

NORMA  
BRASILEIRA

ABNT NBR  
ISO/IEC  
27037

Primeira edição  
09.12.2013

Válida a partir de  
09.01.2014

---

**Tecnologia da informação — Técnicas de  
segurança — Diretrizes para identificação, coleta,  
aquisição e preservação de evidência digital**

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



ICS 35.040

ISBN 978-85-07-04691-2



ASSOCIAÇÃO  
BRASILEIRA  
DE NORMAS  
TÉCNICAS

Número de referência  
ABNT NBR ISO/IEC 27037:2013  
42 páginas



© ISO/IEC 2012

Todos os direitos reservados. A menos que especificado de outro modo, nenhuma parte desta publicação pode ser reproduzida ou utilizada por qualquer meio, eletrônico ou mecânico, incluindo fotocópia e microfilme, sem permissão por escrito da ABNT, único representante da ISO no território brasileiro.

© ABNT 2013

Todos os direitos reservados. A menos que especificado de outro modo, nenhuma parte desta publicação pode ser reproduzida ou utilizada por qualquer meio, eletrônico ou mecânico, incluindo fotocópia e microfilme, sem permissão por escrito da ABNT.

ABNT

Av.Treze de Maio, 13 - 28º andar  
20031-901 - Rio de Janeiro - RJ  
Tel.: + 55 21 3974-2300  
Fax: + 55 21 3974-2346  
[abnt@abnt.org.br](mailto:abnt@abnt.org.br)  
[www.abnt.org.br](http://www.abnt.org.br)

Sumário	Página
<b>Prefácio Nacional .....</b>	<b>v</b>
<b>Introdução .....</b>	<b>vii</b>
<b>1 Escopo .....</b>	<b>1</b>
<b>2 Referências normativas .....</b>	<b>1</b>
<b>3 Termos e definições .....</b>	<b>2</b>
<b>4 Termos abreviados .....</b>	<b>4</b>
<b>5 Visão Geral .....</b>	<b>6</b>
<b>5.1 Contexto para coleta evidência digital .....</b>	<b>6</b>
<b>5.2 Princípios da evidência digital .....</b>	<b>6</b>
<b>5.3 Requisitos para o manuseio da evidência digital .....</b>	<b>7</b>
<b>5.3.1 Geral .....</b>	<b>7</b>
<b>5.3.2 Auditabilidade .....</b>	<b>7</b>
<b>5.3.3 Repetibilidade .....</b>	<b>7</b>
<b>5.3.4 Reprodutibilidade .....</b>	<b>8</b>
<b>5.3.5 Justificabilidade .....</b>	<b>8</b>
<b>5.4 Processo de manuseio da evidência digital .....</b>	<b>8</b>
<b>5.4.1 Visão geral .....</b>	<b>8</b>
<b>5.4.2 Identificação .....</b>	<b>9</b>
<b>5.4.3 Coleta .....</b>	<b>9</b>
<b>5.4.4 Aquisição .....</b>	<b>10</b>
<b>5.4.5 Preservação .....</b>	<b>11</b>
<b>6 Principais componentes de identificação, coleta, aquisição e preservação de evidência digital .....</b>	<b>11</b>
<b>6.1 Cadeia de custódia .....</b>	<b>11</b>
<b>6.2 Precauções no local do incidente .....</b>	<b>12</b>
<b>6.2.1 Generalidades .....</b>	<b>12</b>
<b>6.2.2 Pessoal .....</b>	<b>13</b>
<b>6.2.3 Potencial evidência digital .....</b>	<b>13</b>
<b>6.3 Papéis e responsabilidades .....</b>	<b>13</b>
<b>6.4 Competência .....</b>	<b>14</b>
<b>6.5 Utilizar cuidado razoável .....</b>	<b>14</b>
<b>6.6 Documentação .....</b>	<b>15</b>
<b>6.7 Instruções .....</b>	<b>16</b>
<b>6.7.1 Geral .....</b>	<b>16</b>
<b>6.7.2 Evidência digital específica .....</b>	<b>16</b>
<b>6.7.3 Pessoal específico .....</b>	<b>17</b>
<b>6.7.4 Incidentes em tempo real .....</b>	<b>17</b>
<b>6.7.5 Outras informações nas instruções .....</b>	<b>17</b>
<b>6.8 Priorizando coleta e aquisição .....</b>	<b>18</b>
<b>6.9 Preservação da potencial evidência digital .....</b>	<b>19</b>
<b>6.9.1 Visão geral .....</b>	<b>19</b>

6.9.2	Preservando a potencial evidência digital .....	19
6.9.3	Acondicionando dispositivos digitais e potencial evidência digital .....	19
6.9.4	Transportando potencial evidência digital .....	21
7	Instâncias de identificação, coleta, aquisição e preservação.....	21
7.1	Computadores, dispositivos periféricos e mídias de armazenamento digital .....	21
7.1.1	Identificação .....	21
7.1.2	Coleta .....	24
7.1.3	Aquisição .....	28
7.1.4	Preservação .....	32
7.2	Dispositivos de rede .....	33
7.2.1	Identificação .....	33
7.2.2	Coleta, aquisição e preservação .....	35
	<b>Bibliografia.....</b>	<b>42</b>

