NORMA INTERNACIONAL

ISO/IEC 27037

Primera edición
2012-10-15

Tecnologías de la información - Técnicas de seguridad - Directrices para la identificación, la recogida, la adquisición y la preservación de pruebas digitales

Technologies de l'information - Techniques de sécurité - Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

Número de referencia ISO/IEC 27037:2012(E)

DOCUMENTO PROTEGIDO POR COPYRIGHT

Oficina de derechos de autor de ISO
Case postale 56 CH-1211 Ginebra 20 Tel.
+ 41 22 749 01 11
Fax+ 41 22 749 09 47
Correo
electrónicocopyright@iso.org
Web www.iso.org

Publicado en Suiza

Contenido

Págin
a

Prólogo

La ISO (Organización Internacional de Normalización) y la CEI (Comisión Electrotécnica Internacional) constituyen el sistema especializado de normalización mundial. Los organismos nacionales miembros de la ISO o de la CEI participan en la elaboración de normas internacionales a través de comités técnicos creados por la organización respectiva para ocuparse de campos concretos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC, también participan en los trabajos. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1.

Las normas internacionales se elaboran de acuerdo con las reglas que figuran en la Parte 2 de las Directivas ISO/IEC.

La principal tarea del comité técnico conjunto es preparar Normas Internacionales. Los proyectos de normas internacionales adoptados por el comité técnico conjunto se distribuyen a los organismos nacionales para su votación. La publicación como norma internacional requiere la aprobación de al menos el 75 % de los organismos nacionales que emiten un voto.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan ser objeto de derechos de patente. ISO e IEC no se hacen responsables de la identificación de tales derechos de patente.

ISO/IEC 27037 ha sido elaborado por el Comité Técnico Conjunto ISO/IEC JTC 1, *Tecnología de la información*, Subcomité SC 27, *Técnicas de seguridad informática*.

Introducción

Esta Norma Internacional proporciona directrices para actividades específicas en el manejo de potenciales evidencias digitales; estos procesos son: identificación, recolección, adquisición y preservación de potenciales evidencias digitales. Estos procesos son necesarios en una investigación diseñada para mantener la integridad de las pruebas digitales, una metodología aceptable en la obtención de pruebas digitales que contribuirá a su admisibilidad en acciones legales y disciplinarias, así como en otras instancias requeridas. Esta Norma Internacional también proporciona directrices generales para la obtención de pruebas no digitales que puedan ser útiles en la fase de análisis de las posibles pruebas digitales.

Esta Norma Internacional tiene por objeto proporcionar orientación a las personas responsables de la identificación, recogida, adquisición y conservación de posibles pruebas digitales. Entre estas personas se incluyen los Primeros Responsables de las Pruebas Digitales (DEFR), los Especialistas en Pruebas Digitales (DES), los especialistas en respuesta a incidentes y los directores de laboratorios forenses. Esta Norma Internacional garantiza que las personas responsables gestionen las posibles pruebas digitales de forma práctica y aceptable en todo el mundo, con el objetivo de facilitar la investigación en la que intervengan dispositivos digitales y pruebas digitales de forma sistemática e imparcial, preservando al mismo tiempo su integridad y autenticidad.

Esta Norma Internacional también pretende informar a los responsables de la toma de decisiones que necesitan determinar la fiabilidad de las pruebas digitales que se les presentan. Es aplicable a las organizaciones que necesitan proteger, analizar y presentar posibles pruebas digitales. Es relevante para los organismos responsables de la formulación de políticas que crean y evalúan procedimientos relacionados con las pruebas digitales, a menudo como parte de un conjunto de pruebas más amplio.

Las pruebas digitales potenciales a las que se refiere esta Norma Internacional pueden proceder de diferentes tipos de dispositivos digitales, redes, bases de datos, etc. Se refiere a datos que ya están en formato digital. Esta Norma Internacional no pretende cubrir la conversión de datos analógicos a formato digital.

Debido a la fragilidad de las pruebas digitales, es necesario llevar a cabo una metodología aceptable para garantizar la integridad y autenticidad de las posibles pruebas digitales. Esta Norma Internacional no impone el uso de herramientas o métodos concretos. Los componentes clave que aportan credibilidad a la investigación son la metodología aplicada durante el proceso y las personas cualificadas para realizar las tareas especificadas en la metodología. Esta Norma Internacional no aborda la metodología para procedimientos legales, procedimientos disciplinarios y otras acciones relacionadas en el manejo de potenciales evidencias digitales que estén fuera del ámbito de la identificación, recolección, adquisición y preservación.

La aplicación de esta Norma Internacional exige el cumplimiento de las leyes, normas y reglamentos nacionales. No debe sustituir a los requisitos legales específicos de ninguna jurisdicción. En su lugar, puede servir como directriz práctica para cualquier DEFR o DES en investigaciones que impliquen posibles pruebas digitales. No se extiende al análisis de las pruebas digitales ni sustituye a los requisitos específicos de cada jurisdicción relativos a cuestiones como la admisibilidad, la ponderación probatoria, la pertinencia y otras limitaciones controladas judicialmente sobre el uso de posibles pruebas digitales en los tribunales de justicia. Esta Norma Internacional puede ayudar a facilitar el intercambio de posibles pruebas digitales entre jurisdicciones. Con el fin de mantener la integridad de las pruebas digitales, los usuarios de esta Norma Internacional deberán adaptar y modificar los procedimientos descritos en esta Norma Internacional de acuerdo con los requisitos legales de la jurisdicción específica en materia de pruebas.

Aunque esta Norma Internacional no incluye la preparación forense, una preparación forense adecuada puede apoyar en gran medida el proceso de identificación, recogida, adquisición y preservación de las pruebas digitales. La preparación forense es la consecución de un nivel adecuado de capacidad por parte de una organización para poder identificar, recopilar, adquirir, preservar, proteger y analizar pruebas digitales. Mientras que los procesos y actividades descritos en esta Norma Internacional son esencialmente medidas reactivas utilizadas para investigar un incidente después de que se haya producido, la preparación forense es un proceso proactivo que trata de planificar este tipo de sucesos.

Esta Norma Internacional complementa las normas ISO/IEC 27001 e ISO/IEC 27002, y en particular los requisitos de control relativos a la posible adquisición de pruebas digitales, proporcionando orientaciones de aplicación adicionales. Además, esta Norma Internacional tendrá aplicaciones en contextos independientes de ISO/IEC 27001 e ISO/IEC 27002. Esta Norma Internacional debe leerse junto con otras normas relacionadas con las pruebas digitales y la investigación de incidentes de seguridad de la información.

Tecnología de la información - Técnicas de seguridad - Directrices para la identificación, recogida, adquisición y preservación de pruebas digitales

1 Ámbito de aplicación

Esta Norma Internacional proporciona directrices para actividades específicas en el manejo de pruebas digitales, que son la identificación, recogida, adquisición y preservación de pruebas digitales que puedan tener valor probatorio. Esta Norma Internacional proporciona orientación a los individuos con respecto a situaciones comunes encontradas a lo largo del proceso de manipulación de pruebas digitales y ayuda a las organizaciones en sus procedimientos disciplinarios y a facilitar el intercambio de posibles pruebas digitales entre jurisdicciones.

Esta Norma Internacional ofrece orientación para los siguientes dispositivos y/o funciones que se utilizan en diversas circunstancias:

— Medios de almacenamiento digital utilizados en ordenadores estándar como discos duros, disquetes, discos ópticos y magneto-ópticos, dispositivos de datos con funciones similares,

— Teléfonos móviles, asistentes personales digitales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria,

— Sistemas móviles de navegación,

— Cámaras fotográficas y de vídeo digitales (incluidas las de circuito cerrado de televisión),

— Ordenadores estándar con conexiones de red,

— Redes basadas en TCP/IP y otros protocolos digitales, y

— Dispositivos con funciones similares a los anteriores.

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

NOTA 2 Las circunstancias incluyen los dispositivos anteriores que existen en diversas formas. Por ejemplo, un sistema de automoción puede incluir un sistema de navegación móvil, un sistema de almacenamiento de datos y un sistema sensorial.

2 Referencia normativa

Los siguientes documentos de referencia son indispensables para la aplicación de este documento. Para las referencias fechadas, sólo se aplica la edición citada. Para las referencias sin fecha, se aplica la última edición del documento de referencia (incluidas las modificaciones).

ISO/TR 15801*, Document management - Information stored electronically - Recommendations for trustworthiness and reliability (Gestión de documentos - Información almacenada electrónicamente - Recomendaciones para la confianza y la fiabilidad*).

ISO/IEC 17020*, Conformity assessment - Requirements for the operation of various types of bodies performing inspection (Evaluación de la conformidad - Requisitos para el funcionamiento de los distintos tipos de organismos que realizan inspecciones)*

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

ISO/IEC 27000, *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Visión general y vocabulario*

3 Términos y definiciones

A efectos del presente documento, se aplicarán los términos y definiciones que figuran en las normas ISO/IEC 27000, ISO/IEC 17020, ISO/IEC 17025 e ISO/TR 15801, así como los que se indican a continuación.

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

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

3.2
espacio asignado
área de un soporte digital, incluida la memoria primaria, que se utiliza para el almacenamiento de datos, incluidos los metadatos.

3.3
recopilación
Proceso de recopilación de los elementos físicos que contienen posibles pruebas digitales.

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

3.5
prueba digital
información o datos almacenados o transmitidos en formato binario que puedan servir de prueba

3.6
copia de la prueba digital
Copia de la prueba digital que ha sido producida para mantener la fiabilidad de la prueba incluyendo tanto la prueba digital como los medios de verificación en los que el método de verificación puede estar integrado o ser independiente de las herramientas utilizadas en la verificación.

3.7
Digital Evidence First Responder
DEFR
individuo autorizado, formado y cualificado para actuar en primer lugar en el lugar de un incidente en la recogida y adquisición de pruebas digitales con la responsabilidad de manejar dichas pruebas

NOTA La autoridad, la formación y la cualificación son los requisitos necesarios para obtener pruebas digitales fiables, pero las circunstancias particulares pueden dar lugar a que una persona no cumpla los tres requisitos. En este caso, deberán tenerse en cuenta la legislación local, la política de la organización y las circunstancias individuales.

3.8
Especialista en pruebas digitales
DES
Individuo que puede llevar a cabo las tareas de un DEFR y tiene conocimientos especializados, habilidades y capacidades para manejar una amplia gama de cuestiones técnicas.

NOTA Un DES puede tener conocimientos especializados adicionales, por ejemplo, adquisición de redes, adquisición de RAM, software de sistemas operativos o conocimientos de Mainframe.

3.9
medio de almacenamiento digital
dispositivo en el que pueden grabarse datos digitales

[Adaptado de ISO/IEC 10027:1990].

3.10
instalación de preservación de pruebas
Entorno seguro o ubicación donde se almacenan las pruebas recogidas o adquiridas.

NOTA Una instalación de preservación de pruebas no debe estar expuesta a campos magnéticos, polvo, vibraciones, humedad o cualquier otro elemento ambiental (como temperatura o humedad extremas) que pueda dañar las posibles pruebas digitales que se encuentren dentro de la instalación.

3.11
valor hash
cadena de bits que es la salida de una función hash

[ISO/IEC 10118-1:2000].

3.12
identificación
proceso que implica la búsqueda, el reconocimiento y la documentación de pruebas digitales potenciales.

3.13
creación de imágenes
proceso de creación de una copia en bits de un soporte de almacenamiento digital

NOTA La copia bit a bit también se denomina copia física.

EJEMPLO Al crear una imagen de un disco duro, el DEFR también copiará los datos que se hayan borrado.

3.14
periférico
Dispositivo que se acopla a un aparato digital para ampliar su funcionalidad.

3.15
conservación
proceso destinado a mantener y salvaguardar la integridad y/o el estado original de las posibles pruebas digitales

3.16
fiabilidad
propiedad de que el comportamiento y los resultados

previstos sean coherentes [ISO/IEC 27000:2009].

3.17
repetibilidad
propiedad de un proceso llevado a cabo para obtener los mismos resultados de ensayo en el mismo entorno de ensayo (mismo ordenador, disco duro, modo de funcionamiento, etc.)

3.18
reproducibilidad
propiedad de un proceso para obtener los mismos resultados de ensayo en un entorno de ensayo diferente (ordenador, disco duro, operador, etc.).

3.19
expoliación
acto de realizar o permitir cambios en la prueba digital potencial que disminuyan su valor probatorio

3.20
hora del sistema
hora generada por el reloj del sistema y utilizada por el sistema operativo, no la hora calculada por el sistema operativo

3.21
manipulación
acto de realizar o permitir deliberadamente cambios en las pruebas digitales (es decir, expolio intencionado o deliberado).

3.22
marca de tiempo
parámetro de variante temporal que denota un punto en el tiempo con respecto a una referencia temporal común

[ISO/IEC 11770-1:1996].

3.23
espacio no asignado
área de un soporte digital, incluida la memoria primaria, que no ha sido asignada por el sistema operativo y que está disponible para el almacenamiento de datos, incluidos los metadatos.

3.24
validación
confirmación, mediante la aportación de una prueba objetiva, de que se han cumplido los requisitos para un uso o aplicación específicos previstos.

[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 de datos no idénticos no deben producir una coincidencia idéntica a partir de una función de verificación.

NOTA 2 Las funciones de verificación suelen implementarse utilizando funciones hash como MD5, SHA1, etc., pero pueden utilizarse otros métodos.

3.26
datos volátiles
datos que son especialmente propensos a cambiar y que pueden ser fácilmente modificados.

NOTA Un cambio puede ser desconectar la alimentación o atravesar un campo magnético. Los datos volátiles también incluyen datos que cambian a medida que cambia el estado del sistema. Algunos ejemplos son los datos almacenados en la RAM y las direcciones IP dinámicas.

4 Términos abreviados de

AVI Audio Video Interleave

CCTV Circuito cerrado de

televisión **CD** Disco compacto

ADN Ácido desoxirribonucleico

DEFR Evidencia Digital de Primera Respuesta

DES Especialista en pruebas digitales

DVD Vídeo digital/disco volátil

ESN	Número de serie electrónico
GPS	Sistema de posicionamiento global
GSM	Sistema Mundial de Comunicaciones Móviles
IMEI	Identidad internacional de equipo móvil
IP	Protocolo de Internet
ISIRT	Equipo de respuesta a incidentes de seguridad de la información
LAN	Red de área local
MD5	Algoritmo de cifrado de mensajes 5
MP3	MPEG Audio Capa 3
MPEG	Grupo de Expertos en Imágenes en Movimiento
NAS	Almacenamiento en red
PDA	Asistente digital personal
PED	Dispositivo electrónico personal
PIN	Número de identificación personal
PUK	Clave de desbloqueo del PIN
RAID	Conjunto redundante de discos independientes
RAM	Memoria de acceso aleatorio
RFID	Identificación por radiofrecuencia
SAN	Red de área de almacenamiento
SHA	Algoritmo hash seguro
SIM	Módulo de identidad del abonado
USB	Bus serie universal
SAI	Sistema de alimentación ininterrumpida
USIM	Módulo universal de identidad del abonado
UV	Ultravioleta
Wi-Fi	Fidelidad inalámbrica

5 Visión general

5.1 Contexto de la recogida de pruebas digitales

Las pruebas digitales pueden requerirse para su uso en una serie de escenarios distintos, cada uno de los cuales tiene un equilibrio diferente entre los impulsores de la calidad probatoria, la puntualidad del análisis, la restauración del servicio y el coste de la recogida de pruebas digitales. Por lo tanto, las organizaciones deberán contar con un proceso de priorización que identifique las necesidades y equilibre la calidad de las pruebas, la puntualidad y el restablecimiento del servicio antes de asignar recursos DEFR. Un proceso de priorización implica llevar a cabo una evaluación del material disponible para determinar el posible valor probatorio y el orden en que deben recogerse, adquirirse o conservarse las posibles pruebas digitales. La priorización se lleva a cabo para minimizar el riesgo de que las posibles pruebas digitales se estropeen y maximizar el valor probatorio de las posibles pruebas digitales recogidas.

