimizar el manejo del dispositivo digital original o de la potencial evidencia digital;
- responder por cualquier cambio y documentar las acciones realizadas (en la medida en que, con ello, un experto sea capaz de formar una opinión sobre la confiabilidad);
- cumplir con la normativa local sobre evidencia; y
- se recomienda que el PIED y el EED no tomen medidas más allá de sus competencias.

Cumpliendo con los principios fundamentales y los requisitos del manejo de la potencial evidencia digital, se recomienda preservar esta evidencia. Específicamente en el caso que se hagan cambios inevitables, todas las acciones y sus fundamentos necesitan estar documentados. Cada proceso del manejo de la evidencia digital, es decir, la identificación, la recolección, la adquisición y la preservación, se analizan con más detalle en los capítulos que siguen.

5.4.2 Identificación

La evidencia digital está representada en forma física y lógica. La forma física incluye la representación de los datos dentro de un dispositivo tangible. La forma lógica de la potencial evidencia digital se refiere a la representación virtual de los datos dentro de un dispositivo.

El proceso de identificación implica la búsqueda, el reconocimiento y la documentación de la potencial evidencia digital. Se recomienda que el proceso de identificación identifique los medios de almacenamiento digital y los dispositivos de procesamiento que pueden contener potencial evidencia digital pertinente al incidente. Este proceso también incluye una actividad para priorizar la recolección

de evidencia en función de su volatilidad. Se recomienda identificar la volatilidad de los datos para garantizar el orden correcto de los procesos de recolección y adquisición para minimizar el daño a la potencial evidencia digital y obtener la mejor evidencia. Además, se recomienda que el proceso identifique la posibilidad de potencial evidencia digital oculta. Se recomienda que el PIED y el EED sean conscientes de que no todos los tipos de medios de almacenamiento digital pueden identificarse y ubicarse fácilmente, por ejemplo, la computación en la nube, el NAS y el SAN; todos agregan un componente virtual al proceso de identificación.

Se recomienda que el PIED realice una búsqueda exhaustiva de elementos que puedan contener potencial evidencia digital. Los diferentes tipos de dispositivos digitales que pueden contener potencial evidencia digital pueden pasarse por alto fácilmente (por ejemplo, debido a su pequeño tamaño), disfrazarse o mezclarse entre otros materiales no pertinentes.

Los apartados 6.1 y 6.6 proporcionan información adicional sobre los aspectos de la cadena de custodia, el embalaje y el etiquetado de la identificación de la evidencia digital. El capítulo 7 especifica guías pertinentes a las instancias específicas de identificación, recolección, adquisición y preservación de evidencia digital.

5.4.3 Recolección

Una vez que se identifican los dispositivos digitales que pueden contener potencial evidencia digital, se recomienda que el PIED y el EED decidan entre recopilar o adquirir durante el siguiente proceso. Hay una serie de factores de decisión para esto, que se discuten con más detalle en el capítulo 7. Se recomienda basar la decisión en las circunstancias.

La recolección es un proceso incluido en el proceso de manejo de la evidencia digital en el cual los dispositivos que pueden contener potencial evidencia digital se trasladan de su ubicación original a un laboratorio u otro entorno controlado para su posterior adquisición y análisis. Los dispositivos que contienen potencial evidencia digital pueden estar en uno de dos estados: encendido o apagado. Se requieren diferentes enfoques y herramientas, dependiendo del estado del dispositivo. Los procedimientos locales pueden aplicarse a los enfoques y las herramientas utilizados para el proceso de recolección.

Este proceso incluye documentar todo el enfoque, así como el embalaje de estos dispositivos antes del transporte. Es importante que el PIED y el EED recolecten cualquier material que pueda estar relacionado con la potencial información digital (por ejemplo, papeles con contraseñas anotadas, bases y conectores de energía eléctrica para dispositivos de sistema integrados). La potencial evidencia digital puede perderse o dañarse si no se toman los recaudos pertinentes. Se recomienda que el PIED y el EED adopten el mejor método de recolección posible basado en la situación, el costo y el tiempo, y documenten la decisión de usar un método en particular.

NOTA 1. No siempre se recomienda el traslado de los medios de almacenamiento digital y se recomienda que el PIED se asegure de ser competente para trasladar los medios de almacenamiento, y reconocer cuándo es apropiado y permitido hacerlo.

NOTA 2. Se recomienda documentar los detalles sobre los dispositivos digitales no recopilados con la justificación para su exclusión, de acuerdo con los requisitos de la jurisdicción correspondiente.

5.4.4 Adquisición

El proceso de adquisición implica producir una copia forense (por ejemplo, disco rígido completo, partición, archivos seleccionados) y documentar los métodos utilizados y las actividades realizadas. Se recomienda que el PIED adopte un método de adquisición adecuado basado en la situación, el costo y el tiempo, y documente la decisión de usar un método o herramienta particular de manera adecuada.

Se recomienda documentar de manera clara y detallada los métodos utilizados para adquirir potencial evidencia digital y, en la medida de lo posible, se recomienda que sean reproducibles o verificables por un PIED competente. Se recomienda que un PIED o EED adquiera la potencial evidencia digital de la

manera menos invasiva para evitar la introducción de cambios cuando sea posible. Al realizar este proceso, se recomienda que el PIED considere el método más apropiado para usar. Si el proceso resulta en una alteración inevitable de los datos digitales, se recomienda documentar las actividades realizadas para responder por los cambios en los datos.

Se recomienda que el método de adquisición utilizado produzca una copia forense de la potencial evidencia digital o de los dispositivos digitales que puedan contener potencial evidencia digital. Se recomienda verificar tanto la fuente original como la copia forense con una función de verificación probada (de probada exactitud en ese momento) que sea aceptable para la persona que va a utilizar la evidencia. Se recomienda que la fuente original y cada copia forense produzcan la misma salida de la función de verificación.

NOTA IRAM. Se recomienda conservar, junto con la potencial evidencia digital y la copia forense, las herramientas utilizadas para ejecutar la función de verificación, así como la documentación que demuestre que en ese momento era de probada exactitud.

Hay circunstancias en las que el proceso de verificación no se puede realizar, por ejemplo, al adquirir un sistema en ejecución, cuando la copia original contiene sectores de error o el período de tiempo de adquisición es limitado. En tales casos, se recomienda que el PIED use el mejor método posible disponible y sea capaz de justificar y defender la selección del método. Si la obtención de la copia forense no se puede verificar, entonces esto necesita documentarse y justificarse. Si es necesario, se recomienda que el método de adquisición utilizado pueda obtener el espacio asignado y no asignado.

NOTA 1. Cuando el proceso de verificación no se puede realizar sobre la fuente completa debido a errores en la fuente, se puede realizar la verificación usando aquellas partes de la fuente que se pueden leer de manera confiable.

Puede haber casos en los que no sea factible o permisible crear una copia forense de una fuente de evidencia, como cuando su volumen es demasiado grande. En estos casos, un PIED puede realizar una adquisición lógica, dirigida solo a tipos de datos, directorios o ubicaciones específicos. Esto generalmente se realiza a nivel de archivo y partición. Durante la adquisición lógica, se pueden copiar espacios asignados de archivos activos y no basados en archivos en los medios de almacenamiento digital; según el método utilizado, se puede no copiar los archivos eliminados y el espacio no asignado. Otras instancias en las cuales este método puede ser útil son cuando están involucrados sistemas de misión crítica que no se pueden apagar.

NOTA 2. Algunas jurisdicciones pueden requerir un tratamiento especial para los datos; por ejemplo, que se lo selle en presencia del propietario de los datos. Se recomienda realizar el sellado de acuerdo con los requisitos locales (legislativos y de procedimientos).

5.4.5 Preservación

Se recomienda preservar la potencial evidencia digital para garantizar su utilidad en la investigación. Es importante proteger la integridad de la evidencia. El proceso de preservación implica la salvaguarda de la potencial evidencia digital y los dispositivos digitales que pueden contener potencial evidencia digital de adulteración intencional o no. Se recomienda iniciar y mantener el proceso de preservación a lo largo de los procesos de manejo de evidencia digital, comenzando por la identificación de los dispositivos digitales que contienen potencial evidencia digital.

En el mejor de los casos, se recomienda que no haya ninguna adulteración de los datos en sí mismos ni de ningún metadato asociado con ellos (por ejemplo, marcas de fecha y hora). Se recomienda que el PIED pueda demostrar que la evidencia no ha sido modificada desde que fue recolectada o adquirida, o proporcionar la justificación y las acciones documentadas si se hicieron cambios inevitables.

NOTA. En algunos casos, la confidencialidad de la potencial evidencia digital es un requisito, ya sea un requisito del negocio o un requisito legal (por ejemplo, la privacidad). Se recomienda preservar la potencial evidencia digital de manera tal que garantice la confidencialidad de los datos.

6 COMPONENTES CLAVE DE LA IDENTIFICACIÓN, LA RECOLECCIÓN, LA ADQUISICIÓN Y LA PRESERVACIÓN DE LA EVIDENCIA DIGITAL

6.1 Cadena de custodia

En cualquier investigación, se recomienda que el PIED pueda responder por todos los datos y dispositivos adquiridos en el momento en que estén bajo la custodia del PIED. El registro de la cadena de custodia es un documento que identifica la cronología del movimiento y el manejo de la potencial evidencia digital. Se recomienda instituirlo a partir del proceso de recolección o adquisición. Esto generalmente se logra rastreando el historial del elemento desde el momento en que fue identificado, recolectado o adquirido por el equipo investigador hasta el estado y la ubicación actuales.

El registro de la cadena de custodia es un documento o una serie de documentos relacionados que detalla la cadena de custodia y registra quién fue responsable de manejar la potencial evidencia digital, ya sea en forma de datos digitales u otros formatos (como notas en papel). El propósito de mantener un registro de la cadena de custodia es permitir la identificación del acceso y el movimiento de la potencial evidencia digital en cualquier momento dado. El registro de la cadena de custodia en sí mismo puede constar de más de un documento, por ejemplo, para potencial evidencia digital, se recomienda que exista un documento contemporáneo que registre la adquisición de datos digitales a un dispositivo en particular, el movimiento de ese dispositivo y la documentación que registre extractos o copias posteriores de potencial evidencia digital para su análisis u otros fines. Se recomienda que el registro de la cadena de custodia contenga, como mínimo, la información siguiente:

- un identificador único de evidencia;
- quién accedió a la evidencia, en qué momento y en qué lugar;
- quién ingresó o retiró la evidencia al o del depósito de preservación de la evidencia y cuándo lo hizo;
- por qué retiró la evidencia (qué caso y el propósito) y la autoridad pertinente, cuando corresponda;
- cualquier cambio inevitable en la potencial evidencia digital, así como el nombre de la persona responsable y la justificación para la introducción del cambio.

Se recomienda mantener la cadena de custodia durante todo el ciclo de vida de la evidencia y preservarla durante un cierto período de tiempo después del final del ciclo de vida de la evidencia; este período de tiempo se puede establecer de acuerdo con las jurisdicciones locales respecto de la recolección y el uso de evidencia. Se recomienda establecerla desde el momento en que se adquieren los dispositivos digitales o la potencial evidencia digital y se recomienda no comprometerla.

NOTA. Algunas jurisdicciones pueden tener requisitos especiales con respecto a la cadena de custodia. Se recomienda que el PIED cumpla con esos requisitos.

6.2 Precauciones en el sitio del incidente

6.2.1 Generalidades

Se recomienda que el PIED realice actividades para asegurar y proteger la ubicación de la potencial evidencia digital en cuanto llegue al sitio. Sujeto a la ley local, se recomienda que las actividades se orienten a lo siguiente:

- asegurar y tomar el control del área que contiene los dispositivos;
- determinar quién es la persona a cargo de la ubicación;

- garantizar que las personas se alejen de los dispositivos y los suministros de energía eléctrica;
- documentar a cualquier persona que tenga acceso a la ubicación y a cualquiera que tenga una razón para involucrarse en el lugar del incidente;
- si el dispositivo está encendido, no apagarlo y si el dispositivo está apagado, no encenderlo;
- si es posible, documentar (por ejemplo, a través de boceto, fotografía o video) el lugar del hecho, todos los componentes y cables en su posición original. Si no hay una cámara de fotos o de video disponible, dibujar un boceto del esquema del sistema y etiquetar los puertos y cables para que el sistema pueda ser validado y reconstruido en una fecha posterior; y
- si está permitido, buscar en las áreas, elementos como notas adhesivas, diarios, papeles, computadoras portátiles o manuales de hardware y software con detalles cruciales sobre los dispositivos, como contraseñas y PIN.

NOTA 1. Algunas jurisdicciones pueden tener requisitos especiales para la admisión de fotografías y video como evidencia. Se recomienda que el PIED cumpla con esos requisitos.

NOTA 2. Los PIED necesitan ser conscientes de que la potencial evidencia digital puede no estar siempre en ubicaciones obvias, como el almacenamiento distribuido o virtualizado.

Se recomienda que el PIED primero conozca todos los riesgos involucrados en la realización de todos los procesos durante la investigación. Se recomienda considerar la protección del personal y de la potencial evidencia digital en el lugar del incidente.

6.2.2 Personal

Es importante realizar una evaluación de riesgos con respecto a la seguridad del personal antes de comenzar el proceso, ya que la seguridad del personal involucrado en el proceso es vital. Las cuestiones a considerar al evaluar los riesgos al personal incluyen, entre otras, las siguientes:

- ¿van a estar presentes las personas investigadas? Si están presentes, ¿son propensas a la violencia?
- ¿a qué hora del día se va a llevar a cabo el operativo?
- ¿se puede aislar el lugar del incidente de terceros ajenos?
- ¿hay armas en la zona?
- ¿hay algún peligro físico para las personas presentes?
- ¿se podría haber configurado algo cercano, incluido el dispositivo, que pudiera causar daños físicos si se lo maneja de manera inapropiada, por ejemplo, una trampa oculta?
- ¿el material a recolectar tiene alguna probabilidad de causar daño psicológico u ofensa?
- ¿el lugar del incidente puede considerarse inseguro?
- ¿la zona circundante tiene un impacto en el riesgo potencial?

6.2.3 Potencial evidencia digital

Se recomienda que el PIED tenga cuidado al usar una herramienta específica para recopilar o adquirir potencial evidencia digital. No calcular los riesgos antes de actuar puede conducir a la pérdida de parte o la totalidad de la potencial evidencia digital debido a la tecnología aplicada durante la

recolección o adquisición. Se recomienda evaluar los riesgos para reducir la exposición a demandas por daños y perjuicios.

La evaluación de riesgos implica la evaluación sistemática de los riesgos y el impacto potencial que pueden tener en la investigación de la evidencia digital. Los aspectos a considerar durante la evaluación de riesgos a la potencial evidencia digital incluyen, entre otros a los siguientes:

- ¿qué tipo de métodos de recolección/adquisición se van a aplicar?
- ¿cuál es el equipamiento que se puede necesitar en el lugar?
- ¿cuál es el nivel de volatilidad de los datos y la información relacionados con la potencial evidencia digital?
- ¿es posible el acceso remoto a cualquier dispositivo digital y representa este una amenaza para la integridad de la evidencia?
- ¿qué sucede si los datos o el equipamiento se dañan?
- ¿se podrían haber comprometido los datos?
- ¿podría el dispositivo digital haber sido configurado para destruir (por ejemplo, usando una bomba lógica), adulterar u ofuscar datos si se lo apaga o se lo accede de forma no controlada?