**Anexos**

<b>Anexo A</b> (informativo) <b>DEFR — Competências essenciais e descrição de competências .....</b>	<b>38</b>
<b>Anexo B</b> (informativo) <b>Requisitos mínimos de documentação para transferência de evidência.....</b>	<b>41</b>

**Figuras**

<b>Figura 1 – Diretrizes para tomada de decisão para coleta ou aquisição da potencial evidência digital .....</b>	<b>24</b>
<b>Figura 2 – Diretrizes para coleta de dispositivo digital ligado .....</b>	<b>25</b>
<b>Figura 3 – Diretrizes para coleta de dispositivo digital desligado.....</b>	<b>27</b>
<b>Figura 4 – Diretrizes para aquisição de dispositivo digital ligado.....</b>	<b>29</b>
<b>Figura 5 – Diretrizes para aquisição de dispositivo digital desligado .....</b>	<b>31</b>

**Tabelas**

<b>Tabela A.1 – Exemplos de descrição de competências.....</b>	<b>38</b>
<b>Tabela A.2 – Definição de competências .....</b>	<b>40</b>

## Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

Os Documentos Técnicos ABNT são elaborados conforme as regras da Diretiva ABNT, Parte 2.

A Associação Brasileira de Normas Técnicas (ABNT) chama atenção para a possibilidade de que alguns dos elementos deste documento podem ser objeto de direito de patente. A ABNT não deve ser considerada responsável pela identificação de quaisquer direitos de patentes.

A ABNT NBR ISO/IEC 27037 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Técnicas de Segurança (CE-21:027.00). O Projeto circulou em Consulta Nacional conforme Edital nº 08, de 30.08.2013 a 30.09.2013, com o número de Projeto 21:027.00-029.

Esta Norma é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 27037:2012, *que foi elaborada pelo Join Technical Committee Information Technology (ISO/IEC JTC 1), Subcommittee IT Security Techniques (SC 27), ISO/IEC Guide 21-1:2005.*

O Escopo desta Norma Brasileira em inglês é o seguinte:

### **Scope**

*This Standard provides guidelines for specific activities in handling digital evidence, which are identification, collection, acquisition and preservation of digital evidence that may be of evidential value. This Standard provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.*

*This Standard gives guidance for the following devices and/or functions that are used in various circumstances:*

- *Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions,*
- *Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards,*
- *Mobile navigation systems,*
- *Digital still and video cameras (including CCTV),*
- *Standard computer with network connections,*
- *Networks based on TCP/IP and other digital protocols, and*
- *Devices with similar functions as above.*

*NOTE 1 The above list of devices is an indicative list and not exhaustive.*

*NOTE 2 Circumstances include the above devices that exist in various forms. For example, an automotive system may include mobile navigation system, data storage and sensory system.*



## Introdução

Esta Norma fornece diretrizes para atividades específicas no tratamento de potenciais evidências digitais; esses processos são: identificação, coleta, aquisição e preservação de potenciais evidências digitais. Esses processos são necessários em uma investigação designada para preservar a integridade da evidência digital – uma metodologia aceitável na obtenção de evidência digital que contribuirá para a sua admissibilidade em processos judiciais e disciplinares, bem como em outras instâncias necessárias. Esta Norma também fornece diretrizes gerais para a coleta de evidência não digital capaz de auxiliar no estágio de análise da potencial evidência digital.

Esta Norma pretende fornecer diretrizes às pessoas responsáveis pela identificação, coleta, aquisição e preservação da potencial evidência digital. Essas pessoas incluem os Primeiros Interventores da Evidência Digital (DEFR), Especialistas em Evidência Digital (DES), especialistas em respostas a incidentes e gestores de laboratório na área forense. Esta Norma assegura que os indivíduos responsáveis gerenciem a potencial evidência digital por meio de métodos práticos aceitáveis mundialmente, com o objetivo de facilitar a investigação envolvendo dispositivos digitais e evidências digitais de um modo sistemático e imparcial, preservando a sua integridade e autenticidade.

Esta Norma também pretende informar os tomadores de decisões que precisam determinar a confiabilidade das evidências digitais que lhes são apresentadas. Ela é aplicável a organizações que necessitam proteger, analisar e apresentar potenciais evidências digitais. Ela é relevante para organismos responsáveis pela elaboração de políticas que criam e avaliam procedimentos relativos a evidências digitais, muitas vezes como parte de um conjunto de evidências mais amplo.

A potencial evidência digital referida nesta Norma pode originar-se de diferentes tipos de dispositivos digitais, redes, banco de dados etc. Ela refere-se a dados que já estão em formato digital. Esta Norma não tem a intenção de abranger a conversão de dados analógicos para o formato digital.

Devido à fragilidade da evidência digital, é necessário realizar uma metodologia aceitável para garantir a integridade e autenticidade da potencial evidência digital. Esta Norma não ordena o uso de ferramentas ou métodos particulares. Os principais componentes que fornecem credibilidade à investigação são a metodologia aplicada durante o seu processo e as pessoas qualificadas na execução das tarefas especificadas na metodologia. Esta Norma não trata de metodologias para procedimentos judiciais, procedimentos disciplinares e outras ações relacionadas ao manuseio de potenciais evidências digitais que estão além do escopo de identificação, coleta, aquisição e preservação de potenciais evidências digitais.