5.2 Principios de las pruebas digitales

En la mayoría de las jurisdicciones y organizaciones, las pruebas digitales se rigen por tres principios fundamentales: pertinencia, fiabilidad y suficiencia. Estos tres principios son importantes para todas las investigaciones, no sólo p a r a que las pruebas digitales sean admisibles ante un tribunal. Las pruebas digitales son pertinentes cuando sirven para probar o refutar un elemento del caso concreto que se investiga. Aunque la definición detallada de "fiable" varía según las jurisdicciones, el significado general del principio, "garantizar que las pruebas digitales son lo que pretenden ser", está muy extendido. No siempre es necesario que el DEFR recoja todos los datos o haga una copia completa de las pruebas digitales originales. En muchas jurisdicciones, el concepto de suficiencia significa que el DEFR necesita recoger suficientes pruebas digitales potenciales para permitir que los elementos del asunto se examinen o investiguen adecuadamente. Comprender este concepto es importante para que el DEFR pueda priorizar el esfuerzo adecuadamente cuando el tiempo o el coste sean un problema.

NOTA El DEFR debe asegurarse de que la recogida de posibles pruebas digitales se realiza de acuerdo con las leyes y normativas jurisdiccionales locales, según requieran las circunstancias específicas.

Todos los procesos que vayan a ser utilizados por el DEFR y el DES deberán haber sido validados antes de su uso. Si la validación se lleva a cabo externamente, el DEFR o el DES deberán verificar que la validación es adecuada para el uso específico que hacen de los procesos y para el entorno y las circunstancias en las que se van a utilizar los procesos. El DEFR o DES también deberá

a) documentar todas las acciones;

b) determinar y aplicar un método para establecer la exactitud y fiabilidad de la posible copia de las pruebas digitales en comparación con la fuente original; y

c) reconocer que el acto de preservación de las posibles pruebas digitales no siempre puede ser no intrusivo.

5.3 Requisitos para el manejo de pruebas digitales

5.3.1 Gene ral

Los principios establecidos en la cláusula 5.2 anterior pueden satisfacerse de la siguiente manera:

— Relevancia: Debe ser posible demostrar que el material adquirido es relevante para la investigación, es decir, que contiene información de valor para ayudar a la investigación del incidente concreto y que existe una buena razón para haberlo adquirido. Mediante la auditoría y la justificación, el DEFR deberá ser capaz de describir los procedimientos seguidos y explicar cómo se tomó la decisión de adquirir cada elemento.

— Fiabilidad: Todos los procesos utilizados en el manejo de posibles pruebas digitales deben ser auditables y repetibles. Los resultados de la aplicación de dichos procesos deben ser reproducibles.

— Suficiencia: El DEFR deberá haber tenido en cuenta que se ha reunido suficiente material para poder llevar a cabo una investigación adecuada. El DEFR deberá ser capaz, mediante auditoría y justificación, de

dar una indicación de cuánto material, en total, se tuvo en cuenta y los procedimientos utilizados para decidir cuánto y qué material adquirir.

NOTA Los materiales pueden reunirse mediante actividades de adquisición y/o recopilación.

Hay cuatro aspectos clave en el tratamiento de las pruebas digitales: auditabilidad, justificabilidad y repetibilidad o reproducibilidad, dependiendo de las circunstancias particulares.

5.3.2 Auditabilidad ty

Debe ser posible que un evaluador independiente u otras partes interesadas autorizadas evalúen las actividades realizadas por un DEFR y un DES. Esto será posible documentando adecuadamente todas las acciones realizadas. El DEFR y el DES deberán ser capaces de justificar el proceso de toma de decisiones en la selección de un determinado curso de acción. Los procesos llevados a cabo por un DEFR y un DES deberán estar disponibles para su evaluación independiente con el fin de determinar si se ha seguido un método, técnica o procedimiento científico adecuado.

5.3.3 Repetibilidad

La repetibilidad se establece cuando se obtienen los mismos resultados de ensayo en las siguientes condiciones

- Utilizando el mismo procedimiento y método de medición;
- Utilizando los mismos instrumentos y en las mismas condiciones; y
- Puede repetirse en cualquier momento después de la prueba original.

Un DEFR debidamente cualificado y experimentado debería ser capaz de llevar a cabo todos los procesos descritos en la documentación y llegar a los mismos resultados, sin orientación ni interpretación. El DEFR debe ser consciente de que puede haber circunstancias en las que no sea posible repetir la prueba, por ejemplo, cuando se ha copiado un disco duro original y se ha vuelto a utilizar, o cuando un elemento incluye una memoria volátil. En este caso, el DEFR debe asegurarse de que el proceso de adquisición es fiable. Para lograr la reproducibilidad, debe existir un control de calidad y documentación del proceso.

5.3.4 Reproducibili dad

La reproducibilidad se establece cuando se obtienen los mismos resultados de ensayo en las siguientes condiciones

- Utilizando el mismo método de medición;
- Utilizando instrumentos diferentes y en condiciones diferentes; y
- Pueden reproducirse en cualquier momento después de la prueba original.

La necesidad de reproducir los resultados varía en función de las jurisdicciones y las circunstancias, por lo que el DEFR, o la persona que realice la reproducción, deberá informarse sobre las condiciones aplicables.

5.3.5 Sólo ifiability

El DEFR debe ser capaz de justificar todas las acciones y métodos utilizados en el manejo de las posibles pruebas digitales. La justificación puede lograrse demostrando que la decisión fue la mejor opción para obtener todas las pruebas digitales potenciales. Otro DEFR o DES también podría demostrarlo reproduciendo o validando con éxito las acciones y métodos utilizados.

Lo mejor para cada organización es emplear a un DEFR o DES que posea las habilidades y competencias básicas descritas en el Anexo A de esta Norma Internacional. Esto garantizará que se sigan los procesos y procedimientos correctos al manipular posibles pruebas digitales para garantizar la conservación final de las pruebas digitales que puedan tener valor probatorio. Esto también garantizará que las organizaciones puedan utilizar las

Por ejemplo, en sus procedimientos disciplinarios o para facilitar el intercambio de posibles pruebas digitales entre jurisdicciones.

NOTA La competencia descrita en el Anexo A se limita a la función DEFR, que está en consonancia con la función de DES definida en la cláusula 3.8.

5.4 Tratamiento de pruebas digitales processes

5.4.1 O visión general

Aunque el proceso completo de tratamiento de pruebas digitales incluye otras actividades (por ejemplo, presentación, eliminación, etc.), el ámbito de esta Norma Internacional se refiere únicamente al proceso inicial de tratamiento, que consiste en la identificación, recogida, adquisición y conservación de las posibles pruebas digitales.

Las pruebas digitales pueden ser frágiles por naturaleza. Pueden ser alteradas, manipuladas o destruidas por una manipulación o examen inadecuados. Los manipuladores de pruebas digitales deben ser competentes para identificar y gestionar los riesgos y las consecuencias de los posibles cursos de acción al tratar con pruebas digitales. Si no se manipulan los dispositivos digitales de manera adecuada, las posibles pruebas digitales contenidas en ellos pueden quedar inutilizadas.

El DEFR y el DES deben seguir procedimientos documentados para garantizar el mantenimiento de la integridad y fiabilidad de las posibles pruebas digitales. Los procedimientos deben incluir directrices de manipulación para las fuentes de posibles pruebas digitales y deben incluir los siguientes principios fundamentales:

— Minimizar la manipulación del dispositivo digital original o de las posibles pruebas digitales;

— Dar cuenta de cualquier cambio y documentar las medidas adoptadas (en la medida en que un experto pueda formarse una opinión sobre la fiabilidad);

— Cumplir las normas locales en materia de pruebas; y

— El DEFR y el DES no deben tomar medidas que excedan sus competencias.

El cumplimiento de los principios y requisitos fundamentales del tratamiento de las posibles pruebas digitales debería permitir preservarlas. Concretamente, en caso de que deban realizarse cambios inevitables, deberán documentarse todas las acciones y su justificación. Cada uno de los procesos del tratamiento de las pruebas digitales, es decir, la identificación, la recogida, la adquisición y la conservación, se trata con más detalle en las cláusulas siguientes.

5.4.2 Identificación ación

Las pruebas digitales se representan de forma física y lógica. La forma física incluye la representación de datos dentro de un dispositivo tangible. La forma lógica de la prueba digital potencial 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 las posibles pruebas digitales. El proceso de identificación debe identificar los medios de almacenamiento digital y los dispositivos de procesamiento que puedan contener pruebas digitales potenciales relevantes para el incidente. Este proceso también incluye una actividad para priorizar la recogida de pruebas en función de su volatilidad. La volatilidad de los datos debe identificarse para garantizar el orden correcto de los procesos de recogida y adquisición con el fin de minimizar el daño a las posibles pruebas digitales y obtener las mejores pruebas. Además, el proceso debe identificar la posibilidad de que existan pruebas digitales potenciales ocultas. El DEFR y el DES deben ser conscientes de que no todos los tipos de medios de almacenamiento digital pueden identificarse y localizarse fácilmente, por ejemplo, la computación en nube, NAS y SAN, todos añaden un componente virtual al proceso de identificación.

El DEFR debe llevar a cabo sistemáticamente una búsqueda exhaustiva de objetos que puedan contener posibles pruebas digitales. Los distintos tipos de dispositivos digitales que pueden contener posibles pruebas digitales pueden pasarse por alto fácilmente (por ejemplo, debido a su pequeño tamaño), camuflarse o mezclarse con otro material irrelevante.

Las cláusulas 6.1 y 6.6 proporcionan más información sobre los aspectos de la cadena de custodia, el embalaje y el etiquetado de la identificación de pruebas digitales. La cláusula 7 especifica directrices relativas a casos concretos de identificación, recogida, adquisición y conservación de pruebas digitales.

5.4.3 Recogida

Una vez identificados los dispositivos digitales que pueden contener posibles pruebas digitales, el DEFR y el DES deben decidir si recogerlas o adquirirlas durante el siguiente proceso. Hay una serie de factores de decisión para ello, que se tratan con más detalle en la cláusula 7. La decisión debe basarse en las circunstancias.

La recogida es un proceso del tratamiento de pruebas digitales en el que los dispositivos que pueden contener pruebas digitales potenciales se retiran de su ubicación original y se trasladan a un laboratorio o a otro entorno controlado para su posterior adquisición y análisis. Los dispositivos que contienen posibles pruebas digitales pueden encontrarse en uno de estos dos estados: cuando el sistema está encendido o cuando está apagado. En función del estado del dispositivo, se requieren distintos enfoques y herramientas. Pueden aplicarse procedimientos locales a los enfoques y herramientas utilizados para el proceso de recogida.

Este proceso incluye la documentación de todo el enfoque, así como el embalaje de estos dispositivos antes de su transporte. Es importante que el DEFR y el DES recojan cualquier material que pueda estar relacionado con la información digital potencial (por ejemplo, papel con contraseñas anotadas, cunas y conectores de alimentación para dispositivos de sistemas integrados). Las pruebas digitales potenciales pueden perderse o dañarse si no se aplica un cuidado razonable. El DEFR y el DES deben adoptar el mejor método de recogida posible en función de la situación, el coste y el tiempo, y documentar la decisión de utilizar un método concreto.

NOTA 1 No siempre se recomienda retirar los soportes de almacenamiento digital, por lo que el DEFR debe asegurarse de que es competente para hacerlo, y reconocer cuándo es apropiado y está permitido hacerlo.

NOTA 2 Los detalles sobre los dispositivos digitales no recogidos deben documentarse con la justificación de su exclusión, de acuerdo con los requisitos de la jurisdicción aplicable.

5.4.4 Adquisición ition

El proceso de adquisición implica la producción de una copia de las pruebas digitales (por ejemplo, disco duro completo, partición, archivos seleccionados) y la documentación de los métodos utilizados y las actividades realizadas. El DEFR deberá adoptar un método de adquisición adecuado en función de la situación, el coste y el tiempo, y documentar la decisión de utilizar un método o herramienta concretos de forma apropiada.

Los métodos utilizados para obtener posibles pruebas digitales deben documentarse claramente y en detalle y, en la medida de lo posible, ser reproducibles o verificables por un DEFR competente. Un DEFR o DES deberá adquirir las posibles pruebas digitales de la manera menos intrusiva posible para evitar introducir cambios en la medida de lo posible. Al llevar a cabo este proceso, el DEFR deberá considerar el método más adecuado a utilizar. Si el proceso da lugar a una alteración inevitable de los datos digitales, las actividades realizadas deberán documentarse para dar cuenta de los cambios introducidos en los datos.

El método de adquisición utilizado deberá producir una copia digital de las posibles pruebas digitales o de los dispositivos digitales que puedan contener posibles pruebas digitales. Tanto la fuente original como la copia de las pruebas digitales deberán verificarse con una función de verificación probada (cuya precisión se haya demostrado en ese momento) que sea aceptable para la persona que vaya a utilizar las pruebas. La fuente original y cada copia de la prueba digital deben producir el mismo resultado de la función de verificación.

En circunstancias en las que no se pueda realizar el proceso de verificación, por ejemplo cuando se adquiere un sistema en funcionamiento, la copia original contiene sectores de error o el periodo de tiempo de adquisición es limitado. En tales casos, el DEFR deberá utilizar el mejor método posible disponible y ser capaz de justificar y defender la selección del método. Si no se puede verificar la obtención de imágenes, habrá que documentarlo y justificarlo. En caso necesario, el método de adquisición utilizado deberá poder obtener el espacio asignado y no asignado.

NOTA 1 Cuando el proceso de verificación no pueda realizarse en la fuente completa debido a errores en la fuente, entonces podrá utilizarse la verificación utilizando aquellas partes de la fuente que puedan leerse de forma fiable.

Puede haber casos en los que no sea factible o permisible crear una copia de prueba digital de una fuente de pruebas, como cuando la fuente es demasiado grande. En estos casos, un DEFR puede realizar una adquisición lógica, dirigida únicamente a tipos de datos, directorios o ubicaciones específicos. Por lo general, esto tiene lugar a nivel de archivos y particiones. Durante la adquisición lógica, pueden copiarse los archivos activos y el espacio asignado no basado en archivos del soporte de almacenamiento digital; los archivos eliminados y el espacio no asignado pueden no copiarse, dependiendo del método utilizado. Otros casos en los que este método puede ser útil es cuando se trata de sistemas de misión crítica que no se pueden apagar.

NOTA 2 Algunas jurisdicciones pueden exigir un tratamiento especial para los datos; por ejemplo, sellarlos en presencia del propietario de los mismos. El sellado debe realizarse de acuerdo con los requisitos locales (legislativos y de procedimiento).

5.4.5 Conservación

Las posibles pruebas digitales deben conservarse para garantizar su utilidad en la investigación. Es importante proteger la integridad de las pruebas. El proceso de preservación implica la salvaguarda de las pruebas digitales potenciales y de los dispositivos digitales que puedan contenerlas para evitar su manipulación o expoliación. El proceso de preservación debe iniciarse y mantenerse a lo largo de todo el proceso de tratamiento de las pruebas digitales, empezando por la identificación de los dispositivos digitales que contienen posibles pruebas digitales.