6.3 Roles y responsabilidades

El papel del PIED implica la identificación, recolección, adquisición y preservación de potencial evidencia digital en el lugar del incidente. Incluye el desarrollo de un informe de la recolección y adquisición, pero no necesariamente el informe del análisis. El papel del PIED también implica garantizar la integridad y autenticidad de la potencial evidencia digital. En el cumplimiento de su función, se recomienda que el PIED tenga experiencia, habilidades y conocimientos adecuados para manejar potencial evidencia digital. Esto es crucial porque la potencial evidencia digital se puede adulterar fácilmente.

El PIED también puede necesitar asistencia del personal de soporte técnico en áreas relacionadas. El rol de un EED implica proporcionar soporte técnico al PIED en la identificación, recolección, adquisición y preservación de la potencial evidencia digital en el lugar del incidente. El EED proporciona experiencia especializada al PIED. La matriz de competencias para el PIED (ver Anexo A) sirve como guía para identificar sus niveles de competencia pertinentes.

NOTA. En el contexto del manejo de incidentes cuando existe un ISIRT, los roles de un PIED o EED como miembro del equipo del ISIRT se incluyen en la ISO/IEC 27035:2011.

6.4 Competencia

Se recomienda que tanto el PIED como el EED tengan las competencias técnicas y legales pertinentes (por ejemplo, las del Anexo A) y se recomienda que sean capaces de demostrar que están debidamente capacitados y tienen suficiente conocimiento técnico y legal para manejar la potencial evidencia digital de manera apropiada. Esto incluye una comprensión de los procesos y los métodos apropiados para el manejo de potenciales fuentes de evidencia digital. Una capacitación adecuada permite a los PIED manejar dispositivos digitales que contengan potencial evidencia digital. Tener el mejor conjunto de herramientas no garantiza la calidad de la evidencia digital si el PIED no es competente para realizar las tareas.

Algunas jurisdicciones han prescrito cómo se recomienda que los PIED establezcan sus calificaciones. Es responsabilidad de los PIED garantizar que estén debidamente informados sobre cómo hacer esto en las jurisdicciones pertinentes. Cuando sea necesario, se recomienda que el PIED o el

EED puedan demostrar que son competentes para manejar potencial evidencia digital utilizando las herramientas y los métodos seleccionados para realizar las tareas. También se requiere que los PIED puedan proporcionar evidencia de que continúan siendo competentes.

Algunos de los prerrequisitos para los PIED son los siguientes:

- se recomienda que estén capacitados de manera apropiada y adecuada para manejar dispositivos digitales en el contexto de las actividades de investigación;
- se recomienda que demuestren y mantengan sus habilidades y competencia ante las autoridades apropiadas en el área pertinente de manejo de potencial evidencia digital; y
- es responsabilidad de la(s) persona(s) y del empleador garantizar que estén adecuadamente capacitados y que mantengan las habilidades y las competencias.

NOTA. La competencia de un PIED puede variar de una jurisdicción a otra.

6.5 Recaudos

Evitar cualquier acción que pueda conducir a la adulteración, debido a acciones intencionales o no intencionales, de potencial evidencia digital que se almacene en dispositivos digitales. Por ejemplo, la exposición a campos magnéticos puede adulterar la potencial evidencia digital contenida en medios de almacenamiento magnético. Se recomienda que el PIED no acceda a dispositivos digitales, como por ejemplo realizar un volcado de memoria desde un dispositivo digital encendido, a menos que tengan la competencia requerida y con el uso de procesos confiables y validados.

Hay algunas circunstancias en las que no es práctico recolectar o adquirir potencial evidencia digital. Se recomienda que el PIED considere las circunstancias siguientes, entre otras:

- si no hay justificativo legal o autorización para recolectar el dispositivo digital;
- si existe la obligación de utilizar otros métodos (por ejemplo, para evitar la interrupción del negocio);
- si el PIED desea capturar el método de operación de un sospechoso durante el abuso de un sistema;
- si se recomienda realizar la recolección o adquisición de manera encubierta, en el caso de que la jurisdicción lo considere legal;
- si se trata de un dispositivo digital de misión crítica que no puede tolerar ningún tiempo de inactividad;
- si el tamaño físico del dispositivo digital es demasiado grande, como un servidor en un centro de datos o sistema RAID;
- si se trata de un dispositivo digital crítico para la seguridad de las personas que pondría en peligro la vida si se detuviera; y
- si se trata de un dispositivo digital que también presta servicios a terceras partes no involucradas.

6.6 Documentación

La documentación es crítica cuando se manejan dispositivos digitales que pueden contener potencial evidencia digital. Se recomienda que el PIED acate los puntos siguientes durante la documentación:

- se recomienda documentar cada actividad realizada. Esto es para garantizar que no se excluyan detalles durante los procesos de identificación, recolección, adquisición y preservación. También

puede ayudar en una investigación interjurisdiccional a través de la cual se puede rastrear correctamente la potencial evidencia digital que se recoge de otra parte del planeta;

- se recomienda que el PIED verifique la configuración de fecha y hora si los dispositivos digitales se encuentran encendidos y que compare la configuración de fecha y hora con una fuente de hora confiable, tal como una hora sincronizada con una fuente confiable y trazable. Se recomienda documentar estas configuraciones de hora y tomar nota de cualquier diferencia. Algunos sistemas requieren mucha interacción del usuario para obtener la configuración de fecha y hora. Se recomienda que el PIED tenga cuidado de no modificar el sistema. Se recomienda que solo personal capacitado recupere esta configuración;

- se recomienda que el PIED documente cualquier cosa visible en la pantalla del dispositivo digital: los programas y los procesos activos, así como los nombres de los documentos abiertos. Se recomienda que esta documentación incluya una descripción de aquello visible ya que algunos programas maliciosos pueden enmascararse como software conocido;

- se recomienda documentar todo movimiento de los dispositivos digitales de acuerdo con los requisitos de la jurisdicción local;

- documentar todos los identificadores únicos de los dispositivos digitales y de las partes asociadas, tales como números de serie o marcas únicas.

En el Anexo B se indican ejemplos de un conjunto mínimo de documentación para el intercambio interjurisdiccional de potencial evidencia digital.

NOTA. En los capítulos de control de los documentos y control de los registros de la IRAM 301:2005 ISO/IEC 17025:2005 se puede encontrar más información sobre la documentación.

6.7 Informe previo

6.7.1 Generalidades

Es esencial que el PIED y el EED sean adecuadamente informados por la autoridad pertinente antes de realizar sus tareas, siempre respetando todas las leyes y restricciones de confidencialidad (es decir, el fundamento de la necesidad de saber). Es importante que exista una reunión formal de informe previo para comprender el incidente, saber qué esperar y qué no esperar durante la investigación y advertir sobre la adulteración intencional o no de evidencia. Se recomienda que este informe previo sea suficiente para que los miembros estén preparados para desempeñar sus roles y responsabilidades y de esta manera garantizar la extracción de toda la potencial evidencia digital pertinente.

6.7.2 Específico a la evidencia digital

Se necesita una reunión informativa previa que se enfoque explícitamente en los lineamientos específicos a la evidencia digital para informar a los PIED acerca de detalles relacionados con la investigación. Durante esa reunión, se recomienda brindar al PIED y al EED toda la información pertinente e instrucciones detalladas relacionadas con la potencial evidencia digital a recolectar o adquirir. Esto puede incluir:

- el tipo de incidente (si se lo conoce);

- la fecha y hora del incidente (si se las conoce);

- el plan para la investigación (recolección y/o adquisición, actividad de red conocida, requisitos de datos volátiles conocidos, etc.);

- considerar dónde y cómo se almacena/transporta la potencial evidencia digital luego de la recolección o adquisición;
- las herramientas específicas necesarias para adquirir la potencial evidencia digital;
- la potencial evidencia digital que se relaciona con tipos específicos de investigación;
- el equipamiento y los manuales relacionados con los dispositivos digitales;
- recordarles a los miembros del equipo que apaguen todas las funcionalidades Bluetooth o Wi-Fi de sus teléfonos/computadoras para que estos no interactúen inadvertidamente con los dispositivos digitales, excepto los teléfonos/computadoras que se utilicen para detectar conexiones;
- la importancia de la documentación a lo largo de toda la investigación; y
- los factores legales, o de otro tipo, aplicables que pueden prohibir la recolección de cualquier dispositivo y potencial evidencia digital que contenga.

Esta reunión informativa previa específica puede formar parte de una reunión informativa previa general como se indica en 6.7.1.

6.7.3 Específico al personal

Se necesita una reunión informativa previa que se enfoque explícitamente en los lineamientos específicos sobre el personal para informar a los PIED acerca de los aspectos relacionados con las partes involucradas en la investigación. Durante la reunión de informe previo, se recomienda brindar al equipo de investigación las instrucciones relacionadas con el personal. Esto puede incluir:

- las asignaciones, los roles y las responsabilidades de los miembros del equipo de investigación en el lugar del incidente;
- si se espera que otras autoridades (personal médico, investigadores en biología forense, etc.) estén involucradas en la investigación;
- requerir a los miembros del equipo que no acepten asistencia técnica de personas no autorizadas; y
- requerir a los miembros del equipo que sigan estrictamente el procedimiento minimizando el riesgo de adulteración de la potencial evidencia digital, tal como evitar el uso de cualquier herramienta o material que pueda producir o emitir electricidad estática o un campo magnético ya que pueden dañar o destruir la potencial evidencia digital.

Esta reunión informativa previa específica puede formar parte de una reunión de informe previo general como se indica en 6.7.1.

6.7.4 Incidentes en tiempo real

Es altamente deseable que la investigación de un incidente se planifique con anticipación, pero hay circunstancias (por ejemplo, cuando un incidente se está desarrollando y se está respondiendo en tiempo real) en las cuales la planificación completa puede no haber sido posible. En estas situaciones, se recomienda informar previamente al equipo sobre las estrategias y las tácticas iniciales para la investigación y permitirle desarrollar nuevas estrategias y tácticas en respuesta a las condiciones existentes. Se recomienda que la información sobre el incidente, a medida que se desarrolla, se comparta entre los miembros del equipo lo más rápidamente posible para garantizar que las decisiones sobre las acciones a tomar puedan tomarse eficientemente y considerando debidamente la necesidad de justificación.

6.7.5 Información previa adicional

Además, la información sobre la evidencia digital y el personal, otra información importante a brindar previamente a los equipos de investigación incluye:

- la designación del área bajo investigación, incluyendo el nombre de la organización, la dirección y un mapa de ubicación (si está disponible);
- el plazo de la investigación;
- los detalles de las órdenes de allanamiento y otras autoridades aplicables a la investigación, incluidos los límites de la búsqueda y secuestro;
- los aspectos e implicancias legales;
- los plazos de la investigación;
- el equipamiento necesario para la investigación en el lugar del incidente;
- la información de logística; y
- los potenciales conflictos de interés.

Se recomienda que el PIED evite situaciones que puedan dar lugar a acusaciones de sesgo inherente. Un ejemplo de sesgo inherente es cuando un PIED copia una computadora y no otra (la cual luego resulta que contiene evidencia exculpatoria o disculpatoria) en base a una percepción formada por la información previa recibida.

6.8 Priorización en la recolección y la adquisición

Es imperativo que el PIED, al priorizar la recolección o adquisición de la potencial evidencia digital, comprenda la razón por la cual se está recolectando o adquiriendo. Como regla general, se recomienda que el PIED intente maximizar la cantidad de datos preservados durante las acciones de recolección y adquisición. Sin embargo, puede ser necesario priorizar elementos por volatilidad y/o pertinencia o potencial valor probatorio. Los elementos de alta pertinencia o potencial valor probatorio son aquellos que tienen más probabilidades de contener datos relacionados directamente con el incidente investigado.

La priorización por volatilidad solo es aplicable si las circunstancias específicas del caso investigado la requieren. La potencial evidencia digital se puede dividir en dos categorías: volátil y no volátil. Los datos volátiles pueden destruirse o perderse fácilmente para siempre si no se aplica el debido cuidado para protegerlos. Por ejemplo, desconectar el suministro de energía eléctrica de un dispositivo digital puede resultar en la pérdida de datos volátiles. Los datos no volátiles permanecen en los medios incluso si se desconecta el suministro de energía eléctrica. Debido a que algunos tipos de evidencia digital pueden tener un ciclo de vida corto, la potencial evidencia digital fácilmente puede adulterarse intencionalmente o no. En los casos en los que no está claro si los dispositivos digitales contienen potencial evidencia digital, o qué elementos son más pertinentes que otros, está permitido examinarlos antes de la recolección utilizando un proceso para determinar la prioridad. Los dispositivos digitales a considerar en la recolección incluyen, entre otros, equipos informáticos y medios de almacenamiento digital, sistemas de CCTV, PED, sistemas automotrices, sistemas de control y dispositivos electrónicos improvisados. Es necesario primero adquirir la potencial evidencia digital más volátil, como RAM, espacio de intercambio, procesos en ejecución, etc. Se recomienda que el PIED posea un conocimiento sólido para priorizar según la volatilidad.

Luego de la identificación, se recomienda que el PIED:

- priorice la potencial evidencia digital que se puede perder de forma definitiva si se desconecta el suministro de energía eléctrica; y

- tome medidas rápidas para recolectar y adquirir estos datos con métodos validados.

NOTA 1. Algunos datos volátiles pueden cambiar debido a factores como ubicación, fecha y hora y cambios en los dispositivos digitales circundantes, entre otros. Garantizar que este tipo de datos se preserven antes de mover el dispositivo.

NOTA 2. Los dispositivos digitales que contienen potencial evidencia digital pueden ser una fuente de evidencia física (por ejemplo, huellas digitales, ADN, etc.). Los PIED necesitan tener cuidado de no adulterar tal evidencia y coordinar con los recolectores de evidencias pertinentes antes de continuar con las actividades siguientes.

NOTA 3. Cuando se sospeche de la posibilidad de existencia de cifrado o código malicioso, es deseable examinar los datos volátiles.

En estas circunstancias, el tiempo puede ser un factor limitante durante una investigación. En estos casos, se recomienda dar preferencia a la potencial evidencia digital identificada como pertinente al incidente específico.

6.9 Preservación de la potencial evidencia digital

6.9.1 Generalidades

Al preservar la potencial evidencia digital adquirida y los dispositivos digitales recolectados durante el embalaje, es importante asegurar estos elementos de una manera que elimine la posibilidad de adulteración o adulteración intencional. La adulteración puede ser consecuencia de la degradación magnética, la degradación eléctrica, el calor, la exposición a humedad alta o baja, así como a golpes y vibraciones. La adulteración intencional puede resultar de actos realizados intencionalmente haciendo o permitiendo cambios a la potencial evidencia digital. Por lo tanto, es crucial proteger la potencial evidencia digital de la mejor manera posible y utilizar los datos originales lo menos posible. Es importante que el PIED esté familiarizado con los requisitos de embalaje específicos de la jurisdicción pertinente.

6.9.2 Preservación de la potencial evidencia digital

Se recomienda proteger todos los dispositivos digitales recolectados y la potencial evidencia digital adquirida tanto como sea posible de pérdidas, adulteraciones intencionales o adulteraciones. La actividad más importante en el proceso de preservación es mantener la integridad y autenticidad de la potencial evidencia digital y su cadena de custodia.

Se recomienda almacenar los dispositivos digitales recolectados y la potencial evidencia digital adquirida en un depósito de preservación de la evidencia donde se apliquen controles de seguridad física tales como sistemas de control de acceso, sistemas de vigilancia o sistemas de detección de intrusos u otro entorno controlado para la preservación de la evidencia digital. Los objetivos principales de la seguridad física son proteger y prevenir pérdidas, daños y adulteraciones intencionales, así como permitir la *auditabilidad*.