En el mejor de los casos, no debe haber expoliación de los datos en sí ni de los metadatos asociados a ellos (por ejemplo, marcas de fecha y hora). El DEFR debe ser capaz de demostrar que las pruebas no han sido modificadas desde que fueron recogidas o adquiridas, o proporcionar la justificación y las acciones documentadas en caso de que se hayan realizado cambios inevitables.

NOTA En algunos casos, la confidencialidad de las pruebas digitales potenciales es un requisito, ya sea una exigencia empresarial o un requisito legal (por ejemplo, la privacidad). Las pruebas digitales potenciales deben conservarse de forma que se garantice la confidencialidad de los datos.

6 Componentes clave de la identificación, recogida, adquisición y conservación de pruebas digitales

6.1 Cadena de custodia

En cualquier investigación, el DEFR debe poder dar cuenta de todos los datos y dispositivos adquiridos en el momento en que se encuentran bajo su custodia. El registro de la cadena de custodia es un documento que identifica la cronología del movimiento y manipulación de las posibles pruebas digitales. Debe instituirse desde el proceso de recogida o adquisición. Normalmente, esto se consigue trazando la historia del objeto desde el momento en que fue identificado, recogido o adquirido por el equipo investigador hasta su estado y localización actuales.

El registro de la cadena de custodia es un documento o una serie de documentos relacionados que detallan la cadena de custodia y registran quién fue responsable del manejo de las posibles pruebas digitales, ya sea en forma de datos digitales o en otros formatos (como notas en papel). El objetivo de mantener un registro de la cadena de custodia es permitir la identificación del acceso y el movimiento de posibles pruebas digitales en un momento dado. El propio registro de la cadena de custodia puede constar de más de un documento; por ejemplo, en el caso de las pruebas digitales potenciales, debe existir un documento contemporáneo que registre la adquisición de datos digitales en un dispositivo concreto, el movimiento de dicho dispositivo y la documentación que registre los extractos o copias posteriores de las pruebas digitales potenciales para su análisis u otros fines. El registro de la cadena de custodia debe contener, como mínimo, la siguiente información

— Identificador único de la prueba;

— Quién accedió a las pruebas y la hora y el lugar en que tuvo lugar;

— Quién registró la entrada y salida de las pruebas del centro de conservación de pruebas y cuándo ocurrió;

— Por qué se retiraron las pruebas (en qué caso y con qué fin) y la autoridad competente, si procede; y

— Cualquier cambio inevitable en las posibles pruebas digitales, así como el nombre de la persona responsable y la justificación de la introducción del cambio.

La cadena de custodia debe mantenerse durante toda la vida útil de la prueba y conservarse durante un determinado periodo de tiempo una vez finalizada la vida útil de la prueba - este periodo de tiempo puede establecerse en función de las jurisdicciones locales de recogida y aplicación de pruebas. Debe establecerse desde el momento en que se adquieren los dispositivos digitales y/o las posibles pruebas digitales, y no debe ponerse en peligro.

NOTA Algunas jurisdicciones pueden tener requisitos especiales en relación con la cadena de custodia. El DEFR deberá cumplir dichos requisitos.

6.2 Precauciones en el lugar del incidente

6.2.1 General

El DEFR deberá realizar actividades para asegurar y proteger la ubicación de las posibles pruebas digitales tan pronto como lleguen al lugar. Las actividades deben apoyar lo siguiente, con sujeción a la legislación local:

— Asegurar y tomar el control del área que contiene los dispositivos;

— Determinar quién es la persona encargada del lugar;

— Asegurarse de que las personas se alejan de los dispositivos y de las fuentes de alimentación;

— Documente a cualquier persona que tenga acceso al lugar y a cualquier persona que pueda tener motivos para estar implicada en el lugar del incidente;

— Si el dispositivo está encendido, no lo apague, y si está apagado, no lo encienda;

— Si es posible, documente (por ejemplo, mediante croquis, fotografía o vídeo) la escena, todos los componentes y cables en su posición original. Si no se dispone de cámara fotográfica y/o de vídeo, dibuje un croquis del sistema y etiquete los puertos y cables para que el sistema pueda validarse y reconstruirse posteriormente; y

— Si está permitido, registrar las zonas en busca de objetos como notas adhesivas, agendas, papeles, ordenadores 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 pruebas de vídeo. El DEFR deberá cumplir dichos requisitos.

NOTA 2 Los DEFR deben ser conscientes de que las pruebas digitales potenciales pueden no estar siempre en ubicaciones obvias, como el almacenamiento distribuido o virtualizado.

El DEFR debe conocer en primer lugar todos los riesgos que conlleva la realización de todos los procesos durante la investigación. Debe tenerse en cuenta la protección del personal y de las posibles pruebas digitales en el lugar del incidente.

6.2.2 Personal

Es importante llevar a cabo una evaluación de riesgos en relación con la seguridad del personal antes de iniciar el proceso, ya que la seguridad del personal implicado en el proceso es vital. Las cuestiones que deben tenerse en cuenta al evaluar los riesgos para el personal son, entre otras, las siguientes:

— ¿Estará presente la persona o personas investigadas? Si están presentes, ¿tienen propensión a la violencia?

— ¿A qué hora del día se llevará a cabo la operación?

— ¿Puede aislarse el lugar del incidente de los transeúntes?

— ¿Hay armas en la zona?

— ¿Existen riesgos físicos para las personas presentes?

— ¿Podría haber algo en las proximidades, incluido el dispositivo, configurado para causar daños físicos si se manipula de forma inadecuada, por ejemplo, una trampa oculta?

— ¿Tiene el material que se va a recoger alguna probabilidad de causar daños psicológicos u ofender?

— ¿Puede considerarse inseguro el lugar del incidente?

— ¿Influye la zona circundante en el potencial de riesgo?

6.2.3 Posibles pruebas digitales

El DEFR debe tener cuidado al utilizar una herramienta específica para recoger o adquirir pruebas digitales potenciales. No calcular los riesgos antes de actuar puede llevar a la pérdida de algunas o todas las pruebas digitales potenciales debido a la tecnología aplicada durante la recogida o adquisición. Deben evaluarse los riesgos para reducir la exposición a reclamaciones por daños y perjuicios.

La evaluación de riesgos implica la evaluación sistemática de los riesgos y del impacto potencial que pueden tener en la investigación de las pruebas digitales. Entre los aspectos que deben tenerse en cuenta durante la evaluación de riesgos de las posibles pruebas digitales figuran los siguientes:

— ¿Qué tipo de métodos de recogida/adquisición deben aplicarse?

— ¿Cuál es el equipo que puede necesitarse in situ?

— ¿Cuál es el nivel de volatilidad de los datos y la información relacionados con las posibles pruebas digitales?

— ¿Es posible el acceso remoto a cualquier dispositivo digital y supone una amenaza para la integridad de las pruebas?

— ¿Qué ocurre si se dañan los datos o el equipo?

— ¿Podrían haberse puesto en peligro los datos?

— ¿Podría haberse configurado el dispositivo digital para destruir (por ejemplo, mediante una bomba lógica), estropear u ofuscar datos si se apaga o se accede a él de forma incontrolada?

6.3 Funciones y responsabilidades

La función del DEFR consiste en la identificación, recogida, adquisición y conservación de posibles pruebas digitales en el lugar del incidente. Incluye la elaboración de un informe de recogida y adquisición, pero no necesariamente el informe de análisis. La función del DEFR también implica garantizar la integridad y autenticidad de las posibles pruebas digitales. En el desempeño de su función, el DEFR debe tener la experiencia, las aptitudes y los conocimientos adecuados en el manejo de posibles pruebas digitales. Esto es crucial porque las posibles pruebas digitales pueden estropearse fácilmente.

El DEFR también puede necesitar la ayuda de personal de apoyo técnico en áreas relacionadas. La función de un DES consiste en prestar apoyo técnico al DEFR en la identificación, recogida, adquisición y conservación de posibles pruebas digitales en el lugar del incidente. El DES proporciona conocimientos especializados al DEFR. La matriz de competencias para el DEFR (véase el Anexo A) sirve de guía para identificar sus niveles de competencia pertinentes.

NOTA En el contexto de la gestión de incidentes donde existe un ISIRT, las funciones de un DEFR y/o DES como miembro del equipo ISIRT se tratan en ISO/IEC 27035:2011.

6.4 Competencia

El DEFR y/o el DES deben tener las competencias técnicas y legales pertinentes (por ejemplo, las del Anexo A) y deben poder demostrar que han recibido la formación adecuada y que tienen los conocimientos técnicos y legales suficientes para manejar adecuadamente las posibles pruebas digitales. Esto incluye la comprensión de los procesos y métodos adecuados para el tratamiento de posibles fuentes de pruebas digitales. Una formación adecuada permitirá a los DEFR manejar dispositivos digitales que contengan posibles pruebas digitales. Disponer del mejor conjunto de herramientas no garantizará la calidad de las pruebas digitales si el DEFR no es competente en la realización de las tareas.

Algunas jurisdicciones han prescrito el modo en que los DEFR deben establecer sus cualificaciones. Es responsabilidad de los DEFR asegurarse de que están debidamente informados sobre cómo hacerlo en las jurisdicciones pertinentes. Cuando sea necesario, el DEFR y/o el DES deberán ser capaces de demostrar que son competentes para manejar posibles pruebas digitales utilizando las herramientas y métodos seleccionados para realizar las tareas. También se requiere que los DEFR puedan aportar pruebas de su competencia continua.

Algunos de los requisitos previos para los DEFR son los siguientes:

— Deben haber recibido una formación adecuada y suficiente para manejar dispositivos digitales en el contexto de las actividades de investigación;

— Deben demostrar y mantener sus habilidades y competencia ante las autoridades competentes en el ámbito pertinente de la manipulación de posibles pruebas digitales.

— Es responsabilidad de la(s) persona(s) y del empleador garantizar que reciben la formación adecuada y que se mantienen sus habilidades y competencia.

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

6.5 Tenga un cuidado razonable

Evite cualquier acción que pueda conducir al expolio de posibles pruebas digitales almacenadas en dispositivos digitales debido a acciones intencionadas o no intencionadas. Por ejemplo, la exposición a campos magnéticos puede estropear posibles pruebas digitales contenidas en soportes de almacenamiento magnético. El DEFR no debe acceder a los dispositivos digitales, por ejemplo para realizar un volcado de memoria de un dispositivo digital activo, a menos que cuente con la competencia necesaria y con el uso de procesos fiables y validados.

Existen algunas circunstancias en las que no resulta práctico recopilar o adquirir posibles pruebas digitales. El DEFR debe tener en cuenta las siguientes circunstancias, aunque no se limita únicamente a ellas:

— Si no existe derecho o autorización legal para recoger el dispositivo digital;

— Si existe la obligación de utilizar otros métodos (por ejemplo, para evitar la interrupción de una actividad);

— Si el DEFR desea captar el método de operación de un sospechoso durante el abuso de un sistema;

— Si la recogida o adquisición debe realizarse de forma encubierta, si la jurisdicción lo considera 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 un sistema RAID;

— Si se trata de un dispositivo digital crítico para la seguridad que pondría en peligro la vida si se detuviera; y

— Si se trata de un dispositivo digital que también presta servicio a partes inocentes.

6.6 Documentación

La documentación es fundamental cuando se manipulan dispositivos digitales que pueden contener pruebas digitales potenciales. El DEFR debe respetar los siguientes puntos durante la documentación:

— Todas las actividades realizadas deben documentarse. De este modo se garantiza que no se ha omitido ningún detalle durante los procesos de identificación, recogida, adquisición y conservación. También puede ser útil en una También puede ser útil en una investigación transfronteriza en la que las posibles pruebas digitales obtenidas en otra parte del mundo puedan rastrearse en consecuencia.

— El DEFR debe ser sensible al ajuste de la hora y la fecha si los dispositivos digitales están encendidos. Compare el ajuste de la hora con una fuente horaria fiable, como una hora sincronizada con una fuente horaria fiable y rastreable. Estos ajustes de la hora deben documentarse y anotarse si existen diferencias. Algunos sistemas sistemas requieren mucha interacción del usuario para obtener los ajustes de hora y fecha. El DEFR debe tener cuidado de no modificar el sistema. Sólo el personal debidamente formado debe recuperar estos ajustes.

— El DEFR debe documentar todo lo visible en la pantalla del dispositivo digital: programas y procesos activos, así como los nombres de los documentos abiertos. Esta documentación debe incluir una descripción de lo que es visible, ya que algunos programas maliciosos pueden hacerse pasar por software conocido.

— Cualquier movimiento de los dispositivos digitales debe documentarse de acuerdo con los requisitos locales.

— Documentar todos los identificadores únicos de los dispositivos digitales y las partes asociadas, como los números de serie y las marcas únicas.

En el Anexo B se muestran ejemplos de un conjunto mínimo de documentación para el intercambio transjurisdiccional de posibles pruebas digitales.

NOTA Consulte la cláusula de gestión de documentos y la cláusula de gestión de registros de la norma ISO/IEC 17025:2005 para obtener más información sobre la documentación.

6.7 Sesión informativa

6.7.1 Generalidades

Es esencial que el DEFR y el DES reciban la información adecuada de la autoridad competente antes de realizar sus tareas, respetando al mismo tiempo las leyes y limitaciones de confidencialidad (es decir, la necesidad de conocer). Es importante celebrar una sesión informativa formal para comprender el incidente, qué esperar y qué no esperar durante la investigación, y un recordatorio contra la manipulación o el expolio de pruebas. La sesión informativa debe ser suficiente para que los miembros estén bien preparados para desempeñar sus funciones y responsabilidades, garantizando así la extracción de todas las posibles pruebas digitales pertinentes.

6.7.2 Pruebas digitales específicas

Se necesita una sesión informativa centrada explícitamente en las orientaciones específicas sobre pruebas digitales para informar a los DEFR sobre los detalles relativos a la investigación. Durante la sesión informativa, el DEFR y el DES deben recibir la información pertinente e instrucciones detalladas en relación con las posibles pruebas digitales que deban recogerse o adquirirse. Esto puede incluir

— Tipo de incidente (si se conoce);

— Fecha y hora del incidente (si se conocen);

— Plan de investigación (recogida y/o adquisición, actividad de red conocida, necesidad de datos volátiles conocida, etc.);

— Considerar dónde y cómo se almacenan/transportan las posibles pruebas digitales tras su recogida o adquisición;

— Herramientas específicas necesarias para adquirir las posibles pruebas digitales;

— Pruebas digitales potenciales relacionadas con tipos específicos de investigación;

— Equipos y manuales relacionados con los dispositivos digitales;

— Recordar a los miembros del equipo que desactiven cualquier capacidad Bluetooth o Wi-Fi de sus teléfonos/ordenadores para que no interactúen inadvertidamente con los dispositivos digitales, excepto en el caso de los teléfonos/ordenadores utilizados para detectar las conexiones.

— Importancia de la documentación a lo largo de la investigación; y

— Factores legales aplicables u otros factores que puedan prohibir la recogida de los dispositivos y las posibles pruebas digitales que contengan.

Esta sesión informativa específica puede formar parte de la sesión informativa general descrita en la cláusula 6.7.1.

6.7.3 Específica para el personal

Para informar a los DEFR sobre los aspectos relativos a las partes implicadas en la investigación es necesaria una sesión informativa centrada explícitamente en las orientaciones específicas para el personal. Durante la sesión informativa, el equipo de investigación recibirá instrucciones relacionadas con el personal. Esto puede incluir

— Asignaciones, funciones y responsabilidades de los miembros del equipo de investigación en el lugar del incidente;

— Si se espera que otras autoridades (personal médico, investigadores forenses biológicos, etc.) participen en la investigación;

— Exigir a los miembros del equipo que no acepten asistencia técnica de personas no autorizadas.

— Exigir a los miembros del equipo que sigan estrictamente el procedimiento para minimizar el riesgo de estropear las posibles pruebas digitales, como evitar el uso de herramientas o materiales que puedan producir o emitir electricidad estática o un campo magnético, ya que pueden dañar o destruir las posibles pruebas digitales.

Esta sesión informativa específica puede formar parte de la sesión informativa general descrita en la cláusula 6.7.1.

6.7.4 Incidentes en tiempo real

Es muy deseable que la investigación de un incidente se planifique con antelación, pero hay circunstancias (por ejemplo, cuando un incidente se está desarrollando y se está respondiendo a él en tiempo real) en las que puede no haber sido posible una planificación completa. En estas situaciones, se debe informar al equipo de las estrategias y tácticas iniciales para la investigación y permitirle que desarrolle nuevas estrategias y tácticas en respuesta a las condiciones imperantes. La información sobre el incidente, a medida que se desarrolla, debe compartirse entre el equipo lo más rápidamente posible para garantizar que las decisiones sobre las acciones a emprender puedan tomarse de forma eficaz y teniendo debidamente en cuenta la necesidad de justificación.

6.7.5 Otras informaciones

Aparte de las pruebas digitales y el personal, otra información importante que debe comunicarse a los equipos de investigación es la siguiente:

— Designación del área investigada, incluido el nombre de la organización, la dirección y un mapa de localización (si está disponible);

— Mandato de investigación;

— Detalles de las órdenes de registro y otras autoridades aplicables a la investigación, incluidos los límites del registro y la incautación;

— Aspectos e implicaciones jurídicas;

— Calendario de la investigación;

— Equipo necesario que debe llevarse al lugar del incidente para la investigación;

— Información logística; y

— Posibles conflictos de intereses.

El DEFR debe evitar situaciones en las que puedan hacerse acusaciones de parcialidad inherente. Un ejemplo de parcialidad inherente es cuando un DEFR copia un ordenador y no otro (que más tarde resulta contener pruebas exculpatorias) basándose en una percepción formada por la sesión informativa.

6.8 Priorización de la recogida y adquisición

A la hora de priorizar la recogida o adquisición de posibles pruebas digitales, es imprescindible que el DEFR comprenda la razón por la que se recogen o adquieren dichas pruebas. Como principio general, el DEFR debe intentar maximizar la cantidad de datos conservados mediante acciones de recogida y adquisición. Sin embargo, puede ser necesario priorizar los elementos en función de su volatilidad y/o relevancia/valor probatorio potencial. Los elementos de gran relevancia/valor probatorio potencial son los que tienen más probabilidades de contener datos relacionados directamente con el incidente investigado.

La priorización por volatilidad sólo es aplicable si las circunstancias específicas del caso investigado así lo requieren. Las pruebas digitales potenciales pueden dividirse en dos categorías: volátiles y no volátiles. Los datos volátiles pueden destruirse fácilmente o perderse para siempre si no se aplica el debido cuidado para protegerlos. Por ejemplo, retirar la fuente de alimentación de un dispositivo digital puede provocar la pérdida de los datos volátiles. Los datos no volátiles permanecen en el soporte aunque se retire la fuente de alimentación. Dado que algunos tipos de pruebas digitales pueden tener una vida corta, las pruebas digitales potenciales pueden ser fácilmente manipuladas o estropearse. Cuando no esté claro si los dispositivos digitales contienen pruebas digitales potenciales, o qué elementos son más relevantes que otros, puede ser necesario examinarlos antes de la recogida mediante un proceso para determinar la prioridad. Los dispositivos digitales que deben tenerse en cuenta para la recogida incluyen, entre otros: equipos informáticos y medios de almacenamiento digital, sistemas de circuito cerrado de televisión, PED, sistemas de automoción, sistemas de control y electrónica improvisada. Adquiera primero las pruebas digitales potenciales más volátiles, como la memoria RAM, el espacio de intercambio, los procesos en ejecución, etc. El DEFR debe poseer conocimientos sólidos para priorizar en función de la volatilidad.

Tras la identificación, el DEFR deberá:

— Dar prioridad a las pruebas digitales potenciales que se perderían para siempre si se retira la fuente de alimentación; y

— Tome medidas rápidas para recopilar y adquirir estos datos con métodos validados.

NOTA 1 Algunos datos volátiles pueden cambiar debido a factores que incluyen, entre otros, la ubicación, la hora y los cambios en los dispositivos digitales circundantes; asegúrese de que dichos datos se conservan antes de trasladar el dispositivo.

NOTA 2 Los dispositivos digitales que contengan posibles pruebas digitales pueden ser una fuente de pruebas físicas (por ejemplo, huellas dactilares, ADN, etc.). Los DEFR deben tener cuidado de no estropear dichas pruebas y coordinarse con los recolectores de pruebas pertinentes antes de proceder a las siguientes actividades.

NOTA 3 Cuando se sospecha de cifrado o malware, es conveniente examinar los datos volátiles.

En estas circunstancias, el tiempo puede ser un factor limitante durante una investigación. En estos casos, debe darse preferencia a las pruebas digitales potenciales identificadas como relevantes para el incidente específico.

6.9 Preservación de posibles pruebas digitales

6.9.1 Resumen

Para conservar las posibles pruebas digitales adquiridas y los dispositivos digitales recogidos durante el embalaje, es importante proteger estos elementos de forma que se evite su expoliación o manipulación. El expolio puede deberse a la degradación magnética, la degradación eléctrica, el calor, la exposición a alta o baja humedad, así como a golpes y vibraciones. La manipulación puede ser el resultado de un acto intencionado de hacer o permitir cambios en las posibles pruebas digitales. Por lo tanto, es crucial proteger las pruebas digitales potenciales lo mejor posible y utilizar los datos originales lo menos posible. Es importante que el DEFR esté familiarizado con los requisitos de embalaje específicos de la jurisdicción pertinente.

6.9.2 Conservación de las posibles pruebas digitales

Todos los dispositivos digitales recogidos y las pruebas digitales potenciales adquiridas deben protegerse en la medida de lo posible de pérdidas, manipulaciones o expolios. La actividad más importante en el proceso de conservación es mantener la integridad y autenticidad de las posibles pruebas digitales y su cadena de custodia.

Los dispositivos digitales recogidos y las pruebas digitales potenciales adquiridas deben almacenarse en un centro de conservación de pruebas que aplique controles de seguridad física, como sistemas de control de acceso, sistemas de vigilancia o sistemas de detección de intrusos, u otro entorno controlado para la conservación de pruebas digitales. Los principales objetivos de la seguridad física son proteger y evitar pérdidas, daños y manipulaciones, así como permitir la auditabilidad.

Los dispositivos digitales recogidos deben envolverse o colocarse en un embalaje adecuado a la naturaleza del dispositivo para evitar su contaminación antes de transportarlos a otro lugar. Se puede utilizar un embalaje resistente a los golpes para evitar daños físicos a cualquier componente del dispositivo o dispositivos.

— El DEFR debe tener en cuenta la sensibilidad del dispositivo digital a la electricidad estática. Si esto es motivo de preocupación, el dispositivo debe asegurarse en una bolsa antiestática.

— Las unidades del sistema principal y los ordenadores portátiles deben asegurarse en un contenedor adecuado para evitar la manipulación o el expolio de las posibles pruebas digitales que puedan contener.

NOTA El uso de una bolsa Faraday, u otro embalaje blindado contra radiofrecuencias, puede aumentar el agotamiento de la batería del teléfono móvil. Esto puede requerir el suministro de energía auxiliar al dispositivo mientras está dentro de la bolsa, si los recursos lo permiten.

6.9.3 Embalaje de dispositivos digitales y pruebas digitales potenciales

6.9.3.1 Actividades de base: embalaje de posibles pruebas digitales

Las actividades de base deben llevarse a cabo a menos que exista una buena razón para no hacerlo. También pueden denominarse acciones mínimas que deben realizarse. Durante el empaquetado, el DEFR debe tener en cuenta y abordar las siguientes actividades básicas:

— No tocar la cinta magnética, sino coger las cintas por sus fundas protectoras o por zonas que se sabe que no contienen datos (por ejemplo, los bordes de los discos ópticos). Esto sólo debe hacerse si el DEFR lleva guantes que no suelten pelusa.

NOTA Las zonas específicas de los soportes de almacenamiento que se sabe que no contienen datos dependen del tipo de soporte. Es responsabilidad del DEFR conocer la tecnología actual y estar familiarizado con la manipulación de soportes de almacenamiento.

— Para garantizar una correcta identificación, el DEFR deberá etiquetar todas las posibles pruebas digitales. Algunas jurisdicciones tienen requisitos específicos sobre el formato de etiquetado del material probatorio. El DEFR debe conocer y cumplir los requisitos aplicables al asunto en cuestión. El DEFR deberá etiquetar todas las pruebas digitales potenciales, los dispositivos digitales recogidos y cualquier pieza de hardware asociada a los dispositivos con un etiquetado a prueba de manipulaciones. La etiqueta no debe colocarse directamente sobre las partes mecánicas del dispositivo digital y no debe cubrir ni ocultar información identificativa importante. Todas las posibles

de los dispositivos recogidos deben adquirirse y almacenarse de forma que se garantice la integridad de las pruebas.

— Cuando sea posible, los dispositivos digitales con aberturas y componentes móviles deben precintarse con etiquetas a prueba de manipulaciones que sean apropiadas para los dispositivos, y el DEFR debe firmar en el precinto.

— Los dispositivos conectados a baterías con datos volátiles deben comprobarse periódicamente para asegurarse de que siempre tienen suficiente suministro eléctrico.

— Identifique y asegure los dispositivos digitales en un contenedor adecuado a la naturaleza del dispositivo frente a las posibles amenazas.

— Los ordenadores y dispositivos digitales deben embalarse de forma que se eviten daños por golpes, vibraciones, altitud elevada, calor y exposición a radiofrecuencia durante el transporte.

— Los medios de almacenamiento magnético deben guardarse en embalajes inertes desde el punto de vista magnético, antiestáticos y libres de partículas.

— Los dispositivos digitales también pueden contener pruebas latentes, rastros o pruebas biológicas. Por ello, deben realizarse las actividades adecuadas para preservar las posibles pruebas digitales. La obtención de imágenes de las pruebas digitales debe realizarse después de que se lleven a cabo los procesos de recogida de pruebas latentes, de rastros o biológicas en los dispositivos. No obstante, la
Sin embargo, la decisión de dar prioridad a la recogida de pruebas debe evaluarse minuciosamente para preservar las pruebas.

6.9.3.2 Actividades adicionales: embalaje de posibles pruebas digitales

Las actividades adicionales se refieren a actividades cuya realización se recomienda encarecidamente. Durante el empaquetado, el DEFR deberá tener en cuenta y abordar las siguientes actividades adicionales, cuando proceda:

— Utilizar guantes que no suelten pelusa y asegurarse de que las manos están limpias y secas.

— Proteger los dispositivos digitales de la influencia de fuentes electromagnéticas (por ejemplo, radios policiales, altavoces, máquinas de rayos X). El entorno de embalaje debe estar libre de electricidad estática.

— El entorno de embalaje debe estar libre de polvo, grasa y contaminantes químicos que favorezcan el deterioro oxidativo y la condensación de humedad en la capa magnética.

— Reduzca al mínimo la posibilidad de que se produzcan "print-through" (transferencia de una señal de un bucle de cinta a otro bucle adyacente), que pueden producirse cuando las cintas se almacenan durante largos periodos sin uso activo, lo que da lugar a una mala calidad de la señal.

— Cuando sea necesario, las zonas de envasado deben estar libres de luz UV. Los rayos UV pueden degradar el ADN o dañar algunos tipos de soportes. El DEFR debe considerar si los rayos UV suponen un riesgo para las posibles pruebas digitales antes de seleccionar una zona de embalaje.

— Los dispositivos digitales deben estar fuertemente protegidos de los choques térmicos.

6.9.4 Transporte de posibles pruebas digitales

El DEFR debe preservar los dispositivos digitales recogidos y las posibles pruebas digitales adquiridas durante el transporte. Las pruebas digitales potenciales no deben dejarse desatendidas durante el proceso de transporte. El DEFR deberá mantener la cadena de custodia durante todo el proceso de transporte para evitar posibles manipulaciones o expolios, y mantener la integridad y autenticidad de los dispositivos digitales y las posibles pruebas digitales. Si las posibles pruebas digitales no son transportadas por el DEFR o el DES, se recomienda utilizar el cifrado.

NOTA El DEFR deberá asegurarse de que la recogida de información sensible o personal se ajusta a las leyes y reglamentos locales sobre protección de datos.

Durante el embalaje y el transporte, el DEFR debe ser consciente de la posible presencia de descargas electrostáticas que pueden dañar el valor probatorio de las posibles pruebas digitales. El DEFR debe asegurarse de que los ordenadores y dispositivos digitales se embalan de forma segura durante el transporte para evitar daños por golpes y vibraciones.

El proceso de transporte debe permitir un entorno propicio y controlado. El nivel de humedad y temperatura debe ser adecuado para los dispositivos digitales. Evite mantener las posibles pruebas digitales y los dispositivos digitales en el vehículo de transporte durante periodos prolongados y evite que estén en presencia de rayos UV.

En algunas jurisdicciones, cuando las circunstancias no lo permiten, el DEFR no puede acompañar a las pruebas. En tales casos, puede recurrirse a mecanismos de transporte apropiados y autorizados para garantizar la debida seguridad de las pruebas durante el transporte. Los documentos del transporte y la verificación de la integridad del paquete deben formar parte de la cadena de custodia.

7 Casos de identificación, recogida, adquisición y conservación

7.1 Ordenadores, dispositivos periféricos y soportes de almacenamiento digital

7.1.1 Identificación

7.1.1.1 Búsqueda y documentación en el lugar del incidente físico

En el contexto de esta cláusula, los ordenadores 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 como impresoras, escáneres, cámaras web, reproductores MP3, sistemas GPS, dispositivos RFID, etc. Un dispositivo digital que tenga una interfaz de red, pero que no esté conectado en el momento de la recogida o adquisición, debe considerarse (a efectos de esta Norma Internacional) como un ordenador autónomo. Cuando se encuentre un ordenador con interfaz de red, pero sin conexión evidente, deberán r e a l i z a r s e actividades para identificar los dispositivos a los que puede haber estado conectado en un pasado reciente.

Por lo general, los lugares del incidente contendrán varios tipos de medios de almacenamiento digital. Los medios de almacenamiento digital se utilizan para almacenar datos de dispositivos digitales y varían en capacidad de memoria. Algunos ejemplos de medios de almacenamiento digital son, entre otros, los discos duros portátiles externos, las memorias flash, los CD, los DVD, los discos Blu-ray, los disquetes, las cintas magnéticas y las tarjetas de memoria.

Antes de proceder a cualquier adquisición o recogida, deben tenerse en cuenta los aspectos de seguridad de las posibles pruebas digitales. Estos aspectos se describen en las cláusulas 6.2.1 y 6.2.2. No obstante, el DEFR deberá asegurarse de que un dispositivo aparentemente autónomo no se ha conectado recientemente a una red. Cuando se sospeche que un dispositivo aparentemente autónomo ha sido desconectado recientemente, deberá considerarse la posibilidad de tratarlo como un dispositivo conectado a la red para garantizar que otras partes de la red se gestionan correctamente. El DEFR debe anotar y abordar al menos lo siguiente:

— El DEFR debe documentar el tipo y la marca de cualquier dispositivo digital utilizado e identificar todos los dispositivos informáticos y periféricos que pueda ser necesario adquirir o recoger durante esta fase inicial. Deberán documentarse los números de serie, los números de licencia y otras marcas identificativas (incluidos los daños físicos).
siempre que sea posible.