Se recomienda envolver los dispositivos digitales recolectados o colocarlos en un embalaje apropiado según la naturaleza del dispositivo para evitar la contaminación de los dispositivos digitales antes de transportarlos a otras ubicaciones. Se puede usar embalaje resistente a los golpes para evitar daños físicos a cualquier componente de los dispositivos.

- Se recomienda que el PIED considere la sensibilidad del dispositivo digital a la electricidad estática. De ser así, se recomienda asegurar el dispositivo en una bolsa antiestática.

– Las unidades principales del sistema y las computadoras portátiles necesitan estar aseguradas en un contenedor apropiado para evitar la adulteración o adulteración intencional de la potencial evidencia digital que pueda residir en éstas.

NOTA. El uso de una bolsa de Faraday u otro embalaje blindado de radiofrecuencias pueden aumentar el consumo de la batería de teléfonos móviles. Esto puede requerir la provisión de energía eléctrica auxiliar al dispositivo mientras esté dentro de la bolsa, si los recursos lo permiten.

6.9.3 Embalaje de dispositivos digitales y potencial evidencia digital

6.9.3.1 Actividades básicas: embalaje de la potencial evidencia digital

Se recomienda realizar estas actividades básicas a menos que haya una razón fundada para no hacerlas. Esto también puede conocerse como las acciones mínimas a realizar. Durante el embalaje, se recomienda al PIED tener en cuenta y abordar las actividades básicas siguientes:

– no tocar las cintas magnéticas sino tomar las cintas por su carcaza protectora o áreas que se sabe que no contiene datos (por ejemplo, bordes de los discos ópticos). Se recomienda que lo realice el PIED únicamente cuando use guantes que no dejen pelusa;

NOTA. Las áreas específicas de los medios de almacenamiento que se sabe que no contienen datos dependen del tipo de medio. Es responsabilidad del PIED conocer la tecnología actual y estar familiarizado con el manejo de los medios de almacenamiento.

– para garantizar la correcta identificación, se recomienda al PIED etiquetar toda la potencial evidencia digital. Algunas jurisdicciones tienen requisitos específicos respecto al formato del material para etiquetar la evidencia. Se recomienda que el PIED esté familiarizado y cumpla con los requisitos aplicables en el asunto en cuestión. Se recomienda que el PIED etiquete toda potencial evidencia digital, los dispositivos digitales recolectados y cualquier parte de hardware asociado con los dispositivos, con etiquetado que haga evidente cualquier adulteración intencional. Se recomienda que la etiqueta no se ubique directamente sobre partes mecánicas del dispositivo digital y se recomienda no cubrir u ocultar información de identificación importante. Se recomienda que toda potencial evidencia digital de los dispositivos recopilados se adquiera y almacene de manera de garantizar la integridad de la evidencia;

– cuando sea posible, se recomienda sellar los dispositivos digitales con aperturas y componentes móviles con etiquetas que hagan evidente cualquier adulteración intencional y se recomienda que el PIED firme sobre el sello;

– se recomienda verificar regularmente los dispositivos con baterías que contienen datos que son volátiles para garantizar que siempre tengan suficiente suministro de energía eléctrica;

– identificar y asegurar los dispositivos digitales en un contenedor adecuado a la naturaleza del dispositivo para evitar potenciales amenazas;

– se recomienda que las computadoras y los dispositivos digitales se embalen de manera de prevenir daños causados por golpes, vibraciones, alta altitud, calor y exposición a radio frecuencia durante el transporte;

– se recomienda que los medios de almacenamiento magnéticos se almacenen en embalajes magnéticamente inertes, antiestáticos y libres de partículas;

– los dispositivos digitales también pueden contener evidencia latente de rastros o biológica. Por lo tanto, es necesario realizar actividades apropiadas para preservar la potencial evidencia digital. Se recomienda que la obtención de una copia forense de la evidencia digital se realice luego de que se realice el proceso de recolección de evidencia latente de rastros o biológica sobre los dispositi-

vos. Sin embargo, se recomienda que la decisión de priorizar la recolección de evidencia se evalúe cuidadosamente para preservarla.

6.9.3.2 Actividades adicionales: embalaje de la potencial evidencia digital

Las actividades adicionales se refieren a actividades que se recomienda fuertemente realizar. Durante el embalaje, se recomienda que el PIED tenga en cuenta y aborde las actividades adicionales siguientes, cuando corresponda:

- usar guantes que no dejen pelusa y garantizar que las manos estén limpias y secas;
- proteger los dispositivos digitales de la influencia de fuentes electromagnéticas (por ejemplo, radios de policía, parlantes, máquinas de rayos X). Se recomienda que el entorno en el que se embala esté libre de electricidad estática;
- que el entorno en el que se embala esté libre de polvo, grasa y contaminantes químicos que promuevan el deterioro oxidativo y la condensación de humedad sobre la capa magnética;
- minimizar la posibilidad de sobreimpresión de patrones magnéticos (la transferencia de una señal desde una vuelta de la cinta a otra vuelta adyacente), la cual puede ocurrir cuando las cintas se almacenan por largos periodos sin uso activo, resultando en una calidad de señal pobre;
- cuando sea necesario, que las áreas de embalaje estén libres de luz ultravioleta. La luz ultravioleta puede causar degradación de ADN o dañar algún tipo de medios. Se recomienda que el PIED considere si la luz ultravioleta pone en riesgo a la potencial evidencia digital antes de seleccionar un área de embalaje;
- que los dispositivos digitales estén fuertemente protegidos de las variaciones bruscas de temperatura.

6.9.4 Transporte de la potencial evidencia digital

Se recomienda que el PIED preserve los dispositivos digitales recolectados y la potencial evidencia digital adquirida durante el transporte. Se recomienda no dejar a la potencial evidencia digital desatendida durante el proceso de transporte. Se recomienda que el PIED mantenga la cadena de custodia a lo largo del proceso de transporte para prevenir la posible adulteración o adulteración intencional, y mantener la integridad y la autenticidad de los dispositivos digitales y la potencial evidencia digital. Si la potencial evidencia digital no es transportada por el PIED o el EED, se recomienda usar el cifrado.

NOTA. Se recomienda que el PIED garantice que la recolección de información personal o sensible esté acorde con el marco normativo de la jurisdicción local sobre la protección de datos.

Durante el embalaje y el transporte, el PIED necesita estar consciente de la posible presencia de descarga electroestática que puede dañar el valor probatorio de la potencial evidencia digital. Se recomienda que el PIED garantice que las computadoras y los dispositivos digitales estén embalados en forma segura durante el transporte para prevenir daños provocados por golpes y vibraciones.

Se recomienda que el proceso de transporte permita un entorno propicio y controlado. Se recomienda que los niveles de condensación, humedad y temperatura sean adecuados para los dispositivos digitales. Evitar mantener la potencial evidencia digital y los dispositivos digitales en el vehículo de transporte por periodos prolongados y evitar que estén expuestos a luz ultravioleta.

En algunas jurisdicciones cuando las circunstancias no lo permiten, el PIED puede no acompañar la evidencia. En tales casos, se pueden utilizar mecanismos de envío autorizados y apropiados para

asegurar la seguridad de la evidencia durante el transporte. Se recomienda que los documentos del transporte y la verificación de la integridad del embalaje sean parte de la cadena de custodia.

7 INSTANCIAS DE IDENTIFICACIÓN, RECOLECCIÓN, ADQUISICIÓN Y PRESERVACIÓN

7.1 Computadoras, dispositivos periféricos y medios de almacenamiento digital

7.1.1 Identificación

7.1.1.1 Búsqueda y documentación del lugar físico del incidente

En el contexto de este capítulo, las computadoras se consideran dispositivos digitales autónomos que reciben, procesan y almacenan datos, y producen resultados. Estos dispositivos informáticos no están conectados a una red, pero pueden estar conectados a dispositivos periféricos tales como impresoras, escáneres, cámaras web, reproductores MP3, sistemas de GPS, dispositivos de radio frecuencia, etc. Se recomienda considerar (para el propósito de esta norma) a un dispositivo digital que tiene una interfaz de red pero que no está conectado al momento de la recolección o adquisición, como una computadora autónoma. Cuando se trata de una computadora con una interfaz de red, pero no se puede encontrar una conexión obvia, se recomienda ejecutar actividades para identificar dispositivos a los cuales puede haber estado conectada en el pasado reciente.

Usualmente los lugares de incidentes contienen diversos tipos de medios de almacenamiento digital. Los medios de almacenamiento digital se usan para almacenar datos de dispositivos digitales y varían en capacidad de almacenamiento. Ejemplos de medios de almacenamiento digital incluyen, pero no se limitan, a discos rígidos externos portátiles, dispositivos de memoria "*flash"* (como dispositivos USB o tarjetas SD), CD, DVD, discos Blu-ray, disquetes, cintas magnéticas y tarjetas de memoria.

Antes de poder realizar cualquier adquisición o recolección, se necesita considerar los aspectos de seguridad de las personas relacionados con la potencial evidencia digital. Estos aspectos se describen en 6.2.1 y 6.2.2. Sin embargo, se recomienda que el PIED tenga cuidado y se asegure de que un dispositivo aparentemente autónomo no haya estado recientemente conectado a una red. Cuando se sospecha que un dispositivo aparentemente autónomo ha sido recientemente desconectado, se recomienda tratarlo como un dispositivo en red para garantizar que otras partes de la red se manejen correctamente. Se recomienda que el PIED tenga en cuenta y aborde, como mínimo, lo siguiente:

- que el PIED documente el tipo y marca de cualquier dispositivo digital usado e identifique toda computadora y dispositivo periférico que puede ser necesario adquirir o recolectar, durante esta etapa inicial. Se recomienda documentar los números de serie, números de licencia y otras marcas de identificación (incluidos daños físicos) cuando sea posible;

- en la etapa de identificación, se recomienda que el estado de las computadoras y dispositivos periféricos permanezca como está. Si las computadoras o los dispositivos periféricos están apagados, no encenderlos. Si las computadoras o los dispositivos periféricos están encendidos, se recomienza que el PIED no los apague ya que puede adulterar la potencial evidencia digital;

- si las computadoras están encendidas, se recomienda que el PIED fotografíe o documente por escrito lo que muestran las pantallas. Se recomienda que cualquier documento escrito incluya una descripción de lo que es realmente visible (por ejemplo, la posición aproximada de la ventana, los títulos y los contenidos);

- un dispositivo que tiene baterías que pueden agotarse, necesita cargarse para garantizar que no se pierda la información. El PIED necesita identificar y recolectar potenciales cargadores de baterías y cables durante esta fase;

- se recomienda que el PIED también considere usar un detector de señal inalámbrica para detectar e identificar señales inalámbricas de dispositivos inalámbricos que pueden estar ocultos. Puede haber instancias en las cuales el detector de señal inalámbrica se utilice debido a restricciones de costo y tiempo y si es así, se recomienda que el PIED lo documente. Si se encuentra algún dispositivo en red, se recomienda que el PIED continúe con el proceso de manejo de evidencia como se describe en 7.2.2.2. Cuando se considera utilizar escaneo activo (es decir, difusión "*broadcast*" y/o sondeo "*probing*") en busca de dispositivos de red, se recomienda apagar el escaneo de dispositivos hasta que se haya realizado una evaluación sobre las posibilidades de que el dispositivo interactúe con otros dispositivos en el lugar del hecho. Se recomienda que los miembros del equipo recuerden que ciertos dispositivos en el lugar del hecho pueden detectar la presencia de dispositivos de escaneo activo y el uso de escaneo activo puede desencadenar acciones que pueden adulterar la potencial evidencia digital, y puede, en circunstancias extremas, resultar en la activación de trampas ocultas.

NOTA 1. En algunas jurisdicciones, si hay muchos dispositivos digitales presentes, está permitido encender dispositivos digitales en el lugar del hecho para determinar su pertinencia a la investigación. Esto se realiza en consideración del tiempo y el costo de procesamiento que puede requerirse si se adquieren dispositivos digitales no pertinentes. Si un dispositivo se enciende para evaluarlo en el lugar del hecho, se recomienda que el PIED garantice que se mantengan notas detalladas de las acciones tomadas durante el proceso.

NOTA 2. Se recomienda considerar los resultados de la volatibilidad y el proceso de priorización pertinente al preservar el estado de energía eléctrica del dispositivo digital. Si se decide que la mayoría de la información crítica es la información no volátil en el disco, entonces se puede fotografiar la pantalla del sistema en ejecución y desconectar el cable de la energía eléctrica. Si la información volátil en memoria es pertinente, entonces es crítico dejar al sistema encendido para permitir su adquisición.

7.1.1.2 Recolección de evidencia no digital

Se recomienda que el PIED considere la recolección de evidencia no digital. Para facilitar esto, se recomienda que el líder del equipo identifique a las personas responsables de las instalaciones en el lugar del hecho. A esta persona se le permite proporcionar información y documentación adicionales tales como contraseñas de dispositivos digitales y otros detalles pertinentes. El PIED necesita documentar el nombre y la designación de esta persona.

El PIED también puede necesitar recolectar alguna evidencia entrevistando personas que puedan tener información útil o pertinente sobre la potencial evidencia digital o los dispositivos digitales a recolectar. Se recomienda documentar de forma exacta cualquier respuesta. Estas personas pueden incluir el administrador de sistemas, el dueño del dispositivo, los usuarios de la computadora y de los dispositivos periféricos. Durante esta recolección verbal de evidencia, el PIED puede solicitar información tal como la configuración del sistema y la contraseña de administrador/"*root*". Esta información adicional puede ser útil en la etapa de análisis de la potencial evidencia digital. Se recomienda documentar estas conversaciones para garantizar que los detalles son exactos y las declaraciones documentadas no se puedan modificar. El PIED necesita estar familiarizado con los requisitos pertinentes a la recolección de evidencia no digital de la jurisdicción pertinente.

7.1.1.3 Proceso de toma de decisiones sobre la recolección o la adquisición

Al decidir entre la recolección de un dispositivo digital o la adquisición de la potencial evidencia digital, se recomienda considerar varios factores los cuales incluyen, pero no se limitan a lo siguiente:

- la volatibilidad de la potencial evidencia digital la cual se indica en 5.4.2 y 6.8,

- la existencia de cifrado de disco completo o volúmenes cifrados cuando la clave puede residir como dato volátil en la RAM, en dispositivos USB externos, tarjetas de memoria, otros dispositivos o medios,
- la criticidad del sistema, lo cual se indica en 5.4.4, 7.2.1.1 y 7.1.3.4,
- los requisitos legales de una jurisdicción, y
- los recursos tales como la capacidad de almacenamiento requerido, la disponibilidad de personal, las restricciones de tiempo.

La figura 1 ilustra las generalidades del proceso de toma de decisiones sobre la recolección o la adquisición.