— En la fase de identificación, el estado de los ordenadores y dispositivos periféricos debe seguir siendo el mismo. Si los ordenadores o dispositivos periféricos están apagados, no los encienda. Si los ordenadores o dispositivos periféricos
Si los ordenadores o dispositivos periféricos están encendidos, el DEFR no debe apagarlos, ya que de lo contrario podría estropear las posibles pruebas digitales.

— Si los ordenadores están encendidos, el DEFR debe fotografiar o hacer un documento escrito de lo que aparece en las pantallas. Cualquier documento escrito debe incluir una descripción de lo que es realmente visible (por ejemplo, posiciones aproximadas de las ventanas, títulos y contenidos).

Durante el embalaje y el transporte, el DEFR debe ser consciente de la posible presencia de descargas electrostáticas que pueden dañar el valor probatorio de posibles pruebas digitales. El DEFR debe asegurarse de que los ordenadores y dispositivos digitales se embalan de forma segura durante el transporte para evitar daños por golpes y vibraciones.

El proceso de transporte debe permitir un entorno propicio y controlado. El nivel de humedad y temperatura debe ser adecuado para los dispositivos digitales. Evite mantener las posibles pruebas digitales y los dispositivos digitales en el vehículo de transporte durante periodos prolongados y evite que estén en presencia de rayos UV.

En algunas jurisdicciones, cuando las circunstancias no lo permiten, el DEFR no puede acompañar a las pruebas. En tales casos, puede recurrirse a mecanismos de transporte apropiados y autorizados para garantizar la debida seguridad de las pruebas durante el transporte. Los documentos del transporte y la verificación de la integridad del paquete deben formar parte de la cadena de custodia.

7 Casos de identificación, recogida, adquisición y conservación

7.1 Ordenadores, dispositivos periféricos y soportes de almacenamiento digital

7.1.1 Identificación

7.1.1.1 Búsqueda y documentación en el lugar del incidente

En el contexto de esta cláusula, los ordenadores 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 como impresoras, escáneres, cámaras web, reproductores MP3, sistemas GPS, dispositivos RFID, etc. Un dispositivo digital que tenga una interfaz de red, pero que no esté conectado en el momento de la recogida o adquisición, debe considerarse (a efectos de esta Norma Internacional) como un ordenador autónomo. Cuando se encuentre un ordenador con interfaz de red, pero sin conexión evidente, deberán r e a l i z a r s e actividades para identificar los dispositivos a los que puede haber estado conectado en un pasado reciente.

Por lo general, los lugares del incidente contendrán varios tipos de medios de almacenamiento digital. Los medios de almacenamiento digital se utilizan para almacenar datos de dispositivos digitales y varían en capacidad de memoria. Algunos ejemplos de medios de almacenamiento digital son, entre otros, los discos duros portátiles externos, las memorias flash, los CD, los DVD, los discos Blu-ray, los disquetes, las cintas magnéticas y las tarjetas de memoria.

Antes de proceder a cualquier adquisición o recogida, deben tenerse en cuenta los aspectos de seguridad de las posibles pruebas digitales. Estos aspectos se describen en las cláusulas 6.2.1 y 6.2.2. No obstante, el DEFR deberá asegurarse de que un dispositivo aparentemente autónomo no se ha conectado recientemente a una red. Cuando se sospeche que un dispositivo aparentemente autónomo ha sido desconectado recientemente, deberá considerarse la posibilidad de tratarlo como un dispositivo conectado a la red para garantizar que otras partes de la red se gestionan correctamente. El DEFR debe anotar y abordar al menos lo siguiente:

— El DEFR debe documentar el tipo y la marca de cualquier dispositivo digital utilizado e identificar todos los dispositivos informáticos y periféricos que pueda ser necesario adquirir o recoger durante esta fase inicial. Los números de serie, los números de licencia y otras marcas identificativas (incluidos los daños físicos) deben documentarse siempre que sea posible.

— En la fase de identificación, el estado de los ordenadores y dispositivos periféricos debe seguir siendo el mismo. Si los ordenadores o dispositivos periféricos están apagados, no los encienda. Si los ordenadores o periféricos
Si los ordenadores o dispositivos periféricos están encendidos, el DEFR no debe apagarlos, ya que de lo contrario podría estropear las posibles pruebas digitales.

— Si los ordenadores están encendidos, el DEFR debe fotografiar o hacer un documento escrito de lo que aparece en las pantallas. Cualquier documento escrito debe incluir una descripción de lo que es realmente visible (por ejemplo, posiciones aproximadas de las ventanas, títulos y contenidos).

— Los dispositivos con baterías que puedan agotarse deben cargarse para garantizar que no se pierda información. El DEFR tiene que identificar y recoger posibles cargadores de baterías y cables durante esta fase.

— El DEFR también deberá considerar el uso de un detector de señales inalámbricas para detectar e identificar señales inalámbricas de dispositivos inalámbricos que puedan estar ocultos. Puede haber casos en los que no se utilice un detector de señales inalámbricas debido a limitaciones de coste y tiempo, y el DEFR deberá documentarlo. Si se encuentra algún dispositivo
Si se encuentra algún dispositivo conectado a la red, el DEFR deberá continuar con el proceso de tratamiento de pruebas descrito en la cláusula 7.2.2.2 de este documento. Cuando se vaya a utilizar la exploración activa (es decir, difusión y/o sondeo) en busca de dispositivos en red, los dispositivos de exploración deberán desconectarse hasta que se haya determinado la posibilidad de que el dispositivo interactúe con otros dispositivos en el lugar de los hechos. Los miembros del equipo deben recordar que determinados dispositivos del lugar de los hechos pueden detectar la presencia de dispositivos de exploración activos y que el uso de la exploración activa puede desencadenar acciones que pueden echar a perder posibles pruebas digitales y, en circunstancias extremas, puede dar lugar a la activación de trampas ocultas.

NOTA 1 En algunas jurisdicciones, está permitido encender dispositivos digitales en una escena para determinar su relevancia para la investigación si hay muchos dispositivos digitales presentes. Esto se hace teniendo en cuenta el tiempo de procesamiento y el coste en que se puede incurrir si se adquieren dispositivos digitales no pertinentes. Si se enciende un dispositivo para evaluarlo en el lugar de los hechos, el DEFR deberá asegurarse de que durante el proceso se toman notas detalladas de las medidas adoptadas.

NOTA 2 Al preservar el estado de energía del dispositivo digital, deben tenerse en cuenta los resultados del proceso de priorización de volatilidad y relevancia. Si se toma la decisión de que la información más crítica es la información no volátil en disco, entonces ese sistema en ejecución puede tener su pantalla de consola fotografiada y el enchufe de alimentación desconectado. Si la información volátil en memoria es relevante, entonces es crítico dejar el sistema encendido para permitir su adquisición.

7.1.1.2 Recogida de pruebas no digitales

El DEFR debe considerar la recogida de pruebas no digitales. Para ello, el jefe del equipo deberá identificar a las personas responsables de las instalaciones en el lugar de los hechos. Esta persona puede facilitar información y documentación adicional, como las contraseñas de los dispositivos digitales y otros datos pertinentes. El DEFR debe documentar el nombre y la designación de esta persona.

Es posible que el DEFR también tenga que recopilar algunas pruebas hablando con personas que puedan tener información útil o relevante sobre las posibles pruebas digitales o dispositivos digitales que deban recopilarse. Cualquier respuesta deberá documentarse con precisión. Entre estas personas pueden encontrarse el administrador del sistema, el propietario del dispositivo y los usuarios del ordenador y de los dispositivos periféricos. Durante esta recogida verbal de pruebas, el DEFR puede solicitar información como la configuración del sistema y la contraseña de administrador/root. Esta información adicional puede ser útil en la fase de análisis de las posibles pruebas digitales. Estas conversaciones deben documentarse para garantizar que los detalles son exactos y que la declaración documentada no puede modificarse. El DEFR debe estar familiarizado con los requisitos jurisdiccionales pertinentes para la obtención de pruebas no digitales.

7.1.1.3 Proceso de toma de decisiones para la recogida o adquisición

A la hora de decidir la recogida de un dispositivo digital o la adquisición de posibles pruebas digitales, deberán tenerse en cuenta varios factores, entre los que se incluyen los siguientes

— la volatilidad de las pruebas digitales potenciales, que se trató en las cláusulas 5.4.2 y 6.8

— existencia de cifrado de disco completo o volúmenes cifrados en los que la frase de contraseña o las claves pueden residir como datos volátiles en la memoria RAM, en tokens externos, tarjetas inteligentes, otros dispositivos o medios,

— criticidad del sistema, que se trató en las cláusulas 5.4.4, 7.2.1.2 y 7.1.3.4,

— los requisitos legales de una jurisdicción, y

— los recursos, como el tamaño del almacenamiento necesario, la disponibilidad de personal y las

limitaciones de tiempo. La figura 1 ilustra el proceso de toma de decisiones para llevar a cabo la recogida

o la adquisición.

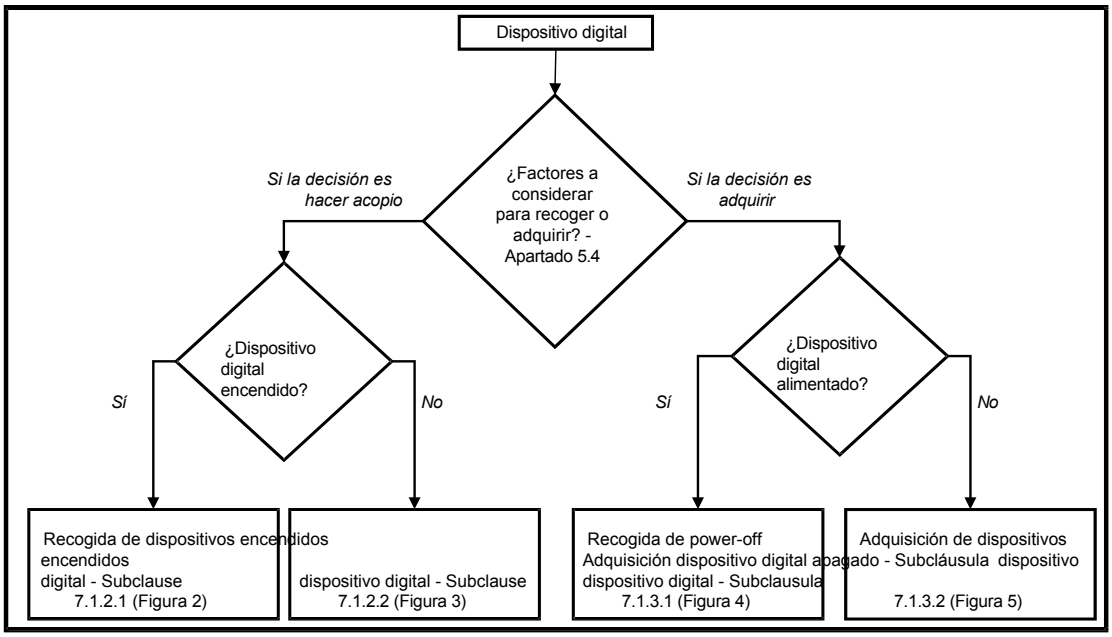

Figura 1 - Directrices para la toma de decisiones sobre la recogida o adquisición de posibles pruebas digitales

7.1.2 Recogida

7.1.2.1 Accionadas en dispositivos digitales

7.1.2.1.1 Resumen

El DEFR puede seguir una serie de directrices para la recogida cuando el dispositivo digital está encendido. No todas las directrices son ideales y adecuadas para cualquier caso; algunas directrices sólo son pertinentes para casos específicos. Por consiguiente, las directrices pueden clasificarse como básicas o adicionales. Las actividades básicas deben aplicarse en todas las circunstancias, mientras que las adicionales deben aplicarse cuando sean pertinentes y aplicables, en función del dispositivo o las circunstancias particulares. La figura 2 ilustra las actividades básicas y adicionales aplicables a la recogida de dispositivos digitales alimentados.

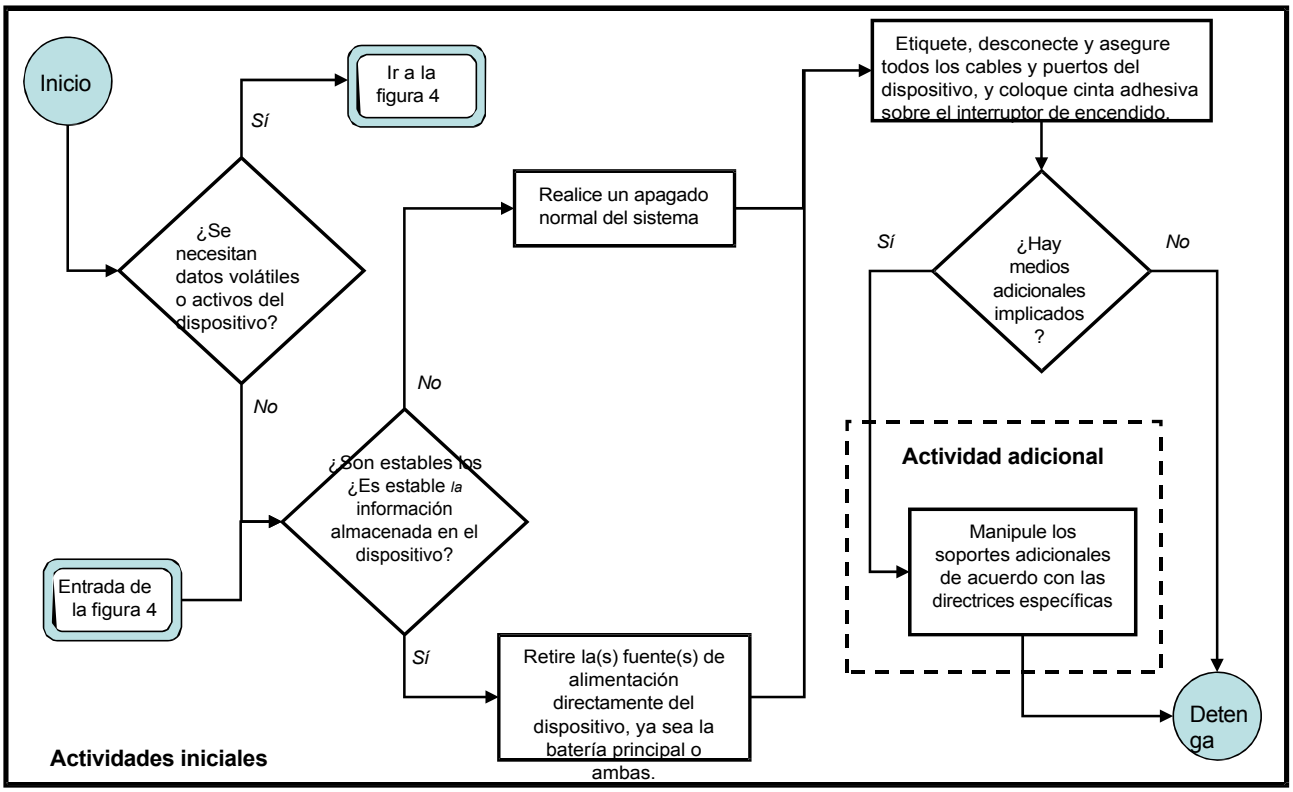

Figura 2 - Directrices para la recogida de energía en dispositivos digitales

NOTA Todas estas actividades deben realizarse de acuerdo con las leyes y normativas jurisdiccionales locales.

Es responsabilidad del DEFR conocer la tecnología actual y estar familiarizado con las directrices de manipulación de los medios de almacenamiento.