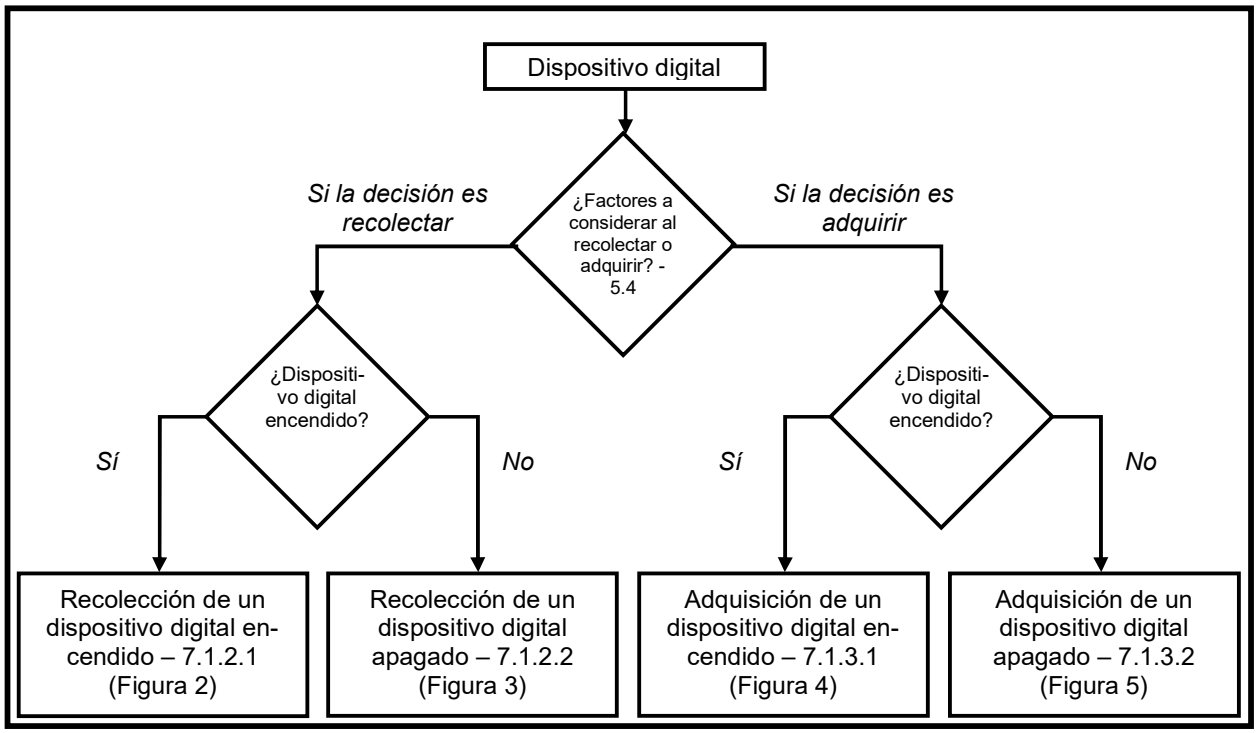

Figura 1 - Guía para la toma de decisiones sobre la recolección o la adquisición de potencial evidencia digital

7.1.2 Recolección

7.1.2.1 Dispositivos digitales encendidos

7.1.2.1.1 Generalidades

El PIED puede seguir varias guías para recolección cuando el dispositivo digital este encendido. No todas las guías son ideales y apropiadas para cualquier caso; algunas guías solo son pertinentes a casos específicos. De acuerdo con esto las guías pueden estar categorizadas como básicas o adicionales. Se recomienda aplicar las actividades básicas en todas las circunstancias, mientras que se recomienda aplicar las actividades adicionales cuando es pertinente y aplicable, dependiendo del dispositivo particular o de la circunstancia. La figura 2 ilustra las actividades básicas y adicionales aplicables a la recolección de dispositivos digitales encendidos.

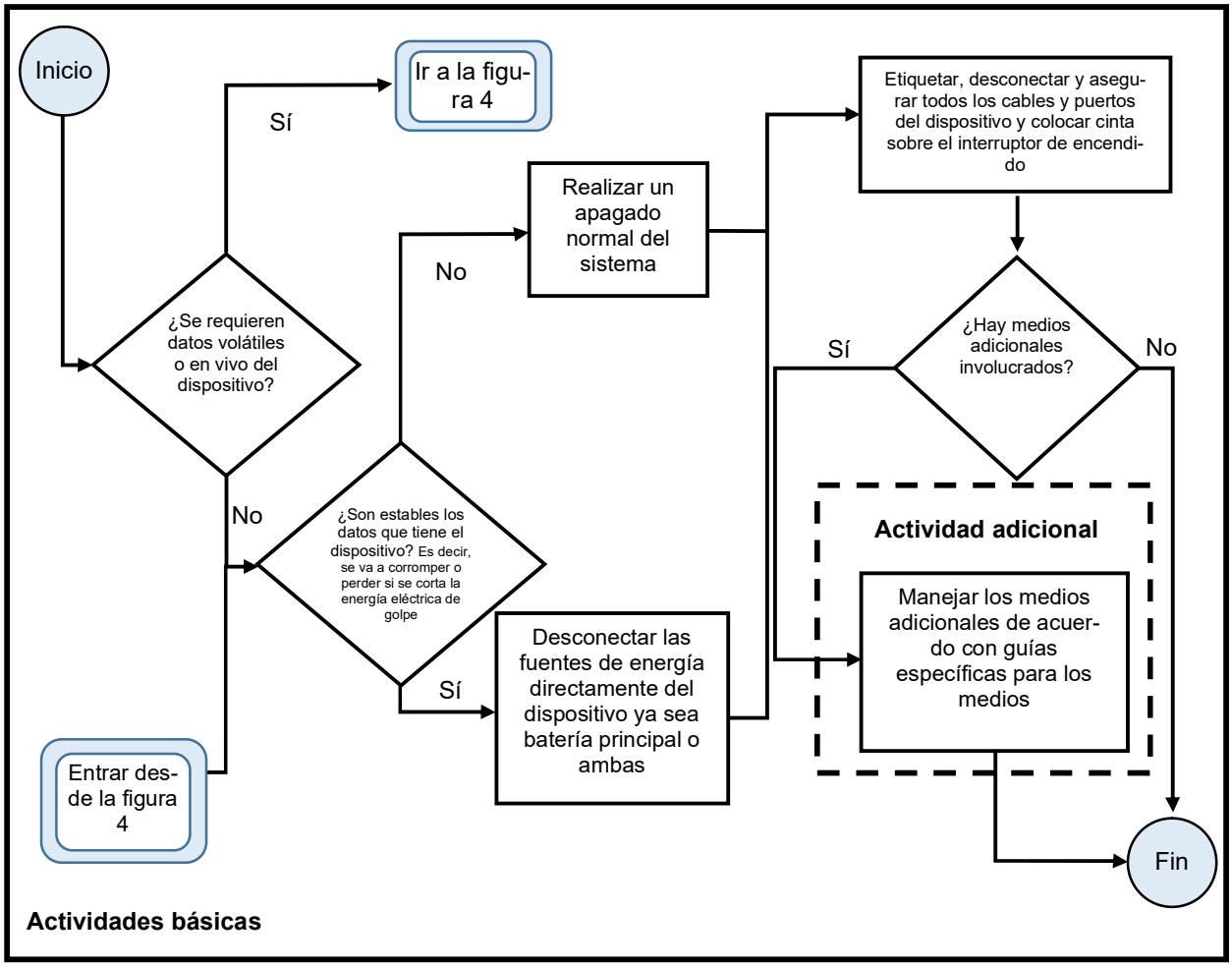

Figura 2 - Guía para la recolección de dispositivos digitales encendidos

7.1.2.1.2 Actividades básicas: recolección de dispositivo digital encendido

Se recomienda que el PIED siga las actividades básicas siguientes en todos los casos que involucren potencial evidencia digital. Estas guías se aplican cuando el PIED ha decidido que es recomendable hacer la recolección de un dispositivo digital que se encuentra encendido:

- considerar una adquisición de los datos volátiles y del estado actual del dispositivo digital antes de apagar el sistema. Es posible que las claves de cifrado y otros datos cruciales residan en la memoria activa, o en la memoria inactiva que aún no ha sido borrada. Cuando se sospecha que la información está cifrada, considerar la adquisición lógica. Cuando este sea el caso, tener en mente que el sistema operativo del equipo bajo estudio puede no ser confiable, por lo tanto, considerar el uso de herramientas apropiadas fiables y validadas;

- la configuración del dispositivo digital puede determinar si el PIED necesita apagar el dispositivo por medio de procedimientos administrativos normales, o si se recomienda desconectar el cable de suministro de energía eléctrica del tomacorriente. El PIED puede necesitar consultar a un EED para determinar la mejor alternativa ante circunstancias específicas. Si se toma la decisión de

desconectar el cable de alimentación eléctrica, el PIED necesita desenchufar el cable de suministro de energía eléctrica desconectando en primer lugar el extremo conectado al dispositivo digital y no el extremo conectado al tomacorriente. Tener en cuenta que si el dispositivo está conectado a una UPS y el cable de suministro de energía eléctrica se desenchufa primero de la pared y no del dispositivo, los datos pueden alterarse;

NOTA 1. Si se desconecta el cable de suministro de energía eléctrica de un dispositivo digital que se encuentra encendido, toda potencial evidencia digital almacenada en volúmenes cifrados va a resultar inaccesible, a menos que se obtenga la clave de descifrado. Potencialmente se podrían también perder datos vivos valiosos, lo cual puede resultar en demandas por daños y perjuicios o la pérdida de vidas humanas, como datos corporativos o dispositivos digitales que controlan equipamiento médico. Por lo tanto, se recomienda que el PIED garantice recolectar los datos volátiles antes de desconectar el suministro de energía eléctrica.

NOTA 2. Hay dispositivos de hardware que permiten que un dispositivo que se encuentra encendido se desconecte del suministro de energía eléctrica de la red y se transfiriera a una UPS portátil sin interrumpir la energía eléctrica al dispositivo. También hay dispositivos que simulan la actividad del "*mouse"* ("*mouse-jigglers*") que se pueden usar para evitar que se active el protector de pantalla. Ambos dispositivos resultan herramientas útiles cuando se está tratando con un dispositivo que se halla encendido en el cual el cifrado puede estar activado. Cuando se realiza la recolección de un dispositivo encendido en el que se va a mantener la energía eléctrica, hay ciertos temas asociados a un sistema en ejecución que el embalaje y el transporte tienen que abordar tales como la provisión de refrigeración, la protección mecánica contra golpes, etc.

- etiquetar, desconectar y asegurar todos los cables desde el dispositivo digital y etiquetar los puertos de forma tal que el sistema se pueda reconstruir en una etapa posterior;

- colocar cinta sobre el interruptor de encendido, si es necesario, para evitar que el interruptor cambie de estado. Considerar si el estado del interruptor de encendido se ha documentado apropiadamente antes de encintarlo o moverlo.

7.1.2.1.3 Actividades adicionales: recolección de dispositivo digital encendido

La siguientes son actividades adicionales cuya pertinencia depende de la configuración del dispositivo digital específico.

- Si se trata de una computadora portátil, garantizar la adquisición de los datos volátiles antes de quitar la batería. Se recomienda que el PIED quite la batería, suministro de energía eléctrica principal, en primer lugar, en vez de presionar el botón de encendido de la computadora portátil para apagarla. Se recomienda que el PIED también tenga en cuenta si hay una fuente de energía eléctrica y si la hay, desconectar la fuente después de haber quitado la batería.

  NOTA 1. La acción de presionar el botón de encendido en un dispositivo digital puede ser configurada para iniciar una rutina que altere la información o borre información del sistema antes de apagarse o alerte a sistemas conectados que ha ocurrido un evento inesperado de forma que les permita borrar datos con valor probatorio antes de que se los identifique. También puede estar configurado para disparar un dispositivo pensado para causar daño físico al PIED y a otras personas presentes.

- Si se encuentra presente una ranura para disquetes, encintarla.

- Asegurarse que las bandejas de las unidades de CD o DVD estén retraídas correctamente; registrar si las bandejas de estas unidades se encuentran vacías, contienen discos o no fueron revisadas y encintar la ranura de la unidad cerrada para evitar que se abra.

NOTA 2. Si se deja dentro cualquier medio de arranque de sistema, la próxima vez que la máquina sea encendida, podría arrancar desde ese medio en vez del disco rígido (o herramientas forenses en dispositivo de memoria *flash*) dependiendo de la configuración de la BIOS de la computadora.

Se recomienda que el PIED conduzca la recolección de evidencia no digital de acuerdo con los códigos de procedimiento legales para garantizar que toda la evidencia sea admisible.

7. 1.2.2 Dispositivos digitales apagados

7.1.2.2.1 Generalidades

El PIED puede seguir varias guías para la recolección cuando el dispositivo digital se encuentra apagado. No todas las actividades contenidas en estas guías son pertinentes en todas las circunstancias. En consecuencia, se debe hacer una distinción entre aquellas actividades que se aplican para todos los casos (actividades básicas) y aquellas que pueden aplicar solamente en algunos casos (actividades adicionales). La Figura 3 ilustra las actividades básicas y las adicionales aplicables a la recolección de un dispositivo digital apagado.

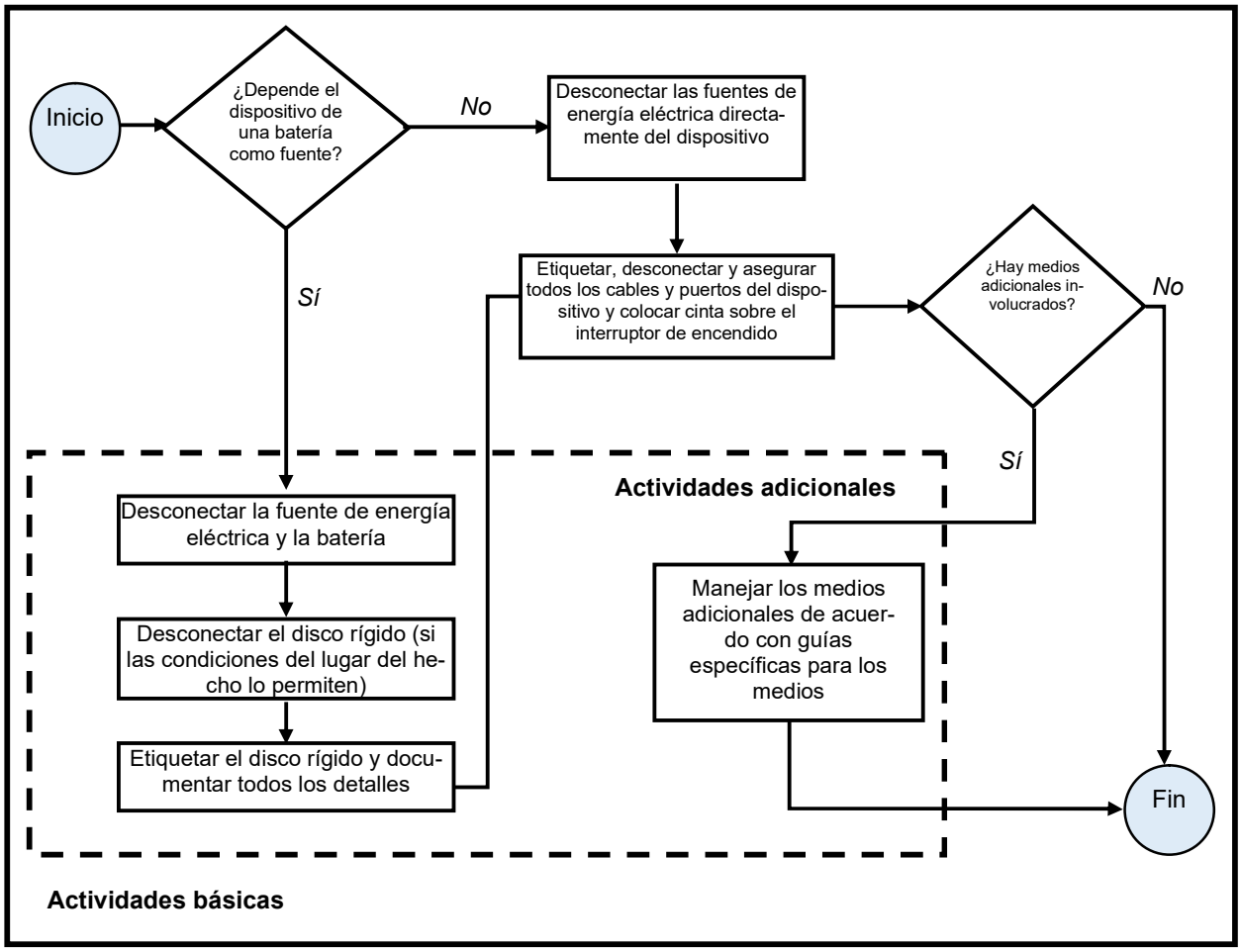

Figura 3 - Guías para la recolección de dispositivos digitales apagados

Es responsabilidad del PIED conocer la tecnología actual y estar familiarizado con las guías para el manejo de medios de almacenamiento.

7.1.2.2.2 Actividades básicas: recolección de dispositivo digital apagado

Las actividades básicas para la recolección cuando el dispositivo digital está apagado son las siguientes:

- desconectar el cable de suministro de energía eléctrica desconectando primero el extremo conectado al dispositivo digital y no el extremo conectado al tomacorriente;

– desconectar y asegurar todos los cables de los dispositivos digitales y etiquetar los puertos para que el sistema se pueda reconstruir en una etapa posterior;

– de ser necesario para evitar el cambio de estado, encintar el interruptor de encendido. Considerar si el estado del interruptor de encendido ha sido apropiadamente documentado antes de encintarlo o moverlo.

NOTA. En la mayoría de los casos, se recomienda no retirar el medio de almacenamiento del dispositivo digital hasta el momento en que se realice la adquisición ya que retirarlo incrementa el riesgo de dañarlo o confundirlo con otro medio de almacenamiento. Se recomienda desarrollar y seguir procedimientos locales sobre la necesidad de retirar medios de almacenamiento de los dispositivos digitales.

7.1.2.2.3 Actividades adicionales: recolección de dispositivo digital apagado

Dependiendo de la configuración del dispositivo digital específico, las actividades adicionales que son pertinentes a la recolección de dispositivos digitales apagados son las siguientes:

– primero, garantizar que la computadora portátil esté realmente apagada ya que alguna puede estar en modo de espera. Considerar que algunas computadoras portátiles se pueden encender abriendo la tapa. Luego proceder a quitar la batería de suministro de energía eléctrica principal de la computadora portátil;

– si las condiciones en el lugar requieren que el disco rígido se retire, se recomienda que el PIED conecte a tierra al dispositivo digital para evitar que la electricidad estática dañe el disco rígido. Caso contrario, no se recomienda retirar el disco rígido en el lugar. Etiquetar el disco rígido como disco dubitado y documentar todos los detalles como marca, nombre del modelo, número de serie y capacidad del disco rígido;

– si se encuentra presente una ranura para disquetes, encintarla;

– asegurarse que las bandejas de las unidades de CD o DVD estén retraídas correctamente; registrar si las bandejas de estas unidades se encuentran vacías, contienen discos, o no fueron revisadas y encintar la ranura de la unidad cerrada para evitar que se abra.

NOTA. Si se deja dentro cualquier medio de arranque de sistema, la próxima vez que la máquina sea encendida, podría arrancar desde ese medio en vez del disco rígido (o herramientas forenses en dispositivos de memoria *flash*) dependiendo de la configuración de la BIOS de la computadora.

7.1.3 Adquisición

7.1.3.1 Dispositivos digitales encendidos

7.1.3.1.1 Generalidades

Existen tres escenarios en los cuales puede ser necesario realizar una adquisición: cuando los dispositivos digitales están encendidos, cuando los dispositivos digitales están apagados y cuando los dispositivos digitales están encendidos, pero no pueden ser apagados (como dispositivos digitales de misión crítica). En todos estos escenarios se requiere que el PIED realice una copia forense exacta de los medios de almacenamiento de los dispositivos digitales que se sospecha puedan contener potencial evidencia digital.

Si no se puede obtener una imagen, se pueden adquirir copias exactas de archivos específicos que se sospecha que contienen potencial evidencia digital. Idealmente se recomienda producir tanto una copia maestra verificada, como también copias de trabajo. No se recomienda volver a utilizar la copia maestra a menos que sea necesario para verificar el contenido de una copia de trabajo o para producir un reemplazo de la copia de trabajo luego de un daño a la primera copia.

El PIED puede seguir varias guías para la adquisición cuando el dispositivo digital se halla encendido. No todas las guías son ideales y apropiadas para todos los casos; algunas guías son solo pertinentes en casos específicos. En consecuencia, las guías se pueden categorizar como básicas o adicionales. Se recomienda considerar la posibilidad de que un sistema encendido pueda entrar en modo protector de pantalla o auto bloquearse y que cualquier esfuerzo realizado para prevenirlo tiene implicancias. Por ejemplo, el uso de un dispositivo que simula la actividad del "*mouse*" ("*mouse-jiggler*") va a generar una entrada de una clave USB en el registro y modificaciones que muy probablemente van a ocurrir sin importar las acciones tomadas. Se recomienda utilizar métodos confiables para minimizar las implicancias de dichas acciones. La figura 4 ilustra las actividades básicas y adicionales aplicables a la adquisición de dispositivos digitales encendidos.

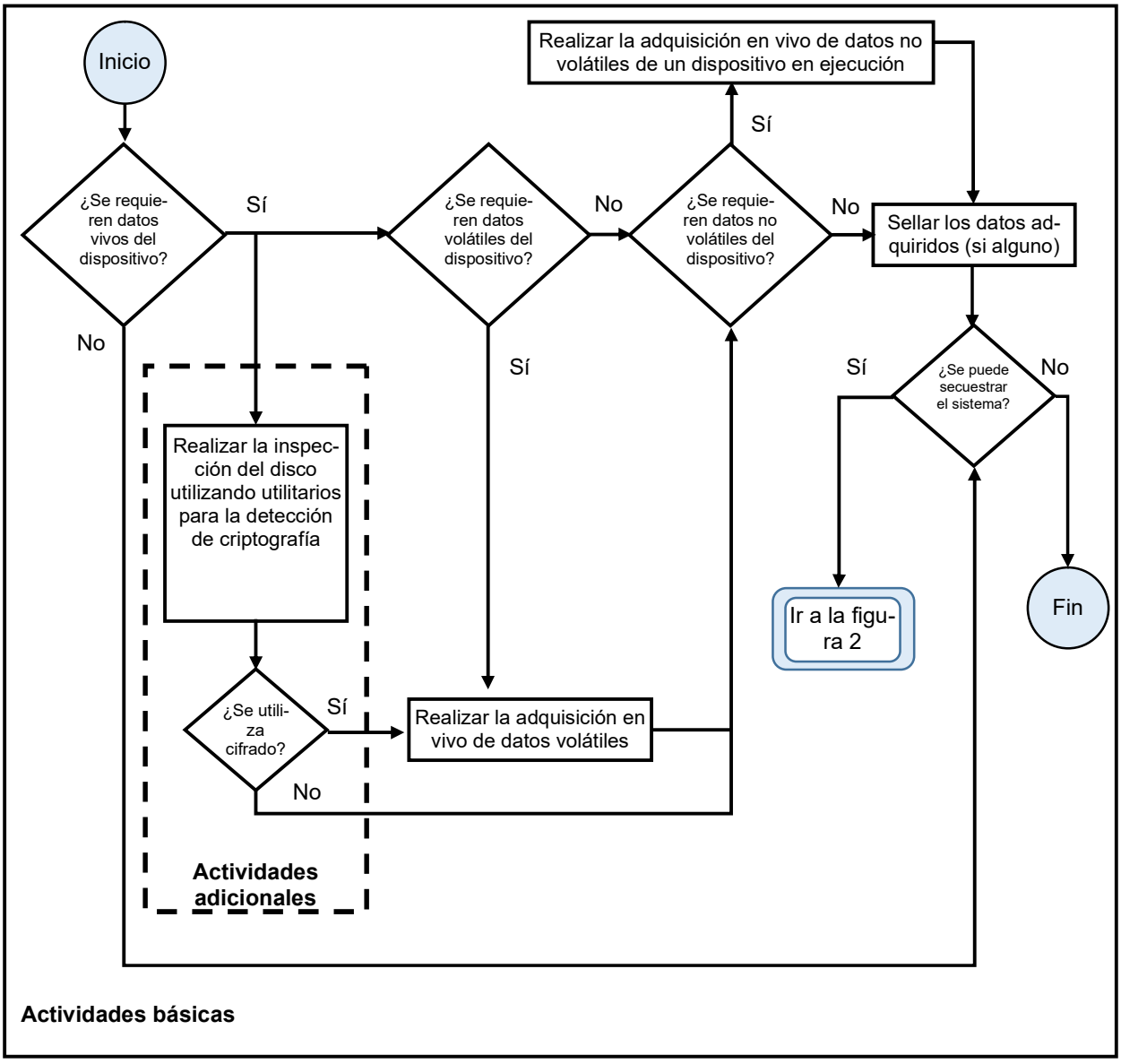

Figura 4 - Guía para la adquisición de un dispositivo digital encendido

7.1.3.1.2 Actividades básicas: adquisición de dispositivo digital encendido

Se recomienda que el PIED en todos los casos que involucren la adquisición de potencial evidencia digital de dispositivos digitales encendidos siga las actividades básicas siguientes:

- primero considere adquirir la potencial evidencia digital que de otra forma pueda perderse si el dispositivo digital se apaga. Esto también se conoce como datos volátiles tales como datos almacenados en RAM, procesos en ejecución, conexiones de red y configuraciones de fecha y hora. En circunstancias en las que es necesario adquirir datos no volátiles de dispositivos que continúan en ejecución, se recomienda considerar la adquisición sobre un sistema encendido;

- para adquirir datos de dispositivos que continúan en ejecución es necesario realizar una adquisición en vivo. La adquisición en vivo de datos volátiles en RAM puede permitir la recuperación de información valiosa como por ejemplo el estado de la red, las aplicaciones y las contraseñas descifradas. La adquisición en vivo se puede realizar desde la consola o desde la red en forma remota. Los procesos son diferentes y requieren el uso de diferentes conjuntos de herramientas;

- se recomienda que el PIED nunca confíe en los programas de los sistemas dubitados. Por esta razón, se recomienda, siempre que sea posible, el uso de herramientas confiables obtenidas por el PIED (binarios estáticos). Se recomienda que el PIED sea competente en el uso de herramientas validadas y sea competente para responder por los efectos que dichas herramientas pueden tener sobre el sistema (por ejemplo, el desplazamiento de potencial evidencia digital, que el contenido de la memoria quede fuera del paginado cuando se cargan las herramientas de software, etc.). Se recomienda que todas las acciones realizadas y los cambios resultantes sobre la potencial evidencia digital se documenten y comprendan. También se recomienda documentar si no es posible determinar el efecto probable de la introducción de las herramientas en el sistema o si no se pueden determinar con certeza los cambios resultantes;

- cuando adquiere datos volátiles se recomienda que el PIED adopte el uso de un contenedor lógico de archivos cuando sea posible y documente su valor del digesto matemático una vez que contenga los archivos de datos volátiles. Cuando esto no sea posible, se recomienda usar un contenedor, tal como un archivo ZIP y luego se recomienda calcular el digesto matemático de este archivo y documentar su valor. Se recomienda almacenar el contenedor de archivos resultante en un medio de almacenamiento digital que haya sido preparado para este propósito, es decir, formateado;

- realice el proceso de obtención de una copia forense sobre un almacenamiento no volátil en vivo utilizando una herramienta validada para la obtención de una copia forense. Se recomienda que la copia forense resultante se almacene en un medio de almacenamiento digital que haya sido preparado para este propósito. Aunque es preferible el uso de un medio de almacenamiento digital nuevo, el uso de copias forenses obtenidas utilizando procesos validados garantiza la integridad de los datos cuando se los reconstruye. Por lo tanto, es suficiente un medio almacenamiento digital que se haya borrado de manera segura. Si la imagen tiene que almacenarse en un contenedor lógico de archivos, se recomienda que el PIED garantice que la imagen no se pueda corromper ni dañar.

NOTA. En situaciones en las cuales el dispositivo esté bloqueado se permite realizar el acceso físico a través de otros medios que tengan habilitado el acceso directo a la memoria, por ejemplo, interfaces FireWire.

7.1.3.1.3 Actividades adicionales: adquisición de dispositivo digital encendido

Dependiendo de la configuración del dispositivo digital específico, las actividades adicionales que son pertinentes a la adquisición de dispositivos digitales encendidos son las siguientes:

- considerar la adquisición de datos volátiles en la RAM cuando se sospecha el uso de cifrado. Primero comprobar si este puede ser el caso inspeccionando el disco en crudo o utilizando alguna utilidad de detección de cifrado. Cuando así sea, tener en cuenta que el sistema operativo del dis-

positivo en vivo puede no ser confiable y considerar el uso de herramientas apropiadas confiables y validadas;

- usar una fuente confiable de fecha y hora y documentar la fecha y hora de cada acción realizada;

- puede ser apropiado asociar al PIED con la potencial evidencia digital adquirida utilizando firma digital, biometría y fotografía.

NOTA. La acción de presionar el botón de encendido en un dispositivo digital puede ser configurada para iniciar una rutina que altere la información o borre información del sistema antes de apagarse o alerte a sistemas conectados que ha ocurrido un evento inesperado de forma que les permita borrar datos con valor probatorio antes de que se los identifique. También puede estar configurado para disparar un dispositivo pensado para causar daño físico al PIED y a otras personas presentes.

7.1.3.2 Dispositivos digitales apagados

7.1.3.2.1 Generalidades

Es más fácil manejar un dispositivo digital apagado comparado con un dispositivo digital encendido porque no hay necesidad de adquirir datos volátiles. La figura 5 ilustra las actividades que son aplicables a la adquisición de los dispositivos digitales apagados.

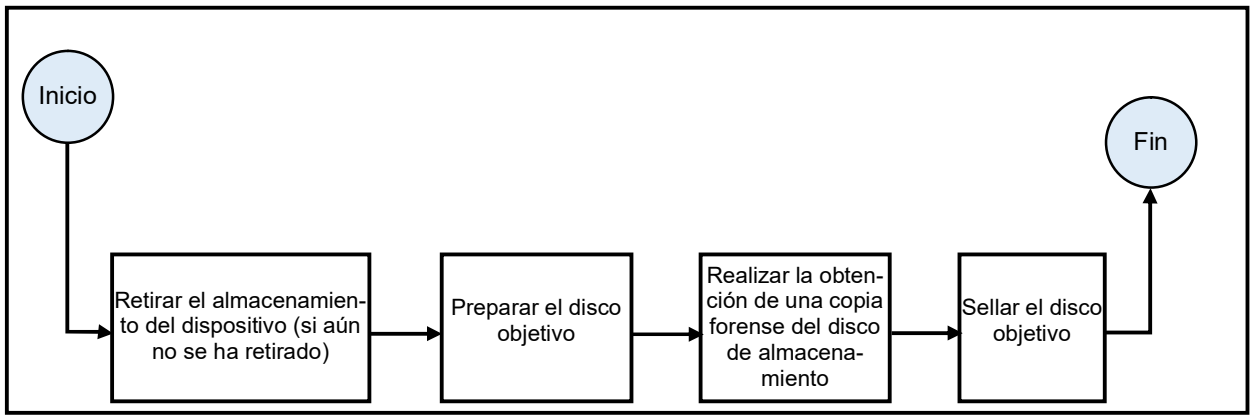

Figura 5 - Guías para la adquisición de un dispositivo digital apagado

7.1.3.2.2 Adquisición de dispositivos digitales apagados

Las actividades para la adquisición cuando el dispositivo digital se encuentra apagado son las siguientes:

- garantizar que el dispositivo esté realmente apagado;

- si resulta apropiado, retirar el medio de almacenamiento del dispositivo digital apagado si todavía no ha sido retirado. Etiquetar el almacenamiento como almacenamiento dubitado y documentar todos los detalles, tales como marca, nombre de modelo, número de serie y capacidad del almacenamiento;

- realizar el proceso de obtención de una copia forense usando una herramienta validada para ese fin para crear una copia forense del disco dubitado.