7.1.2.1.2 Actividades básicas: recogida de dispositivos digitales alimentados

El DEFR deberá seguir las siguientes actividades básicas en todos los casos que impliquen posibles pruebas digitales. Estas directrices se aplican cuando el DEFR ha decidido que debe recogerse un dispositivo digital encendido:

— Considere la posibilidad de adquirir los datos volátiles y el estado actual del dispositivo digital antes de apagar el sistema. Las claves de cifrado y otros datos cruciales pueden residir en la memoria activa o en la memoria inactiva que aún no se ha borrado. Considere la posibilidad de realizar una adquisición lógica cuando sospeche que se trata de un cifrado. En este caso
ten en cuenta que el sistema operativo del host en vivo puede no ser de confianza, así que considera el uso de herramientas apropiadas de confianza y validadas.

— La configuración del dispositivo digital puede determinar si el DEFR necesita apagar el dispositivo mediante los procedimientos administrativos normales o si debe desenchufarlo de la toma de corriente. El DEFR puede necesitar consultar con un DES para determinar el mejor enfoque dadas las
circunstancias específicas. Si se toma la decisión de desenchufar el dispositivo, el DEFR deberá retirar el cable de alimentación quitando primero el extremo conectado al dispositivo digital y no el que está conectado a la toma de corriente. Tenga en cuenta que un dispositivo conectado a un SAI puede ver alterados sus datos si se desenchufa el cable de alimentación de la pared y no el dispositivo.

NOTA 1 Si se retira la alimentación de un dispositivo digital encendido, cualquier prueba digital potencial almacenada en volúmenes cifrados será inaccesible, a menos que se obtenga la clave de descifrado. También podrían perderse datos vivos potencialmente valiosos, lo que daría lugar a reclamaciones por daños y perjuicios o a la pérdida de vidas humanas, como datos corporativos o dispositivos digitales que controlan equipos médicos. Por ello, el DEFR debe asegurarse de que los datos volátiles se recogen antes de retirar la fuente de alimentación.

NOTA 2 Existen dispositivos de hardware que permiten desconectar el dispositivo encendido de la red eléctrica y transferirlo a un SAI portátil sin interrumpir la alimentación del dispositivo. También hay dispositivos que se pueden utilizar para evitar que se active el salvapantallas. Ambos dispositivos proporcionan herramientas útiles cuando se trata de un dispositivo encendido en el que puede estar activo el cifrado. Cuando un dispositivo encendido se recoge de forma que se mantenga la alimentación, el embalaje y el transporte de un sistema en funcionamiento tienen que abordar cuestiones relacionadas con el suministro de refrigeración, la protección contra golpes mecánicos, etc.

— Etiquete, desconecte y asegure todos los cables del dispositivo digital y etiquete los puertos para que el sistema pueda reconstruirse posteriormente.

— Coloque cinta adhesiva sobre el interruptor de alimentación si es necesario para evitar que cambie de estado. Considere si el estado del interruptor se ha documentado adecuadamente antes de grabarlo o moverlo.

7.1.2.1.3 Actividades adicionales: recogida de dispositivos digitales encendidos

A continuación se indican actividades adicionales que son pertinentes en función de la configuración del dispositivo digital específico.

— Si se trata de un ordenador portátil, asegúrese de que los datos volátiles se adquieren antes de retirar la batería. El DEFR debe retirar primero la batería de la fuente de alimentación principal, en lugar de pulsar el botón de encendido del del ordenador portátil para apagarlo. El DEFR también debe tomar nota de si hay un adaptador de corriente y, en caso afirmativo, retirarlo después de extraer la batería.

NOTA 1 La acción de pulsar el botón de encendido de un dispositivo digital puede estar configurada para iniciar una secuencia de comandos que puede alterar información o borrar información del sistema antes de apagarlo, o para alertar a los sistemas conectados de que se ha producido un suceso inesperado, de modo que puedan borrar datos de valor probatorio antes de ser identificados. También puede configurarse para activar un dispositivo destinado a causar daños físicos al DEFR y a otras personas presentes.

— Coloca cinta adhesiva sobre la ranura para disquetes, si la hay.

— Asegúrese de que las bandejas de las unidades de CD o DVD están retraídas en su sitio; observe si estas bandejas de unidades están vacías, contienen discos o están desmarcadas; y cierre con cinta adhesiva la ranura de la unidad para evitar que se abra.

NOTA 2 Si se deja algún medio de arranque, la próxima vez que se encienda la máquina podría arrancar desde ese medio en lugar de desde el disco duro (o la unidad flash de las herramientas forenses), dependiendo de la configuración de la BIOS del ordenador.

El DEFR debe llevar a cabo la recogida de pruebas no digitales de acuerdo con las leyes procesales para garantizar que cualquier prueba sea admisible.

7.1.2.2 Dispositivos digitales apagados

7.1.2.2.1 Resumen

El DEFR puede seguir una serie de directrices para la recogida de pruebas cuando el dispositivo digital está apagado. No todas las actividades contenidas en estas directrices son pertinentes en todas las circunstancias. Por lo tanto, hay que distinguir entre las actividades que se aplican en todos los casos (actividades básicas) y las que sólo pueden aplicarse en algunos casos (actividades adicionales). La figura 3 ilustra las actividades básicas y adicionales aplicables a la recogida de dispositivos digitales apagados.

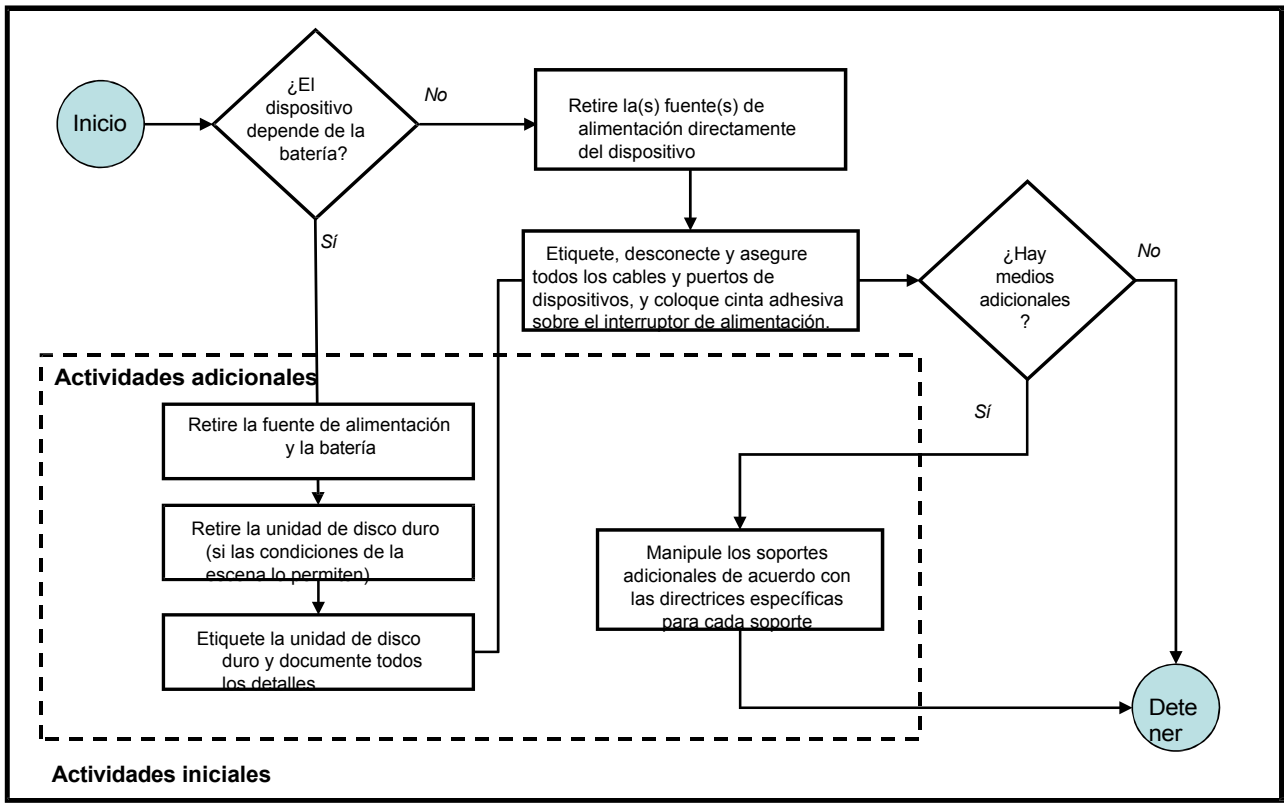

Figura 3 - Directrices para la recogida de dispositivos digitales apagados

Es responsabilidad del DEFR conocer la tecnología actual y estar familiarizado con las directrices de manipulación de los medios de almacenamiento.

7.1.2.2.2 Actividades básicas: recogida de dispositivos digitales apagados

A continuación se indican las actividades básicas recomendadas para la recogida cuando el dispositivo digital está apagado:

— Retire el cable de alimentación retirando primero el extremo conectado al dispositivo digital y no el extremo conectado a la toma de corriente.

— Desconecte y fije todos los cables de los dispositivos digitales y etiquete los puertos para poder reconstruir el sistema más adelante.

— Coloque cinta adhesiva sobre el interruptor de alimentación si es necesario para evitar que el interruptor cambie de estado. Tenga en cuenta si el estado del interruptor se ha documentado correctamente antes de grabarlo o moverlo.

NOTA En la mayoría de los casos, el soporte de almacenamiento no debe retirarse del dispositivo digital hasta que vaya a adquirirse, ya que su retirada aumenta el riesgo de dañarlo o confundirlo con otro soporte de almacenamiento. Deben desarrollarse y seguirse los procedimientos locales relativos a la necesidad de retirar los soportes de almacenamiento de los dispositivos degitales.

7.1.2.2.3 Actividades adicionales: recogida de dispositivos digitales apagados

A continuación se indican actividades adicionales pertinentes para la recogida de dispositivos digitales apagados, en función de la configuración del dispositivo digital específico:

— En primer lugar, asegúrese de que el ordenador portátil está apagado, ya que algunos pueden estar en modo de espera. Tenga en cuenta que algunos ordenadores portátiles pueden encenderse abriendo la tapa. A continuación, proceda a extraer la batería de la fuente de alimentación principal del ordenador portátil.

— Si las condiciones sobre el terreno obligan a retirar el disco duro, el DEFR debe tener cuidado de conectar a tierra el dispositivo digital para evitar que la electricidad estática dañe el disco duro. De lo contrario, el disco duro no debe extraerse sobre el terreno. Etiquete el disco duro como disco sospechoso y documente todos los detalles, como la marca, nombre del modelo, número de serie y tamaño del disco duro.

— Coloque cinta adhesiva sobre la ranura para disquetes, si la hay.

— Asegúrese de que las bandejas de las unidades de CD o DVD están retraídas en su sitio; anote si estas bandejas están vacías, contienen discos o no están marcadas; y cierre con cinta adhesiva la ranura de la unidad para evitar que se abra.

NOTA: Si se deja algún soporte de arranque, la próxima vez que se encienda el equipo, podría arrancar desde ese soporte en lugar de desde el disco duro (o la unidad flash de las herramientas forenses), dependiendo de la configuración de la BIOS del ordenador.

7.1.3 Adquisición

7.1.3.1 Dispositivos digitales encendidos

7.1.3.1.1 Resumen

Existen tres escenarios en los que puede ser necesario realizar la adquisición: cuando los dispositivos digitales están encendidos, cuando los dispositivos digitales están apagados y cuando los dispositivos digitales están encendidos pero no se pueden apagar (como los dispositivos digitales de misión crítica). En todos estos casos, el DEFR debe realizar una copia exacta de las pruebas digitales de los soportes de almacenamiento de los dispositivos digitales sospechosos de contener posibles pruebas digitales.

Si no puede obtenerse una imagen, podrían adquirirse copias exactas de archivos específicos sospechosos de contener posibles pruebas digitales. Lo ideal sería producir tanto una copia maestra verificada como copias de trabajo. La copia maestra no debería volver a utilizarse a menos que sea necesario verificar el contenido de la copia de trabajo o producir una copia de trabajo de sustitución tras los daños sufridos por la primera copia de trabajo.

El DEFR puede seguir una serie de directrices para la adquisición cuando se detecta que el dispositivo digital está encendido. No todas las directrices son ideales y apropiadas para todos los casos; algunas directrices sólo son relevantes para casos específicos. En consecuencia, las directrices pueden clasificarse como básicas o adicionales. Debe tenerse en cuenta la posibilidad de que un sistema encendido entre en modo salvapantallas o se bloquee automáticamente y que cualquier esfuerzo que se haga para evitarlo tiene consecuencias. Por ejemplo, el uso de un "mouse-jiggler" requerirá la entrada de una llave USB en el registro y lo más probable es que se produzcan modificaciones para cualquier acción que se tome. El uso de métodos fiables debería minimizar las implicaciones de tales acciones. La figura 4 ilustra la línea de base y las actividades adicionales aplicables a la adquisición de dispositivos digitales alimentados.

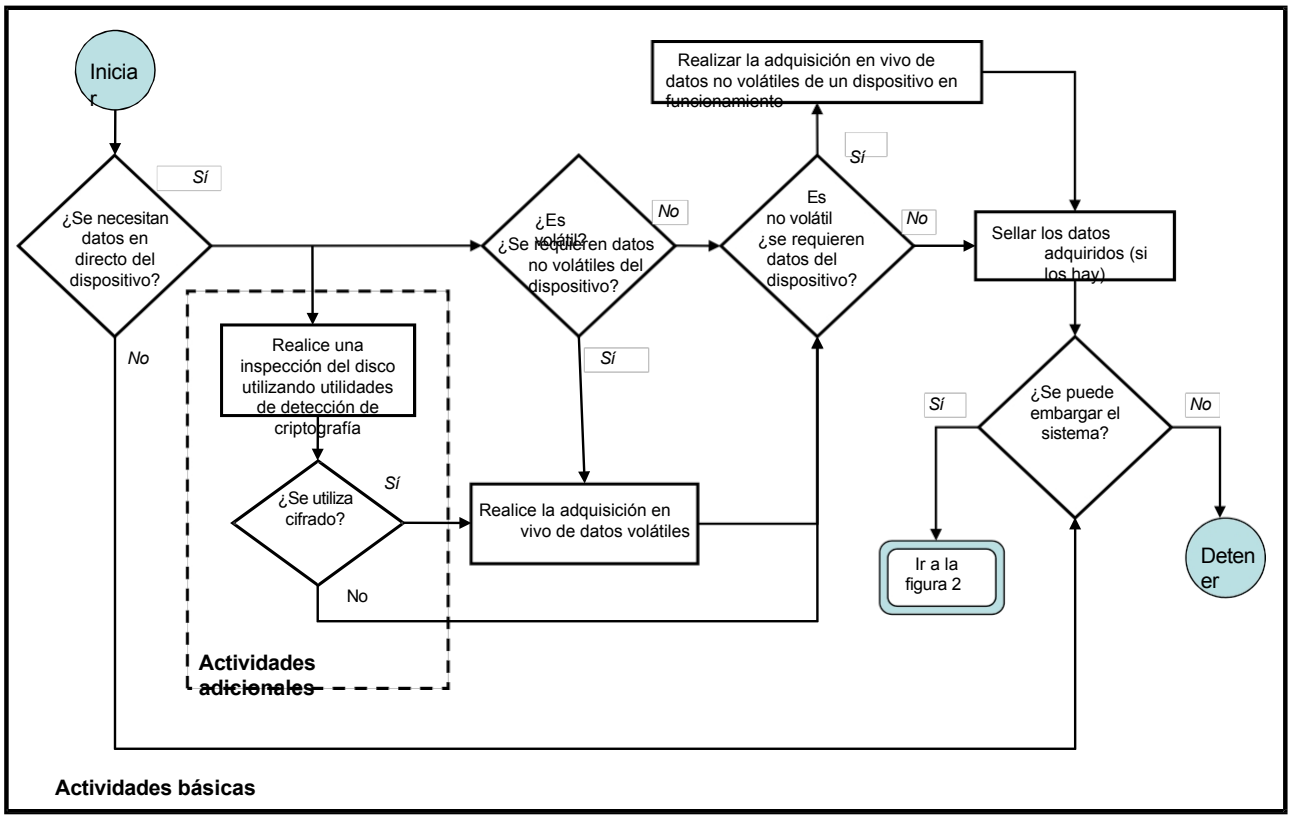

Figura 4 - Directrices para la adquisición de dispositivos digitales encendidos

7.1.3.1.2 Actividades básicas: adquisición de dispositivos digitales encendidos

A continuación se exponen las actividades básicas que debe seguir el DEFR en todos los casos que impliquen la posible obtención de pruebas digitales en dispositivos digitales encendidos:

— En primer lugar, considerar la adquisición de las posibles pruebas digitales que, de otro modo, podrían perderse si se apaga el dispositivo digital. Esto también se conoce como datos volátiles, como los almacenados en la memoria RAM, los procesos en ejecución, las conexiones de red y los ajustes de fecha y hora.
conexiones de red y ajustes de fecha y hora. En circunstancias en las que es necesario adquirir datos no volátiles de dispositivos que aún están en funcionamiento, debe considerarse la posibilidad de realizar una adquisición en un sistema encendido.