NOTA. En la mayoría de los casos, se recomienda no retirar el medio de almacenamiento del dispositivo digital hasta el momento en que vaya a realizarse la adquisición ya que retirarlo incrementa el riesgo de dañarlo o confundirlo con otro medio de almacenamiento. Se recomienda desarrollar y seguir procedimientos locales sobre la necesidad de retirar medios de almacenamiento.

7.1.3.3 Dispositivos digitales de misión-crítica

En algunos casos, los dispositivos digitales no se pueden apagar debido a la naturaleza crítica de los sistemas. Estos sistemas, tales como servidores en centros de cómputos que pueden estar prestando servicio a terceras partes no involucradas, sistemas de vigilancia, sistemas médicos y muchos otros pueden ser afectados críticamente si se los interrumpe o apaga. Se recomienda tener cuidados especiales cuando se esté tratando con estos sistemas.

Cuando un dispositivo digital no se puede apagar, realizar una adquisición en vivo y/o parcial según lo indicado en 7.1.3.1.2 y 7.1.3.4.

7.1.3.4 Adquisición parcial

Varias razones permiten que se realice una adquisición parcial, tales como:

- que el sistema de almacenamiento sea demasiado grande para adquirirlo (por ejemplo, servidor de base de datos);
- un sistema es demasiado crítico para apagarlo;
- cuando solo los datos seleccionados para la adquisición contienen otros datos no pertinentes dentro del mismo sistema; o
- cuando exista una restricción por parte de una autoridad legal tal como una orden de allanamiento que limite el alcance de la adquisición.

Cuando se haya tomado la decisión de realizar una adquisición parcial, se recomienda que las actividades para la adquisición incluyan, pero no se limiten a lo siguiente:

- identificar las carpetas, los archivos o las opciones pertinentes del sistema propietario disponibles para adquirir los datos deseados;
- conducir una adquisición lógica sobre aquellos datos identificados.

7.1.3.5 Medios de almacenamiento digital

Se pueden encontrar distintos tipos de medios de almacenamiento digital en un lugar del incidente. Generalmente estos tienen el tipo de datos menos volátiles y pueden tener la prioridad más baja durante la recolección y la adquisición. Esto no significa que no sean importantes porque en muchos casos, los medios de almacenamiento digital externos contienen la evidencia que los analistas están buscando. El PIED necesita garantizar lo siguiente:

- comprobar y documentar la ubicación (por ejemplo, bahía de disco, cable y conector, ranura USB, etc.), marca, modelo y número de serie (si se encuentran) de cada medio de almacenamiento digital hallado;
- decidir si recolecta el medio de almacenamiento digital identificado o si realiza una adquisición en el lugar; se sugiere que la decisión esté basada en la naturaleza del incidente y los recursos disponibles. Para poder conducir una adquisición en el lugar del medio de almacenamiento digital (disco rígido primario), ver la Figura 4;
- si el PIED lo decide y se le permite recolectar un medio de almacenamiento digital, se recomienda envolver el medio recolectado o colocarlo en un embalaje apropiado;
- etiquetar todos los medios de almacenamiento digital y todas las partes asociadas con ellos. Se recomienda que las etiquetas de evidencias no se coloquen directamente sobre partes mecánicas

de los medios digitales, ni que cubran u oculten información importante como número de serie, número de modelo y número de parte. Se recomienda que todos los medios recolectados se adquieran y almacenen de forma tal que se pueda garantizar la integridad de los medios recolectados. Se recomienda que, cuando sea posible, la evidencia se selle con un sello que haga evidente cualquier adulteración intencional y también se recomienda que el PIED o el personal a cargo firme sobre la etiqueta;

- se recomienda almacenar el medio de almacenamiento digital recolectado en un entorno apto para la preservación de los datos;

- diferentes medios de almacenamiento digital tienen diferente capacidad de conservación de datos. Se recomienda que el PIED sea consciente del tiempo máximo aceptable especificado por la jurisdicción pertinente, con respecto a la capacidad de conservación de datos del medio de almacenamiento digital.

7.1.4 Preservación

Luego del proceso de adquisición, se recomienda que el PIED selle los datos adquiridos usando funciones de verificación o firmas digitales para determinar que las copias forenses sean equivalentes a los originales. Adicionalmente, los aspectos de seguridad requieren controles que aplican los principios de la preservación de la confidencialidad, la integridad y la disponibilidad de la potencial evidencia digital. Para poder proteger contra la adulteración, se recomienda tratar los aspectos del entorno con las medidas apropiadas. El PIED necesita garantizar lo siguiente:

- usar una función de verificación apropiada para proveer evidencia de que los archivos copiados son equivalentes a los originales;

- puede ser apropiado asociar al PIED con la potencial evidencia digital adquirida, usando firmas digitales, biometría y fotografía.

Se necesita preservar apropiadamente todos los dispositivos digitales que fueron recolectados. Diferentes tipos de dispositivos digitales pueden requerir diferentes métodos de preservación. La potencial evidencia digital se necesita preservar a lo largo de su ciclo de vida, que puede variar según la jurisdicción y las políticas de las organizaciones.

NOTA. Como una alternativa al sellado de los datos adquiridos con funciones de verificación o firmas digitales, el PIED puede también usar características biométricas. La biometría utiliza características físicas y del comportamiento para determinar la identidad de una persona. Adjuntando una característica biométrica a la evidencia adquirida, se puede garantizar que la evidencia no pueda ser adulterada intencionalmente sin comprometer la característica biométrica.

7.2 Dispositivos en red

7.2.1 Identificación

7.2.1.1 Generalidades

En el contexto de este capítulo, los dispositivos en red se consideran como las computadoras u otros dispositivos digitales que están conectados a una red ya sea cableada o inalámbrica. Estos dispositivos en red pueden incluir unidades centrales (“*mainframes*”), servidores, computadoras de escritorio, puntos de acceso, conmutadores (“*switches*”), concentradores (“*hubs*”), enrutadores, dispositivos móviles, PDA, PED, dispositivos Bluetooth, sistemas de CCTV y muchos más. Cabe destacar que, si un dispositivo digital está en red, es difícil cerciorarse dónde está almacenada la potencial evidencia digital que se busca. Los datos pueden estar ubicados en cualquier parte de la red.

La identificación de un dispositivo digital incluye los componentes como los logos del fabricante, los números de serie, bases de carga y fuentes de energía eléctrica. El PIED puede considerar los aspectos siguientes como formas de identificación:

- características del dispositivo: la marca y el fabricante de un dispositivo digital a veces se puede identificar por sus características observables, particularmente si existen elementos de diseño únicos;

- interfaz del dispositivo: el conector de energía eléctrica suele ser especifico de un fabricante y es una ayuda confiable para la identificación;

- etiqueta del dispositivo: para dispositivos móviles apagados, se obtiene información reveladora dentro de la cavidad que contiene la batería, particularmente cuando se constata con una base de datos apropiada. Por ejemplo, el IMEI es un número de 15 dígitos que indica el fabricante, el tipo de modelo y el país de aprobación para dispositivos GSM; el ESN es un identificador único de 32 bits documentado dentro de un chip seguro en un teléfono móvil por su fabricante - los primeros 8 a 14 bits identifican el fabricante y los bits restantes identifican el número de serie asignado;

- búsqueda inversa: en el caso de teléfonos móviles, si se conoce el número telefónico del teléfono, se puede utilizar una búsqueda inversa para identificar al operador de red.

Debido a que generalmente los dispositivos móviles son de pequeño tamaño, el PIED necesita tener cuidados adicionales para identificar todos los tipos de dispositivos móviles que pueden ser pertinentes al caso. El PIED necesita asegurar el supuesto lugar del incidente y garantizar que ninguna persona pueda trasladar del lugar del hecho dispositivos móviles o cualquier otro tipo de dispositivos digitales. Se recomienda proteger a los dispositivos digitales que pueden contener evidencia digital de accesos no autorizados.

NOTA. En algunos casos, se recomienda no interrumpir la comunicación (por ejemplo, para no advertir a personas desconocidas que se apagó un dispositivo) e informar a las personas autorizadas sobre posibles consecuencias.

7.2.1.2 Búsqueda y documentación del lugar físico del incidente

Antes de realizar cualquier adquisición o recolección, se recomienda documentar al lugar del incidente de manera visual con fotografías, filmaciones de video o bocetos del lugar del hecho tal como se encuentra al ingreso. La elección del método de documentación necesita sopesar las circunstancias, el costo, el tiempo, la disponibilidad de recursos y las prioridades. Se recomienda que el PIED documente todos los otros elementos en el lugar del hecho que puedan contener materiales de potencial pertinencia como notas escritas, notas adhesivas, diarios, etc.

- Se recomienda que el PIED documente el tipo, la marca, el modelo y los números de serie de cualquier dispositivo digital usado e identifique todos los dispositivos digitales que puede ser necesario adquirir o recolectar durante esta etapa inicial. Se recomienda documentar y recolectar todos los dispositivos móviles y sus elementos asociados, tales como tarjetas de memoria, tarjetas SIM, cargadores y bases de carga encontrados en el lugar del hecho, sus números de serie asociados y cualquier característica de identificación, si es requerido. También tratar de encontrar el embalaje original de los teléfonos móviles; este puede contener notas como códigos de PIN y PUK.

- Si el dispositivo está conectado a una red, se recomienda que el PIED identifique los servicios prestados por el dispositivo para comprender dependencias y confirme la criticidad del dispositivo dentro de la red antes de decidir si se lo desconecta de la red. Esto es importante si el dispositivo está brindando funciones de misión-critica que no pueden tolerar ninguna baja o para evitar la destrucción de potencial evidencia digital. Sin embargo, si parece haber amenazas constantes basadas en red a los dispositivos, el PIED puede tener que decidir desconectar el dispositivo de la red para proteger la potencial evidencia digital.

- Si el dispositivo en red es un sistema de CCTV, se recomienda que el PIED tome nota del número de cámaras conectadas al sistema, así como también cuáles son las cámaras que están activamente funcionando. Se recomienda que el PIED también tome nota de la marca, el modelo y la configuración básica del sistema, tal como la configuración de la pantalla, la configuración actual de las grabaciones y la ubicación del almacenamiento de manera tal que, si tienen que realizarse cambios para facilitar el proceso de recolección y adquisición, luego sea posible retornar el sistema a su estado original.

- Tanto como sea posible, se recomienda que el estado de los dispositivos digitales se mantenga como está. Generalmente, si el dispositivo digital se encuentra apagado, se recomienda que el PIED no lo encienda y si se encuentra encendido, se recomienda que el PIED no lo apague. Esto previene innecesaria adulteración de la potencial evidencia digital. Un dispositivo que tiene batería que se puede agotar, necesita ser recargado para garantizar que no se pierda información. En esta fase el PIED necesita identificar potenciales medios de carga y cables. Si se va a transportar un dispositivo y se lo va a examinar en una fecha indeterminada, puede ser apropiado apagarlo para minimizar el potencial daño a los datos almacenados en el dispositivo.

- Se recomienda que el PIED también considere el uso de un detector de señales inalámbricas para detectar e identificar una señal inalámbrica de algún dispositivo inalámbrico que puede estar oculto. Puede haber instancias en las cuales los detectores de señales inalámbricas no se utilicen debido a las restricciones de costo y tiempo y se recomienda que el PIED lo documente.

7.2.2 Recolección, adquisición y preservación

7.2.2.1 Generalidades

El PIED necesita decidir si va a recolectar o adquirir la potencial evidencia digital de los dispositivos digitales. La decisión necesita sopesar las circunstancias, los costos, el tiempo, la disponibilidad de recursos y las prioridades.

Si el PIED decide desconectar los dispositivos, el proceso de recolección o adquisición de la potencial evidencia digital procede como se indica en 5.4. En el caso de que el dispositivo no pueda ser desconectado de la red debido a la criticidad de su función o la probabilidad de destrucción de potencial evidencia digital, se recomienda que el PIED realice una adquisición en vivo mientras el dispositivo permanece conectado a la red.

NOTA. Es crítico contar con procedimientos normalizados y robustos que empleen herramientas validadas, acompañados de una buena documentación y un PIED capacitado y experimentado.

La recolección y la adquisición de potencial evidencia digital de dispositivos móviles conectados a una red son complejas porque pueden existir en múltiples estados y modos de interacción, tales como Bluetooth, frecuencia de radio, pantalla táctil e infrarrojo. Además, diferentes fabricantes de dispositivos móviles utilizan diferentes tipos de sistemas operativos, lo cual requiere diferentes métodos de adquisición de la evidencia. También existe una amplia gama de tarjetas de memoria que se utilizan con dispositivos móviles y retirar estas tarjetas de memoria de un dispositivo móvil encendido puede interferir con los procesos en ejecución.

Generalmente, los dispositivos móviles como PDA y teléfonos móviles necesitan estar encendidos para la adquisición de la potencial evidencia digital. Estos dispositivos pueden constantemente alterar su entorno operativo mientras están encendidos, por ejemplo, el tiempo del reloj se puede actualizar. El problema asociado es que, para dos copias forenses del mismo dispositivo, las funciones de verificación normalizadas como el digesto matemático pueden arrojar distintos resultados. En esta situación, puede ser apropiado el uso de funciones de verificación alternativas para identificar áreas comunes y/o diferentes.

Es importante que el PIED no introduzca dispositivos Wi-Fi o Bluetooth al lugar del hecho que pudiera modificar la información de los potenciales dispositivos que contengan evidencia. Esto es particularmente importante si el investigador necesita conocer qué dispositivos han sido conectados.

Si el PIED decide seguir el proceso de adquisición, se recomienda mantener a los dispositivos de red en ejecución para el análisis posterior para confirmar los otros dispositivos conectados a los dispositivos de red. Se recomienda que el PIED considere la posibilidad de sabotaje por el sospechoso a través de una conexión de red activa y decida si monitorea el sistema o lo desconecta.