— La adquisición en vivo es necesaria para adquirir datos en vivo de dispositivos que aún están en funcionamiento. La adquisición en vivo de datos volátiles en RAM puede permitir la recuperación de información valiosa, como el estado de la red,
aplicaciones descifradas y contraseñas. La adquisición en vivo puede realizarse en la consola o de forma remota a través de la red. Los procesos son diferentes y requieren el uso de un conjunto diferente de herramientas.

— El DEFR nunca debe confiar en los programas de los sistemas. Por este motivo, siempre que sea posible, se recomiendan herramientas de confianza obtenidas por el DEFR (binarios estáticos). El DEFR debe ser competente para utilizar
herramientas validadas y ser competente para tener en cuenta los efectos que dichas herramientas pueden tener en el sistema (por ejemplo, desplazamiento de posibles pruebas digitales, contenido de la memoria que se pagina al cargar el software, etc.). Todas las acciones realizadas y los cambios resultantes en las pruebas digitales potenciales deben documentarse y comprenderse. Si no es posible determinar el efecto probable de la introducción de herramientas en el sistema o si los cambios resultantes no pueden determinarse con certeza, esto también deberá documentarse.

— Cuando se adquieran datos volátiles, el DEFR deberá utilizar un contenedor de archivos lógicos siempre que sea posible y documentar su valor hash una vez que contenga el archivo o archivos de datos volátiles. Cuando esto no sea posible, se utilizará un contenedor como, por ejemplo, un archivo ZIP, al que se le aplicará el hash y cuyo valor se documentará. La dirección

— Interfaz del dispositivo: El conector de alimentación suele ser específico de un fabricante y una ayuda fiable para la identificación.

— Etiqueta del dispositivo: En el caso de los dispositivos móviles apagados, la información obtenida del interior de la cavidad de la batería puede ser reveladora, sobre todo si se combina con una base de datos adecuada. Por ejemplo, el IMEI es un número de 15 dígitos que indica el fabricante, el tipo de modelo y el país de homologación de los dispositivos GSM; el ESN
es un identificador único de 32 bits documentado en un chip seguro de un teléfono móvil por el fabricante: los primeros 8-14 bits identifican al fabricante y los restantes al número de serie asignado.

— Búsqueda inversa: en el caso de los teléfonos móviles, si se conoce el número de teléfono, puede utilizarse una búsqueda inversa para identificar al operador de la red.

Debido al pequeño tamaño general de los dispositivos móviles, el DEFR debe tener especial cuidado para identificar todos los tipos de dispositivos móviles que puedan ser relevantes para el caso. El DEFR debe proteger el lugar del presunto incidente y asegurarse de que nadie se lleva dispositivos móviles o digitales del lugar. Los dispositivos digitales que puedan contener pruebas digitales deben protegerse del acceso no autorizado.

NOTA En algunos casos, la comunicación no debe interrumpirse. Informar a las personas autorizadas sobre posibles problemas (por ejemplo, no avisar a personas desconocidas sobre el dispositivo apagado).

7.2.1.2 Búsqueda y documentación en el lugar del incidente físico

Antes de proceder a cualquier adquisición o recogida, el lugar del incidente debe documentarse de forma visual, ya sea fotografiando, videografiando o dibujando el lugar tal y como aparecía en el momento de la entrada. La elección del método de documentación debe sopesarse en función de las circunstancias, el coste, el tiempo, los recursos disponibles y las prioridades. El DEFR deberá documentar todos los demás objetos del lugar de los hechos que puedan contener material potencialmente relevante, como notas garabateadas, notas adhesivas, agendas, etc.

— El DEFR deberá documentar el tipo, la marca, el modelo y los números de serie de todos los dispositivos digitales utilizados e identificar todos los dispositivos digitales que pueda ser necesario adquirir o recoger durante esta fase inicial. Todos los
Todos los dispositivos móviles y sus elementos asociados, como tarjetas de memoria, tarjetas SIM, cargadores y soportes encontrados en el lugar de los hechos, sus números de serie asociados y cualquier característica identificativa deben documentarse y recogerse, si es necesario. También hay que tratar de encontrar el embalaje original de los teléfonos móviles, que puede contener notas con los códigos PIN y PUK.

— Si el dispositivo está conectado en red, el DEFR debe identificar los servicios prestados por los dispositivos para comprender las dependencias y determinar la criticidad de los dispositivos dentro de la red antes de decidir sobre
desconectar el dispositivo de la red. Esto es importante si los dispositivos cumplen funciones críticas que no pueden tolerar ningún tiempo de inactividad o para evitar la destrucción de posibles pruebas digitales. Sin embargo, si parece haber amenazas continuas a los dispositivos basadas en la red, el DEFR puede tener que decidir desconectar el dispositivo de la red para proteger las posibles pruebas digitales.

— Si el dispositivo en red es un sistema de CCTV, el DEFR deberá anotar el número de cámaras conectadas al sistema, así como cuáles de estas cámaras están funcionando activamente. El DEFR también deberá anotar la marca, el modelo y los ajustes básicos del sistema, como los ajustes de visualización, los ajustes de grabación actuales y el
para que, en caso de que haya que realizar cambios para facilitar el proceso de recogida y adquisición, sea posible devolver el sistema a su estado original.

— En la medida de lo posible, el estado de los dispositivos digitales debe permanecer tal cual. En general, si los dispositivos digitales están apagados, el DEFR no debe encenderlos y si están encendidos, el DEFR no debe apagarlos. Esto puede evitar el expolio innecesario de posibles pruebas digitales. Un dispositivo que tenga
Las baterías que puedan agotarse deben cargarse para garantizar que no se pierda información. Durante esta fase, el DEFR debe identificar los posibles medios y cables de carga. Si un dispositivo va a ser transportado y examinado en una fecha futura indeterminada, puede ser conveniente apagarlo para minimizar la posibilidad de que se dañen los datos que contiene.

— El DEFR también debería considerar la posibilidad de utilizar un detector de señales inalámbricas para detectar e identificar una señal inalámbrica procedente de dispositivos inalámbricos que puedan estar ocultos. Puede haber casos en los que no se utilice el detector de señales inalámbricas debido a limitaciones de coste y tiempo, y el DEFR deberá documentarlo.

7.2.2 Recogida, adquisición y conservación

7.2.2.1 Resumen

El DEFR debe decidir si recoge o adquiere las posibles pruebas digitales de los dispositivos digitales. La elección debe sopesarse en función de las circunstancias, el coste, el tiempo, los recursos disponibles y las prioridades.

Si el DEFR decide desconectar los dispositivos, el proceso de recogida o adquisición de las posibles pruebas digitales seguirá lo descrito en la cláusula 5.4. En caso de que los dispositivos no puedan desconectarse de la red debido a la criticidad de su función o a la probabilidad de destrucción de las posibles pruebas digitales, el DEFR deberá llevar a cabo la adquisición en vivo mientras los dispositivos permanezcan conectados a la red.

NOTA Es fundamental contar con procedimientos sólidos y normalizados que empleen herramientas validadas, junto con una buena documentación y un DEFR formado y con experiencia.

La recogida y adquisición de posibles pruebas digitales de dispositivos móviles conectados a la red son complicadas porque pueden existir en múltiples estados y modos de interacción, como Bluetooth, radiofrecuencia, pantalla táctil e infrarrojos. Además, los distintos fabricantes de dispositivos móviles utilizan diferentes tipos de sistemas operativos, lo que requiere diferentes métodos de adquisición de pruebas. También existe una amplia gama de tarjetas de memoria que se utilizan con los dispositivos móviles, y la extracción de estas tarjetas de memoria de los dispositivos móviles encendidos podría interferir con los procesos en ejecución.

Por lo general, los dispositivos móviles como PDA y teléfonos móviles necesitan estar encendidos para adquirir posibles pruebas digitales. Estos dispositivos pueden alterar continuamente su entorno operativo mientras están encendidos, por ejemplo, el temporizador del reloj puede actualizarse. El problema asociado es que dos copias de pruebas digitales del mismo dispositivo pueden no superar funciones de verificación estándar como el hashing. En esta situación, pueden ser más apropiadas funciones de verificación alternativas que identifiquen áreas comunes y/o diferentes.

Es importante que el DEFR no introduzca dispositivos Wi-Fi o Bluetooth en el lugar de los hechos que puedan cambiar la información de emparejamiento de los posibles dispositivos de pruebas. Esto es especialmente importante si el investigador necesita saber qué dispositivos se han conectado.

Si el DEFR decidiera seguir un proceso de adquisición, los dispositivos de red deberían mantenerse en funcionamiento para su posterior análisis con el fin de averiguar qué otros dispositivos están conectados a los dispositivos de red. El DEFR deberá considerar la posibilidad de sabotaje por parte del sospechoso a través de una conexión de red activa y decidir si vigila el sistema o lo desconecta.

7.2.2.2 Directrices para la recogida de dispositivos conectados en red

En algunas circunstancias, puede ser conveniente dejar conectados los dispositivos en red para que su actividad pueda ser supervisada y documentada por un DEFR y/o un DES con la debida autoridad. Cuando esto no sea necesario, los dispositivos deberán recogerse como se describe a continuación:

— El DEFR debe aislar el dispositivo de la red, cuando esté seguro de que no se sobrescribirán datos relevantes con esta acción y no se produzcan fallos de funcionamiento en sistemas importantes (como los sistemas de gestión de instalaciones en hospitales). Esto puede hacerse desconectando las conexiones de red por cable al sistema telefónico o puerto de red, o desactivando la conexión al punto de acceso inalámbrico.

— Antes de desenchufar las redes cableadas, el DEFR debe rastrear las conexiones a los dispositivos digitales y etiquetar los puertos para una futura reconstrucción de toda la red. Un dispositivo puede tener más de un método de comunicación. Por ejemplo, un ordenador puede tener redes LAN cableadas, un módem inalámbrico y tarjetas de telefonía móvil. Los PED también pueden estar conectados a la red mediante Wi-Fi, conexiones Bluetooth o conexiones de red de telefonía móvil. El DEFR debe intentar identificar todos los métodos de comunicación y llevar a cabo las actividades apropiadas para protegerse contra la destrucción de posibles pruebas digitales.

— Tenga en cuenta que la desconexión de los dispositivos conectados a la red en este punto puede destruir datos volátiles como procesos en ejecución, conexiones de red y datos almacenados en la memoria. El sistema operativo anfitrión puede ser poco fiable y proporcionar información falsa. El DEFR debe capturar esta información utilizando métodos

de confianza antes de desconectar la alimentación de los dispositivos. Una vez que el DEFR esté seguro de que no se perderá ninguna prueba digital potencial como consecuencia de ello, se pueden retirar las conexiones de los dispositivos digitales.

— Si la recopilación tiene prioridad sobre la adquisición y se sabe que el dispositivo contiene memoria volátil, el dispositivo deberá estar conectado continuamente a una fuente de alimentación.

— Si el dispositivo móvil está apagado, embálelo, séllelo y etiquételo con cuidado. Así se evitará cualquier manipulación accidental o deliberada de las teclas o botones. Como medida de precaución, DEFR también debería considerar el uso de las cajas de Faraday o blindadas.

— En algunas circunstancias, los dispositivos móviles deben apagarse en el momento de la recogida para evitar que se modifiquen los datos. Esto puede ocurrir a través de la conexión saliente y entrante o de comandos que pueden causar la destrucción de posibles pruebas digitales.

— Posteriormente, cada dispositivo digital puede tratarse como si fuera un dispositivo independiente (véase la cláusula 7.1) hasta que sea examinado. Durante el examen, debe considerarse como un dispositivo en red.

NOTA Es posible implementar una forma de red utilizando dispositivos de almacenamiento extraíbles como medio de transmisión. El DEFR deberá considerar si los dispositivos que se están recogiendo pueden haber sido utilizados de este modo y buscar información sobre los demás dispositivos de dicha red.

7.2.2.3 Directrices para la adquisición de dispositivos en red

En la situación en la que los dispositivos están conectados a una red, existe la posibilidad de que los dispositivos 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, de hecho, estar ejecutando una red privada virtual (VPN) y una máquina virtual con más de una (1) dirección IP. Por ello, antes de desconectar el dispositivo de la red, el DEFR debe realizar una adquisición lógica de los datos relacionados con la conexión de red lógica (por ejemplo, la conectividad a Internet). Los datos relacionados incluyen, entre otros, la configuración IP y las tablas de enrutamiento.

En el caso de un dispositivo de red que deba estar continuamente encendido, deberá impedirse que dicho dispositivo interactúe con la red de radio inalámbrica, incluidos los dispositivos habilitados para GPS. El DEFR debe utilizar métodos permitidos por la legislación local para aislar las señales de radio. Sin embargo, se debe tener cuidado de garantizar que el dispositivo tenga una fuente de alimentación adecuada, ya que los métodos de aislamiento pueden hacer que utilice energía adicional en un intento de ponerse en contacto con una red. Los métodos de aislamiento pueden incluir, entre otros, los siguientes:

— Utilizar un dispositivo de interferencia capaz de bloquear la transmisión mediante la creación de fuertes interferencias cuando el dispositivo emite señales en la misma gama de frecuencias que utilizan los dispositivos móviles.

NOTA 1 El uso de dispositivos de interferencia puede infringir los requisitos legales de algunas jurisdicciones.

NOTA 2 El uso de dispositivos de interferencia puede afectar negativamente al comportamiento de dispositivos electrónicos como los equipos médicos.

— Utilizar un área de trabajo apantallada para realizar exámenes de forma segura en un lugar fijo. El apantallamiento puede realizarse para toda la zona de trabajo o mediante la instalación de una tienda de Faraday que permita su portabilidad. La introducción de cables en la
Sin embargo, la introducción de cables en la carpa es problemática, ya que sin el aislamiento adecuado pueden comportarse como una antena, anulando el propósito de la carpa. El espacio de trabajo también puede ser muy restrictivo.

— Utilización de un área de trabajo blindada para realizar exámenes de forma segura en un lugar fijo. Se puede utilizar un espacio de trabajo blindado contra radiofrecuencias o un contenedor (una jaula de Faraday) para impedir las conexiones a la red.