7.2.2.2 Guía para recolección de dispositivos en red

En algunas circunstancias, puede ser apropiado dejar dispositivos conectados a la red para que el PIED y/o EED con autoridad apropiada puedan monitorear y documentar su actividad. Cuando esto no es necesario, se recomienda recolectar los dispositivos como se describe a continuación:

- se recomienda que el PIED aísle el dispositivo de la red cuando esté seguro de que esta acción no va a sobrescribir datos pertinentes y no van a ocurrir malfuncionamientos en sistemas importantes (como, por ejemplo, sistemas de gestión de instalaciones en hospitales). Esto se puede realizar desconectando las conexiones de red cableada al sistema telefónico o al puerto de red, o deshabilitando las conexiones al punto de acceso inalámbrico;

- antes de la desconexión de la red cableada, se recomienda que el PIED rastree las conexiones de los dispositivos digitales y etiquete los puertos para futuras reconstrucciones de toda la red. Un dispositivo puede tener más de un método de comunicación. Por ejemplo, una computadora puede tener LAN cableada, un modem inalámbrico y tarjetas de telefonía móvil. Los PED también pueden estar conectados a la red vía conexiones Wi-Fi, Bluetooth o conexiones a la red de telefonía móvil. Se recomienda que el PIED intente identificar todos los métodos de comunicaciones y realice las actividades apropiadas para proteger a la potencial evidencia digital de su destrucción;

- ser consciente de que desconectar la energía eléctrica de los dispositivos en red en ese momento puede destruir datos volátiles tales como procesos en ejecución, conexiones de red y datos almacenados en memoria. El sistema operativo anfitrión puede no ser confiable y reportar información falsa. Se recomienda que el PIED capture esta información utilizando métodos confiables verificados antes de desconectar a los dispositivos de la energía eléctrica. Una vez que el PIED está seguro de que la potencial evidencia digital no se va a perder como resultado, se pueden desconectar los dispositivos digitales;

- si la recolección precede a la adquisición y se sabe que el dispositivo contiene memoria volátil, se recomienda conectar de manera continua al dispositivo a una fuente de energía eléctrica;

- si el dispositivo móvil está apagado, proceder a embalarlo, sellarlo y etiquetarlo cuidadosamente. Esto es para evitar cualquier operación accidental o deliberada de las teclas o botones. Como precaución, se recomienda que el PIED considere el uso de cajas blindadas de radiaciones electromagnéticas o de Faraday;

- en algunas circunstancias, se recomienda apagar los dispositivos móviles durante la recolección para prevenir que se modifiquen los datos. Esto puede suceder a través de conexiones salientes o entrantes o comandos que pueden causar la destrucción de la potencial evidencia digital;

- subsiguientemente, cada dispositivo digital puede tratarse como si fuera un dispositivo no conectado (ver 7.1) hasta que se lo examine. Durante el examen, se recomienda considerarlo como un dispositivo en red.

NOTA. Es posible implementar un tipo de red utilizando dispositivos de almacenamiento removibles como medios de transmisión. Se recomienda que el PIED considere si los dispositivos recolectados pueden haber sido utilizados de esta forma y buscar información acerca de los otros dispositivos conectados a dicha red electrónica (“sneakernet”).

7.2.2.3 Guía para la adquisición de dispositivos en red

En la situación en la cual los dispositivos están conectados a una red, existe la posibilidad de que estén conectados a más de una (1) red física y/o virtual. Por ejemplo, un dispositivo que parece tener una (1) conexión de red física visible puede en realidad estar ejecutando una red privada virtual (VPN) y una máquina virtual con más de una (1) dirección IP. Como tal, antes de desconectar el dispositivo de la red, se recomienda que el PIED realice la adquisición lógica de los datos relacionados con las conexiones lógicas a la red (por ejemplo, conectividad a internet). Los datos relacionados incluyen, pero no se limitan a la configuración IP y las tablas de enrutamiento.

Para un dispositivo de red que necesita estar constantemente encendido, se recomienda prevenir que él interactúe con la red inalámbrica incluyendo dispositivos con GPS activo. Se recomienda que el PIED use métodos permitidos por la ley local para aislar señales de radio. Sin embargo, se recomienda tomar recaudos para garantizar que el dispositivo tenga una fuente de energía eléctrica adecuada, ya que los métodos de aislamiento pueden causar que utilice energía eléctrica adicional en un intento de contactar a la red. Los métodos de aislamiento pueden incluir, pero no se limitan a los siguientes:

- utilizar un dispositivo de interferencia que sea capaz de bloquear las transmisiones a través de la creación de una fuerte interferencia cuando el dispositivo emite señales en el mismo rango de frecuencia que utilizan los dispositivos móviles;

  NOTA 1. El uso de dispositivos de interferencia puede violar requisitos legales en algunas jurisdicciones.

  NOTA 2. El uso de dispositivos de interferencia puede afectar negativamente el comportamiento de los dispositivos electrónicos tales como equipamiento médico.

- utilizar un área de trabajo blindada de radiaciones electromagnéticas para realizar los exámenes de manera segura en una ubicación fija. El blindaje se puede hacer para toda el área de trabajo o a través de una jaula de Faraday que permita portabilidad. Sin embargo, introducir cables en la jaula es problemático ya que sin el aislamiento apropiado pueden comportarse como una antena, lo cual impide el propósito de la jaula. El espacio de trabajo también puede ser muy restrictivo;

- utilizar un área de trabajo blindada de radiaciones electromagnéticas para realizar los exámenes de manera segura en una ubicación fija. Se puede utilizar un área de trabajo blindada de radiofrecuencias o un contenedor (una jaula de Faraday) para prevenir conexiones a la red;

  NOTA 3 Se recomienda que todos los métodos de bloqueo del acceso inalámbrico a redes estén validados para el uso en la frecuencia apropiada. Se recomienda que esta validación se extienda a los cables que atraviesan el blindaje.

- utilizar una (U)SIM sustituta que imita la identidad del dispositivo original y previene que el dispositivo acceda a la red. Estas tarjetas permiten engañar al dispositivo para que las acepte como la (U)SIM original y permiten realizar exámenes de manera segura en cualquier ubicación. Se recomienda que la (U)SIM se valide para el dispositivo y la red antes de su uso;

- desactivar servicios de red mediante un acuerdo con el prestador de servicios de telefonía móvil e identificar detalles sobre los servicios a deshabilitar (por ejemplo, el identificador del equipamiento, el identificador del suscriptor o número de teléfono). Sin embargo, dicha información no siempre está fácilmente disponible cuando el proceso de coordinación y confirmación puede generar retraso.

El PIED puede realizar la adquisición en vivo de los dispositivos móviles antes de quitar la batería (por ejemplo, para acceder a la tarjeta SIM). Esto se puede realizar para prevenir la pérdida de potencial información importante en la RAM del teléfono o para acelerar el proceso de examen (por ejemplo, cuando se cree que el dispositivo puede estar protegido por PIN y/o PUK que puede tomar un tiempo significativo conseguirlos).

NOTA 4. Se recomienda que el PIED garantice que la recolección y la adquisición de la potencial evidencia digital se realizan de acuerdo con el marco normativo de la jurisdicción local, como requisito básico en circunstancias específicas.

7.2.2.4 Guía para la preservación de dispositivos en red

Debido a la naturaleza de los dispositivos digitales y la potencial evidencia digital, las guías para la preservación de dispositivos en red son similares a las de la preservación de computadoras, dispositivos periféricos y medios de almacenamiento digital. Ver 7.1.4 para la guía detallada sobre la preservación de dispositivos.

7.3 Recolección, adquisición y preservación de CCTV

Se recomienda que el PIED entienda que el enfoque para extraer secuencias de video de un sistema de CCTV DVR instalado en una computadora o embebido, es diferente a la extracción convencional de evidencia digital de una computadora. A continuación, se encuentran guías específicas para la adquisición de potencial evidencia digital de sistemas de CCTV:

- antes de comenzar el proceso de adquisición, se recomienda que el PIED primero determine si el sistema registró la secuencia de video de interés. Luego, se recomienda que el PIED determine el intervalo de tiempo de video requerido y compare la fecha y hora del sistema con la fecha y hora real y tome nota de cualquier diferencia. Asimismo, se recomienda que el PIED determine cuáles son las cámaras necesarias y si pueden adquirirse por separado. Se recomienda que el PIED tome nota de la marca y el modelo del sistema. Esta información puede ser necesaria para conseguir el software correcto de reproducción;

- se recomienda que el PIED adquiera todas las grabaciones de video pertinentes durante el tiempo de interés para preservar información adicional de la investigación que se puede desarrollar más adelante. Se recomienda que el PIED registre todas las cámaras conectadas a un sistema de CCTV y determine si están grabando activamente o no.

Se recomienda que el PIED determine la capacidad de almacenamiento del sistema de CCTV, al igual que cuándo está programado el sistema para sobrescribir la información del video. Esta información le permite al PIED conocer por cuánto tiempo se va a conservar la secuencia de video en el sistema antes de que se pierda. Se deben tomar acciones para garantizar que la evidencia no se modifique. Para la evidencia de video digital, se necesita establecer la protección contra escritura.

- Existen algunas opciones de las cuales el PIED puede elegir para adquirir potencial evidencia digital de los sistemas de CCTV:

  1) adquirir los archivos de video y grabarlos en un disco CD/DVD/Blu-ray, lo que puede no ser práctico si el archivo de video es muy grande;

  2) adquirir los archivos de video y grabarlos en un medio de almacenamiento externo;

  3) adquirir los archivos de video a través de una conexión de red. Esto puede estar disponible si el sistema de CCTV está equipado con un puerto de red;

  4) utilizar la función de exportación de los sistemas de CCTV a otros formatos de archivo (por lo general MPEG o AVI) lo que es una versión comprimida de las grabaciones de video. Esto solo se recomienda usarlo como última opción debido a que la recompresión de los videos altera los datos originales y siempre elimina los detalles de la imagen. No se recomienda confiar en datos recomprimidos para examinar si los datos originales existen y están disponible para su análisis;

     NOTA 1. La calidad de los videos exportados puede ser menor que la del video original.

  5) cuando no es posible adquirir directamente una copia forense de los archivos en el dispositivo de grabación, se recomienda que el PIED o EED intente adquirir una copia analógica desde la

salida analógica presente en el dispositivo de grabación original utilizando un adecuado dispositivo de grabación analógica.

- Al completar la adquisición, se recomienda comprobar el archivo adquirido para confirmar que se adquirió el archivo correcto o la porción correcta de éste. También se recomienda comprobar el archivo con el software de reproducción (para formatos de archivo de dispositivos digitales) para asegurar que se pueda reproducir en otros sistemas (la mayor parte de los sistemas de CCTV son propietarios y los archivos no necesariamente se pueden reproducir usando otro software de reproducción). El correcto software de reproducción puede estar disponible para descargar desde los sistemas de CCTV al mismo tiempo que los datos.

- Se recomienda tratar al medio de almacenamiento digital que contiene los archivos adquiridos como la copia forense maestra. Si el archivo se descargó a una computadora portátil, a una tarjeta de memoria o a un dispositivo USB, se recomienda realizar una copia maestra permanente a partir de estos lo antes posible.

- Se recomienda que el PIED luego reinicie el sistema de CCTV si estuviera apagado. Se recomienda realizar esto en presencia de una persona autorizada.

En las circunstancias en las cuales no fuera práctico realizar la adquisición en el lugar del hecho, el PIED puede tener que decidir recolectar el medio de almacenamiento digital. Un método rápido es el reemplazo del disco rígido del sistema de CCTV con un disco rígido en blanco o clonado. Sin embargo, se recomienda que el PIED evalúe los distintos riesgos antes de usar este método, tales como la compatibilidad del nuevo disco rígido con el sistema o la compatibilidad del disco rígido retirado con otros sistemas para examinarlo.

NOTA 2. Algunos sistemas tienen un disco rígido removible en un carrito, pero este disco rígido puede requerir del hardware del sistema para su reproducción.

Si ninguno de los métodos mencionados es posible, se recomienda trasladar la totalidad del sistema de CCTV del lugar del hecho y que el proceso de adquisición se realice en el laboratorio forense. Este es el último recurso del PIED, asumiendo que es físicamente posible de hacer debido a que algunos sistemas de CCTV son extremadamente grandes y complejos. Nuevamente, se recomienda que el PIED evalúe los riesgos con consecuencias legales y de seguros antes de trasladarlo.

Debido a la naturaleza de los dispositivos digitales y la potencial evidencia digital, las guías para la preservación de los sistemas de CCTV son similares a la preservación de computadoras, dispositivos periféricos y medios de almacenamiento digital. Ver 7.1.4 para la guía sobre la preservación de los sistemas de CCTV.

Anexo A
(Informativo)

Descripción de las competencias y habilidades básicas del PIED

Tabla A.1 - Ejemplos de descripciones de las competencias

No	Habilidades básicas	Descripciones de las habilidades básicas	Descripciones de las competencias		
			Concientización (1)	Conocimientos (2)	Habilidades (3)
1	Identificación de la evidencia digital	Caracterizar dispositivos digitales, componentes, información que puede ayudar a la investigación y leyes pertinentes al manejo de potencial evidencia digital y a los delitos informáticos. Identificar los requisitos de las herramientas para la recolección y la adquisición de datos, dispositivos y evaluar los riesgos.	General de TI como usuario y administrador en múltiples tipos de dispositivos TI y de red; procedimientos de investigación en lugares del hecho; determinación del estado del dispositivo; valor de la información como indicio; dispositivos e información relacionados con la red forense.	Configuración de registros y sistemas/aplicaciones; identificación de registros de sistemas y aplicaciones, incluyendo registros de correo electrónico, registros de internet, registros de acceso, archivos de contraseñas, archivos de configuración de sistemas e información de IP del servidor anfitrión; funcionalidad y dependencia de los dispositivos; habilidad para comprender el impacto sobre la evidencia volátil y no volátil.	Análisis especial; interpretación de registros para la detección de instrucciones para identificar otros sistemas afectados (algunas jurisdicciones requieren la confirmación de la presencia de evidencia antes de la recolección); identificar las contraseñas requeridas para los respectivos dispositivos antes de la recolección; identificar el diagrama de red y los mecanismos de control de acceso para comprender las dependencias; direcciones de enlace de IP y direcciones MAC para la confirmación de los dispositivos.
2	Recolección de la evidencia digital	Requisitos de las herramientas e implementación del embalaje de la evidencia digital protección contra amenazas del entorno. Las áreas de conocimiento cubiertas incluyen el aseguramiento de la información.	Seguridad general en la recolección de datos; principios y diseño de herramientas básicas; determinar el mejor método de recolección para preservar la máxima cantidad de información pertinente al incidente.	Formular y ejecutar un proceso de recolección; recolectar evidencia; generar la documentación de la evidencia; cadena de custodia de la evidencia; control de calidad del proceso de recolección de la evidencia; entrevistar sospechosos.	Optimizar el proceso de recolección; documentar la evidencia que no puede ser adquirida debido a restricciones diversas; recolectar contraseñas, claves, llaves, llaves electrónicas USB “*dongles*” y otra información requerida para realizar un análisis en el laboratorio.

(continúa)

Tabla A.1 (fin)

No	Habilidades básicas	Descripciones de las habilidades básicas	Descripciones de las competencias		
			Concientización (1)	Conocimientos (2)	Habilidades (3)
3	Adquisición de la evidencia digital	Aplicar los requisitos para la adquisición de la potencial evidencia digital en forma lógica, garantizando que sea repetible, *auditable*, reproducible y defendible. Las áreas a cubrir son realizar la adquisición sobre un sistema encendido, sobre un sistema apagado y adquisición forense sobre la red.	Entender la información disponible en los dispositivos digitales, las bases de datos, documentos generados por sistemas, datos generados por usuarios y datos volátiles; archivos, estructuras sistemas de archivos Unix y Windows y otros dispositivos con software embebido; concientización acerca del impacto sobre datos volátiles.	Saber cómo determinar los requisitos de almacenamiento; ejecutar un proceso de adquisición de una copia forense (por ejemplo, adquisición parcial o total de medios de almacenamiento digital); adquisición realizada sobre un sistema encendido y sobre uno apagado; generación del valor del digesto matemático.	Habilidad para realizar una adquisición de medios de almacenamiento digital, incluyendo RAID, bases de datos, dispositivos con software embebido y dispositivos miniaturizados; entender las dependencias e impactos de los diferentes métodos de adquisición.
4	Preservación de la evidencia digital	Aplicar y evaluar los requisitos de preservación de la potencial evidencia digital, entender los factores y los parámetros que influyen sobre su exactitud. Las áreas a cubrir son metodología, mantenimiento de la cadena de custodia, manejo de dispositivos informáticos y de medios de almacenamiento digital.	Entender los requisitos y procedimientos para el mantenimiento de la cadena de custodia considerando los requisitos legales; impacto del entorno como la humedad, la temperatura y los golpes sobre los dispositivos digitales; comprender las opciones de embalaje, los requisitos para el transporte y almacenamiento.	Conocimiento sobre la generación de documentos para la auditoría de la evidencia; definir parámetros para los documentos; aseguramiento de la seguridad de la información, amenazas, vulnerabilidades y controles para la evidencia digital.	Aplicar medidas para asegurar la evidencia digital, desde los dispositivos más grandes hasta los más pequeños; procedimientos para documentar los detalles de la evidencia.

Tabla A.2 - Definición de las competencias

1	Concientización - Reconocer, identificar - pedir ayuda cuando se necesita.
2	Conocimiento - Adquirido a través de capacitación formal o trabajando en equipo. Contribuir, participar - realizar con ayuda.
3	Habilidades - Experiencia demostrada a través de la aplicación en el entorno del trabajo. Trabajar sin supervisión. Aplicar, demostrar - realizar sin ayuda.

NOTA. Las competencias del PIED pueden variar de una jurisdicción a otra.

Anexo B
(Informativo)

Requisitos mínimos de documentación para la transferencia de evidencia

Se recomienda que el PIED sea responsable por los datos adquiridos y los dispositivos digitales recolectados en todo momento mientras estén bajo su custodia. Para mantener este control, el PIED necesita estar apropiadamente autorizado, capacitado y calificado. Sin embargo, como la legislación local es un factor determinante respecto de la capacidad del PIED de cumplir con los tres requisitos esperados, la competencia del PIED puede variar de una jurisdicción a otra. Como resultado, es posible que los requisitos de documentación para la transferencia de evidencia digital entre jurisdicciones no sean iguales en jurisdicciones diferentes.

En consecuencia, se necesita especificar un conjunto mínimo de requisitos para la documentación para facilitar el intercambio de potencial evidencia digital entre jurisdicciones. Los requisitos para esta documentación necesitan considerarse con los puntos de documentación mencionados en 6.6. Como esta norma no reemplaza los requisitos legales específicos de ninguna jurisdicción, sirve como una guía práctica para la transferencia de potencial evidencia digital a través de límites jurisdiccionales.

La documentación mínima a comunicar es:

- el nombre y dirección de la autoridad pertinente;
- una declaración de la autorización, la capacitación y las calificaciones del PIED;
- el objetivo del examen;
- las acciones que fueron realizadas;
- quiénes realizaron qué y cuándo;
- la cadena de custodia pertinente a la investigación específica;
- una lista descriptiva de la potencial evidencia digital y de los medios de almacenamiento digital recolectados y adquiridos; y
- la información pertinente a cualquier examen, ensayo o investigación usada para crear la copia forense.

Los requisitos específicos a la jurisdicción pueden incluir lo siguiente:

- si la evidencia se considera como un testimonio experto, puede requerirse la aceptación del código de conducta pertinente; y
- una orden judicial que especifique qué documentación se necesita transferir y el motivo de la transferencia.

Bibliografía ISO/IEC 27037:2012

[1] ILAC-G19:2002. *Guidelines for forensic science laboratories*. Available from: www.ilac.org/documents/g19_2002.pdf

[2] IOCE, *G8 proposed principles for the procedures relating to digital evidence*. Available from: http://ioce.org/core.php?ID=5

[3] ISO/IEC 15489:2001, *Information and Documentation - Records Management*

[4] ISO/IEC 17024:2003, *Conformity assessment - General requirements for bodies operating certification of persons*

[5] ISO/IEC 17043:2010, *Conformity assessment - General requirements for proficiency testing*

[6] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*

[7] ISO/IEC 27002, *Information technology - Security techniques - Information security management systems - Code of practice for information security management*

[8] ISO/IEC 24760-1, *Information technology - Security techniques - A framework for identity management - Part 1: Terminology and concepts*

[9] ISO/IEC 27031:2010, *Information technology - Security techniques - Guidelines for ICT readiness for business continuity*

[10] ISO/IEC 27035:2011, *Information technology - Security techniques - Information security incident management*

[11] *Forensic Science Society Academic Accreditation Standards & CPD*. Available from: http://www.forensic-science-society.org.uk

[12] *Guidelines for evidence collection and archiving*. Available from: http://www.ietf.org/rfc/rfc3227.txt

Anexo C - IRAM

(Informativo)

Introducción a la prueba documental informática y descripción de los principios de la criminalística dentro del marco legislativo de la República Argentina

C.1 Introducción a la prueba documental informática

En nuestro país, la gestión de la prueba documental informática, para ser válida como elemento probatorio, en el marco de un conflicto judicializado (o judicializable) necesita cumplir requisitos formales, desde el punto de vista legal (procesal de cada fuero), criminalístico (como prueba indiciaria digital) y técnico (informática).

La mayoría de las nulidades se producen por fallas en el cumplimiento de dichos requisitos (en especial los legales y criminalísticos).

En criminalística, la prueba indiciaria se define como: *"La prueba integrada por el conjunto de elementos físicos y virtuales, que obran en un lugar determinado o determinable, necesarios y suficientes (*), conducentes y pertinentes (**), para efectuar una reconstrucción lógica, científica, tecnológica y técnica de los hechos investigados, por medio del correspondiente análisis pericial forense."*

(*) Requisitos criminalísticos, con su correspondiente justificación lógica.

(**) Requisitos legales, para asegurar el derecho a la privacidad, constitucionalmente protegido.

Como la prueba indiciaria digital es una especie de la prueba indiciaria criminalística, debe reunir estos requisitos.

Además, por su eventual condición de *"prueba potencial digital"* es frecuente que requiera su ejecución como: *"prueba anticipada, medida previa o preliminar"*, que necesita autorizar el Juez, por lo que requiere:

1. verosimilitud del derecho invocado (*fomus boni iuris*);
2. peligro en la demora (*periculum in mora*);
3. contracautela de privacidad (acceso solo a la información necesaria y suficiente, conducente y pertinente para la investigación pretendida, descartando el resto de inmediato y sin más trámite).

C.2 Principios de la criminalística

C.2.1 Principio de compatibilización

Legislativa internacional. Gran parte de los contratos particulares, celebrados en el marco del derecho internacional privado, se realizan mediante comunicaciones digitales (instrumentadas en correo electrónico abierto o cifrado y certificada por medio de claves criptográficas o firma digital). La pertinencia y utilidad de la prueba informática, es siempre relativa a las definiciones que la ley de fondo y forma de cada país establece en particular y las que regulan los tratados internacionales.

C.2.2 Principio de entidad pericial

Es el empleo de los medios Informáticos, como instrumentos de conformación de prueba indiciaria informático forense. Prueba que, si bien constituye una parte de la criminalística y en lo formal no

difiere de cualquier otra prueba pericial, se integra con metodología propia que permite asegurar la detección, identificación, documentación, preservación y traslado de la prueba obtenida, con técnicas e instrumentos propios e inéditos. En este sentido, la prueba indiciaria informático forense requiere de cuidados específicos que la diferencian de otras pruebas periciales.

C.2.3 Principio de identidad atípico o principio de identidad de copias
En la duplicación de un archivo informático, la copia no es igual a la original, sino idéntica (un bit no difiere de otro bit y entre sí son indistinguibles biunívocamente). No se está en presencia de un original y su copia, sino ante dos originales.

C.2.4 Principio de sensibilidad remota
Alta sensibilidad del soporte digital a las acciones externas dolosas o culposas y posibilidad de modificación local o remota (en línea).

C.2.5 Principio de oportunidad
Refiere a las tareas complementarias (medidas preliminares, inspecciones o reconocimientos judiciales, órdenes de allanamiento o de intercepción judiciales) que aseguren su recolección, debido a su facilidad de destrucción.

C.2.6 Principio de protección y preservación
Cadena de custodia estricta y con certificación unívoca comprobable.

C.2.7 Principio tecnológico interdisciplinario
Refiere a los conocimientos específicos que se requiere por parte de todos los involucrados en la prueba indiciaria informático forense: jueces para evaluar correctamente la prueba, fiscales y abogados para efectuar la requisitoria de manera adecuada y oportuna, profesionales de la criminalística y otros profesionales para no contaminar dicha prueba durante sus propias tareas periciales y contribuir a su preservación, así como funcionarios judiciales y policiales, a efectos de proteger y mantener la cadena de custodia establecida.

C.2.8 Principio de vinculación estricta.
Refiere que la prueba indiciaria informático forense puede estar relacionada con múltiples actividades delictivas dentro de la legislación internacional o el derecho interno.

Anexo D - IRAM

(Informativo)

Bibliografía

En el estudio de esta norma se ha tenido en cuenta el antecedente siguiente:

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION
ISO/IEC 27037:2012, Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence

Anexo E - IRAM

(Informativo)

Integrantes de los organismos de estudio

El estudio de esta norma ha estado a cargo de los organismos respectivos, integrados en la forma siguiente:

Comisión Informática Forense

Integrante		Representó a:
Sr.	Sergio APPENDINO	UNIVERSIDAD CATÓLICA DE SALTA (UCASAL)
Prof.	Luis ARELLANO GONZALEZ	UNIVERSIDAD ARGENTINA J. F. KENNEDY / MINISTERIO PÚBLICO - FISCALÍA DESCENTRALIZADA DE BERAZATEGUI / UNIVERSIDAD TECNOLÓGICA NACIONAL (UTN) - FACULTAD REGIONAL AVELLANEDA / FACULTAD DEL EJÉRCITO - UNIVERSIDAD DE LA DEFENSA
Sr.	Guido BUHL	MINISTERIO PÚBLICO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES
Sr.	Gastón CAINO	SUBSECRETARÍA DE DESARROLLO URBANO Y VIVIENDA
Mg.	Juan Carlos CASALE	CONSEJO PROFESIONAL DE CIENCIAS INFORMÁTICAS DE CÓRDOBA
Ing.	Jorge Luis CEBALLOS	FUNDACIÓN UNIVERSIDAD DE BELGRANO DR. AVELINO PORTO
Sra.	Marisa CEREZOLI	INSTITUTO UNIVERSITARIO DE GENDARMERÍA NACIONAL (IUGNA)
Sr.	César CICHERCHIA	EJÉRCITO ARGENTINO - FACULTAD DE INGENIERÍA DEL EJÉRCITO
Sr.	Pablo CISTOLDI	UNIVERSIDAD DE FRATERNIDAD DE AGRUPACIONES SANTO TOMÁS DE AQUINO (FASTA)
Ing.	Pablo CROCI	EJERCITO ARGENTINO - FACULTAD DE INGENIERÍA DEL EJÉRCITO
Prof.	María Elena DARAHUGE	UNIVERSIDAD ARGENTINA J. F. KENNEDY / MINISTERIO PÚBLICO - FISCALÍA DESCENTRALIZADA DE BERAZATEGUI / UNIVERSIDAD TECNOLÓGICA NACIONAL (UTN) - FACULTAD REGIONAL AVELLANEDA / FACULTAD DEL EJÉRCITO - UNIVERSIDAD DE LA DEFENSA
Sra.	Patricia DELBONO	CONSEJO PROFESIONAL DE INGENIERÍA DE TELECOMUNICACIONES, ELECTRÓNICA Y COMPUTACIÓN (COPITEC)
Sr.	Martín DESPO	POLICÍA FEDERAL ARGENTINA (PFA)
Ing.	Ana DI IORIO	UNIVERSIDAD DE FRATERNIDAD DE AGRUPACIONES SANTO TOMÁS DE AQUINO (FASTA)

Integrante		Representó a:
Lic.	Leandro DIKENSTEIN HIDALGO	LEANDRO DIKENSTEIN HIDALGO
Sr.	Enrique DUTRA	PUNTO NET SOLUCIONES S.R.L.
Sra.	Valeria ESPÍNDOLA	ADMINISTRACIÓN FEDERAL DE INGRESOS PÚBLICOS (AFIP)
Sr.	Franco FILIPPI	MINISTERIO PÚBLICO FISCAL DE LA PROVINCIA DE CÓRDOBA
Sr.	Guillermo Javier FRITZ	PODER JUDICIAL ENTRE RÍOS
Sra.	Cintia GIOIA	UNIVERSIDAD NACIONAL DE LA MATANZA (UNLAM)
Ing.	Manrique GONZÁLEZ AVELLANEDA	MANRIQUE IGNACIO GONZÁLEZ AVELLANEDA
Sr.	Tomás GREEN	SUBSECRETARÍA DE DESARROLLO URBANO Y VIVIENDA
Sr.	Sergio Daniel GUERRERO	ADMINISTRACIÓN FEDERAL DE INGRESOS PÚBLICOS (AFIP)
Sr.	Ricardo HOLOVAT	CONSEJO FEDERAL DE MODERNIZACIÓN
Dr.	Rodrigo IGLESIAS	RODRIGO SEBASTIÁN IGLESIAS
Sr.	Mario JUÁREZ	INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMÍA SOCIAL (INAES)
Sr.	Antonio MAZA	PREFECTURA NAVAL ARGENTINA (PNA)
Sr.	Sergio MENDOZA	INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMÍA SOCIAL (INAES)
Ing.	Jorge NAGUIL	UNIVERSIDAD DE LA PATAGONIA (UNPA)
Sr.	Guillermo ODDINO	CONSEJO PROFESIONAL DE CIENCIAS INFORMÁTICAS DE CÓRDOBA
Dr. Ing.	H. Beatriz PARRA DE GALLO	UNIVERSIDAD CATÓLICA DE SALTA (UCASAL)
Sra.	Marianela PI	INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMÍA SOCIAL (INAES)
Ing.	Pablo ROMANOS	UNIVERSIDAD DE LA MARINA MERCANTE
Sr.	Rubén ROMERO	MINISTERIO PÚBLICO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES
Ing.	Diana SOLÓRZANO	UNIVERSIDAD TECNOLÓGICA NACIONAL (UTN)
Sr.	Gastón TERÁN CASTELLANOS	CONSEJO PROFESIONAL DE INGENIERÍA DE TELECOMUNICACIONES, ELECTRÓNICA Y COMPUTACIÓN (COPITEC)
Sr.	Santiago TRIGO	UNIVERSIDAD DE FRATERNIDAD DE AGRUPACIONES SANTO TOMÁS DE AQUINO (FASTA)
Ing.	Fernando VILLARES TERAN	FERNANDO MAXIMILIANO VILLARES TERAN
Lic.	Verónica MARINELLI	IRAM
Ing.	Adriana NUÑEZ	IRAM

Comité General de Normas (C.G.N.)

Integrante

Lic. Alicia GUTIÉRREZ
Dr. Ricardo MACCHI
Téc. Hugo D. MARCH
Lic. Héctor MUGICA
Ing. Roberto NATTA
Lic. Marta RAINONE de BARBIERI
Ing. Adriana NUÑEZ

ICS 35.040
* CNA 0000

* Corresponde a la Clasificación Nacional de Abastecimiento asignada por el Servicio Nacional de Catalogación del Ministerio de Defensa.