NOTA 3 Todos los métodos de bloqueo del acceso inalámbrico a las redes deben validarse para su uso en las frecuencias adecuadas. Esta validación debe extenderse a los cables que atraviesan el apantallamiento.

— Utilizar una (U)SIM sustitutiva que imite la identidad del dispositivo original e impida el acceso del dispositivo a la red. Estas tarjetas son capaces de engañar al dispositivo para que las acepte como la (U)SIM original y permiten realizar exámenes de forma segura en cualquier lugar. La (U)SIM debe validarse para el dispositivo y la
red antes de su uso.

— Desactivar los servicios de red acordándolo con el operador de servicios móviles e identificando los detalles de los servicios que se van a desactivar (por ejemplo, el identificador del equipo, el identificador del abonado o el número de teléfono). Sin embargo, esta información no siempre está disponible fácilmente y el proceso de coordinación y confirmación puede imponer retrasos.

El DEFR puede realizar una adquisición en vivo del dispositivo móvil antes de retirar la batería (por ejemplo, para acceder a la tarjeta SIM). Esto puede hacerse para evitar la pérdida de información potencialmente importante en la memoria RAM del teléfono o para agilizar el proceso de examen (por ejemplo, cuando se crea que el dispositivo puede estar protegido por un PIN y/o PUK cuya obtención llevaría mucho tiempo).

NOTA 4 El DEFR deberá asegurarse de que la recogida y adquisición de posibles pruebas digitales se realiza de conformidad con las leyes y reglamentos de la jurisdicción local, según se requiera en función de las circunstancias específicas.

7.2.2.4 Directrices para la conservación de dispositivos en red

Debido a la naturaleza de los dispositivos digitales y de las pruebas digitales potenciales, las directrices para la preservación de dispositivos en red son similares a las de la preservación de ordenadores, dispositivos periféricos y medios de almacenamiento digital. Consulte la cláusula 7.1.4 para obtener orientaciones detalladas sobre la preservación de dispositivos.

7.3 Recogida, adquisición y conservación de CCTV

El DEFR debe entender que el enfoque para extraer secuencias de vídeo de un sistema de vídeovigilancia basado en ordenador o en DVR incorporado es diferente de la extracción convencional de pruebas digitales de un ordenador. A continuación se ofrecen directrices específicas para la adquisición de posibles pruebas digitales de sistemas de CCTV:

— Antes de iniciar el proceso de adquisición, el DEFR debe determinar en primer lugar si el sistema ha documentado la secuencia de vídeo de interés. A continuación, el DEFR debe determinar el marco temporal de la secuencia de vídeo necesaria y comparar la hora del sistema con la hora correcta, anotando cualquier desfase. El DEFR
también deberá determinar qué cámaras se necesitan y si pueden adquirirse por separado. El DEFR deberá anotar la marca y el modelo del sistema. Esta información puede ser necesaria para obtener el software de reproducción correcto.

— El DEFR deberá adquirir todas las grabaciones de cámara relevantes durante el tiempo de interés para preservar la información adicional de la investigación que pueda desarrollarse posteriormente. El DEFR deberá tomar nota de todas las cámaras conectadas a un sistema de CCTV y determinar si están grabando activamente o no.

El DEFR deberá determinar el tamaño de almacenamiento del sistema de CCTV, así como cuándo está previsto que el sistema sobrescriba la información de vídeo. Esta información permitirá al DEFR saber cuánto tiempo se conservará la secuencia de vídeo en el sistema antes de que se pierda. Deben tomarse medidas para garantizar que las pruebas no se modifican. En el caso de las pruebas de vídeo digital, es necesario establecer una protección contra escritura.

— El DEFR puede elegir entre varias opciones para obtener posibles pruebas digitales de los sistemas de vídeovigilancia:

1) Adquirir los archivos de vídeo grabándolos en un disco CD/DVD/Blu-ray, pero esto puede no ser práctico si el archivo de vídeo es demasiado grande.

2) Adquirir los archivos de vídeo grabándolos en un medio de almacenamiento externo.

3) Adquirir los archivos de vídeo a través de una conexión de red. Esto puede ser posible si el sistema CCTV está equipado con un puerto de red.

4) Utilice la función de exportación del sistema de vídeovigilancia a otros formatos de archivo (normalmente MPEG o AVI), que es una versión comprimida de las secuencias de vídeo. Esto sólo debe utilizarse como último recurso, ya que la recompresión altera los datos originales y siempre elimina detalles de la imagen. No se recomienda confiar en los datos recomprimidos para su examen si los datos originales existen y están disponibles para su análisis.

NOTA 1 La calidad de las secuencias de vídeo exportadas puede no ser tan buena como la de las secuencias originales.

5) Cuando no sea posible obtener directamente una copia digital de los archivos del dispositivo de grabación, el DEFR o el DES deberán intentar obtener una copia analógica a partir de la salida analógica presente en el dispositivo de grabación original utilizando un dispositivo de grabación analógico adecuado.

— Una vez finalizada la adquisición, deberá comprobarse el archivo adquirido para confirmar que se ha adquirido el archivo correcto o la parte correcta del mismo. El archivo también debe comprobarse con el software del reproductor (para
La mayoría de los sistemas de vídeovigilancia están patentados y los archivos no pueden reproducirse necesariamente con otro software de reproducción. El software de reproducción correcto puede estar disponible para su descarga desde el sistema de CCTV al mismo tiempo que los datos.

— El soporte de almacenamiento digital que contiene el archivo adquirido debe tratarse como la copia maestra de las pruebas digitales. Si el archivo se ha descargado en un ordenador portátil o en una tarjeta de memoria/dispositivo USB, deberá realizarse una copia maestra permanente a partir de ellos lo antes posible.

— A continuación, el DEFR deberá reiniciar el sistema de vídeovigilancia si estaba apagado. Esto debe hacerse e n presencia de la persona autorizada.

En circunstancias en las que no resulta práctico realizar la adquisición en el lugar de los hechos, el DEFR puede tener que decidir recoger los medios de almacenamiento digital. Un método rápido consiste en sustituir el disco duro del sistema de vídeovigilancia por un disco duro virgen o clonado. Sin embargo, el DEFR debe evaluar varios riesgos antes de utilizar este método, como la compatibilidad del nuevo disco duro con el sistema y la compatibilidad del disco duro retirado con otros sistemas para su examen.

NOTA 2 Algunos sistemas tienen un disco duro extraíble en un caddy, pero este disco duro puede requerir el hardware del sistema para su reproducción.

Si no es posible aplicar ninguno de los métodos anteriores, deberá retirarse todo el sistema de vídeovigilancia del lugar de los hechos y el proceso de adquisición deberá llevarse a cabo en el laboratorio forense. Este es el último recurso del DEFR, suponiendo que sea físicamente posible hacerlo, ya que algunos sistemas de CCTV son extremadamente grandes y complejos. Una vez más, el DEFR deberá evaluar los riesgos para las implicaciones legales y el seguro antes de proceder a la retirada.

Debido a la naturaleza de los dispositivos digitales y de las pruebas digitales potenciales, las directrices para la conservación de los sistemas de vídeovigilancia son similares a las de la conservación de ordenadores, dispositivos periféricos y medios de almacenamiento digital. Consulte la cláusula 7.1.4 para obtener orientaciones sobre la conservación de los sistemas de vídeovigilancia.

Anexo A
(informativo)

Descripción de las aptitudes y competencias básicas del DEFR

Tabla A.1 - Ejemplos de descripciones de competencias

No	Competencias básicas	Descripciones de competencias básicas	Descripciones de competencias		
			Conciencia (1)	Conocimiento (2)	Destreza (3)
1	Digital pruebas identificación	Caracterizar de dispositivos digitales, de los componentes, información que puede ayudar a investigación y leyes pertinentes para manejo de posibles pruebas digitales y ordenador delito relacionado. Identificar la herramienta requisitos de recopilación y adquisición de datos y dispositivos y evaluación de riesgos.	Usuario general de TI y administración en múltiples tipos de dispositivos informáticos y dispositivos de red; investigación procedimientos en escena del crimen; determinación de el estado de dispositivo; valor de pruebas información; análisis forense de redes dispositivos relacionados e información.	Registros y sistema/aplicación configuración; identificación de sistema y registros de aplicaciones incluido, el correo electrónico registros, registro web, registros de acceso, archivos de contraseñas, archivos sysconfig, host información IP; funcionalidad del dispositivo y dependencia; capacidad para comprender impacto en volátiles y no volátil pruebas.	Análisis especial; log interpretación para detección de intrusos en identificación de otros sistemas afectados (algunas jurisdicciones exigen confirmación de pruebas presentes antes a la recogida); identificar contraseñas necesarias para los respectivos dispositivos antes de la recogida; identificar la red diagrama y acceso mecanismos de control comprender dependencias; vincular IP direcciones y MAC direcciones para la confirmación.
2	Digital pruebas recogida	Requisitos de la herramienta y aplicación de pruebas digitales embalaje, protección contra medioambiental amenazas. Áreas cubiertos incluyen información garantía.	Datos generales seguridad de la recogida; principios y diseño de pruebas herramientas; determinar el mejor método de recogida a conservar máximo información relevante para el incidente.	Formulación y ejecutar la recogida proceso; recopilar pruebas; generar pruebas documentos; cadena de custodia de pruebas; control de calidad de recogida de pruebas proceso; entrevista sospechoso.	Optimización de proceso de recogida; pruebas documentales que no pueden ser adquiridas debido a diversas limitaciones; recogida de contraseñas, llaves, dongles y otra información necesaria para llevar a cabo análisis en el laboratorio.
3	Digital pruebas adquisición	Aplicar el requisitos de potencial digital pruebas adquisición en forma lógica, garantizando repetibilidad, auditabilidad, reproducibles y defendible. Áreas cubiertas son	Comprender el información disponible en digital dispositivos, bases de datos, sistema generado documentos, usuario datos generados y volatilidad de los datos; Unix y Windows archivo del sistema estructuras y	Saber hacer determinar el almacenamiento requisitos; ejecución de imágenes adquisición procedimiento (por ejemplo digital parcial y total medios de almacenamiento adquisición); adquisición realizadas en un sistema encendido,	Capacidad para realizar adquisición de digital medios de almacenamiento incluyendo RAID, base de datos, aparatos y miniaturizado dispositivos; comprender dependencias y impacto en diferentes método de adquisición.

No	Competencias básicas	Descripciones de competencias básicas	Descripciones de competencias		
			Conciencia (1)	Conocimiento (2)	Habilidad (3)
		adquisición realizada en un accionado en sistema, adquisición realizado en un apagado sistema y forense de redes.	aparatos; conocimiento de impacto en un datos.	adquisición realizada en un sistema apagado; valor hash generación.	
4	Digital pruebas preservación	Aplicar y evaluar requisitos para preservación de potencial digital pruebas, comprender factores y parámetros que influyen en su precisión. Áreas digitales son metodología, mantenimiento de cadena de custodia, dispositivo informático manipulación y almacenamiento digital manipulación de soportes.	Comprender requisitos y procedimientos de conservación de cadena de custodia contra documentos requisitos; medioambientales impacto como humedad, temperatura y choque hacia dispositivo digital; comprender opciones de embalaje, transporte y almacenamiento requisitos.	Saber cómo generación de auditoría de pruebas documentos; definir parámetros para legales; seguridad de la información seguridad, amenazas, vulnerabilidad y controles de pruebas.	Aplicar medidas para preservación digital pruebas, en forma de grandes dispositivos para mano miniaturizados-dispositivos portátiles; procedimiento para pruebas documentales detalles.

Tabla A.2 - Definición de competencias

1	Conciencia - Reconocer, identificar - preguntar cuando se necesita ayuda
2	Conocimientos - Adquiridos mediante formación formal o trabajando en e q u i p o . Contribuir, participar - hacer con ayuda
3	Habilidad - Experiencia demostrada a través de la aplicación en el entorno de trabajo. Trabaja sin supervisión. Aplicar, demostrar - hacer sin ayuda.

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

Anexo B
(informativo)

Requisitos mínimos de documentación para la transferencia de pruebas

El DEFR debe ser responsable de los datos y dispositivos digitales adquiridos en todo momento mientras estén bajo su custodia. Para mantener este control, el DEFR debe estar debidamente autorizado, formado y cualificado. Sin embargo, dado que la legislación local es un factor determinante en la capacidad de un DEFR para cumplir los tres requisitos previstos, la competencia de un DEFR puede variar de una jurisdicción a otra. En consecuencia, es posible que los requisitos de documentación para la transferencia transjurisdiccional de pruebas digitales no sean iguales en las distintas jurisdicciones.

En consecuencia, es necesario especificar un conjunto mínimo de requisitos de documentación para facilitar el intercambio transjurisdiccional de posibles pruebas digitales. Estos requisitos de documentación deben considerarse junto con los puntos de documentación mencionados en la cláusula 6.6. Dado que esta Norma Internacional no sustituye a los requisitos legales específicos de ninguna jurisdicción, sirve como directriz práctica para la transferencia de posibles pruebas digitales a través de las fronteras jurisdiccionales.

La documentación mínima que debe comunicarse es

- el nombre y la dirección de la autoridad pertinente
- una declaración de la autorización, formación y cualificaciones del DEFR
- el propósito del examen
- qué acciones se llevaron a cabo;
- quién hizo qué y cuándo;
- la cadena de custodia relativa a la investigación específica;
- lista descriptiva de las posibles pruebas digitales y soportes de almacenamiento digital recogidos y adquiridos; e
- información relativa a los exámenes, pruebas o investigaciones utilizados para crear la copia de las pruebas.

Los requisitos específicos de cada jurisdicción pueden incluir lo siguiente
- si la prueba se considera un dictamen pericial, el reconocimiento del correspondiente Código de conducta de peritos; y
- una orden judicial que especifique qué documentación debe transferirse y el motivo de la transferencia.

Bibliografía

[1] ILAC-G19:2002. *Directrices para los laboratorios de policía científica.* Disponible en:www.ilac.org/ documents/ g19_2002.pdf

[2] IOCE, G8 *principios propuestos para los procedimientos relativos a pruebas digitales* . Disponible en: http://ioce.org/core.php?ID=5

[3] ISO/IEC 15489:2001, *Información y documentación - Gestión de registros*

[4] ISO/IEC 17024:2003, *Evaluación de la conformidad - Requisitos generales para los organismos de certificación de personas*

[5] ISO/IEC 17043:2010, *Evaluación de la conformidad - Requisitos generales para los ensayos de aptitud*

[6] ISO/IEC 27001, *Información tecnología de la información - Seguridad técnicas - Información Sistemas de gestión de la seguridad de la información - Requisitos*

[7] ISO/IEC 27002, *Información tecnología de la información - Seguridad técnicas - Información Sistemas de gestión de la seguridad de la información - Código de buenas prácticas para la gestión de la seguridad de la información*

[8] ISO/IEC 24760-1, *Tecnología de la información - Técnicas de seguridad - Marco para la gestión de identidades - Parte 1: Terminología y conceptos*

[9] ISO/IEC 27031:2010, *Tecnología de la información - Técnicas de seguridad - Directrices para la preparación de las TIC para la continuidad del negocio*

[10] ISO/IEC 27035:2011, *Tecnología de la información - Técnicas de seguridad - Gestión de incidentes de seguridad de la información*

[11] *Forense Ciencia Sociedad Académico Acreditación Normas & DPC.* Disponible en: http://www.forensic-science-society.org.uk

[12] *Directrices para la recogida y el archivo de pruebas*. Disponible en: http://www.ietf.org/rfc/rfc3227.txt

ICS 035.040

Precio basado en 38 páginas