A aplicação desta Norma requer conformidade com leis, regras e regulamentos nacionais. É recomendado que ela não substitua exigências legais de qualquer jurisdição. Em vez disso, ela pode servir de diretriz prática para qualquer DEFR ou DES em investigações envolvendo potenciais evidências digitais. Esta Norma não se estende à análise de evidências digitais e não substitui requisitos específicos de jurisdições no que tange a admissibilidade, força probatória, relevância e outras limitações controladas judicialmente no uso de potenciais evidências digitais perante os tribunais. Esta Norma pode auxiliar na facilitação do intercâmbio de potenciais evidências digitais entre diferentes jurisdições. A fim de manter a integridade da evidência digital, usuários desta Norma são requisitados a adaptar e aperfeiçoar os procedimentos descritos nesta Norma de acordo com requerimentos legais específicos da jurisdição do usuário.

Apesar de esta Norma não possuir prontidão forense, tal prontidão forense pode apoiar amplamente o processo de identificação, coleta, aquisição e preservação de evidências digitais. Prontidão forense é o alcance de um nível apropriado de capacidade de uma organização a fim de que ela possa identificar, coletar, adquirir, preservar, proteger e analisar a evidência digital. Considerando que

os processos e atividades descritas nesta Norma são essencialmente medidas reativas usadas para investigação de um incidente depois de ocorrido, prontidão forense é um processo proativo de tentativa de planejar tal evento.

Esta Norma complementa a ABNT NBR ISO/IEC 27001 e a ABNT NBR ISO/IEC 27002, e, em particular, os requisitos de controle sobre a aquisição de potencial evidência digital, fornecendo diretrizes adicionais de implementação. Ainda, esta Norma terá aplicação em contextos independentes das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002. Convém que esta Norma seja lida em conjunto com outras normas relativas à evidência digital e à investigação de incidentes de segurança da informação.



# Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital

## 1 Escopo

Esta Norma fornece diretrizes para atividades específicas no manuseio de evidências digitais que são a identificação, coleta, aquisição e preservação de evidência digital que possam possuir valor probatório. Esta Norma fornece diretrizes para pessoas em relação às situações comuns encontradas durante o processo de manuseio da evidência digital e auxilia organizações em seus procedimentos disciplinares e na facilitação de intercâmbio de potenciais evidências digitais entre jurisdições.

Esta Norma fornece diretrizes para os seguintes dispositivos e/ou funções que são utilizadas em várias circunstâncias:

- Meios de armazenamento digitais usados em computadores, como discos rígidos, disquetes, discos ópticos e magneto-ópticos, dispositivos de dados com funções semelhantes,
- Telefones móveis, assistentes digitais pessoais (PDA), dispositivos eletrônicos pessoais (PED), cartões de memória,
- Sistemas de navegação móveis,
- Câmeras digitais de vídeo e fotografias (incluindo CFTV),
- Computadores-padrão com conexões de rede,
- Redes baseadas em TCP/IP e outros protocolos digitais, e
- Dispositivos com funções semelhantes das descritas acima.

NOTA 1 A lista acima de aparelhos é uma lista indicativa e não é exaustiva.

NOTA 2 Circunstâncias incluem os dispositivos acima citados existentes em várias formas. Por exemplo, um sistema automotivo pode incluir sistema de navegação móvel, sistema de armazenamento de dados e sistema sensorial.

## 2 Referências normativas

Os documentos relacionados a seguir são indispensáveis para aplicação desta Norma. Para referências datadas, somente a edição citada se aplica. Para referências não datadas, aplica-se a última edição do documento referenciado (incluindo as emendas).

ABNT NBR ISO/IEC 17020, *Avaliação de conformidade – Requisitos para o funcionamento de diferentes tipos de organismos que executam inspeção*

ABNT NBR ISO/IEC 17025:2005, *Requisitos gerais para a competência de laboratórios de ensaio e calibração*

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

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

### 3 Termos e definições

Para os efeitos deste documento, aplicam-se os termos e definições da ISO/IEC 27000, ABNT NBR ISO/IEC 17020, ABNT NBR ISO/IEC 17025 e ISO/TR 15801 e os seguintes.

#### 3.1

##### **aquisição**

processo de criação de cópia de dados em um conjunto definido

NOTA O produto de uma aquisição é uma cópia de uma potencial evidência digital.

#### 3.2

##### **espaço alocado**

área de mídia digital, incluindo memória principal, que está em uso para armazenamento de dados, incluindo metadados

#### 3.3

##### **coleta**

processo de recolhimento de itens físicos que contêm potencial evidência digital

#### 3.4

##### **dispositivo digital**

equipamento eletrônico usado para processar ou armazenar dado digital

#### 3.5

##### **evidência digital**

informações ou dados, armazenados ou transmitidos em forma binária, que podem ser invocados como evidência

#### 3.6

##### **cópia de evidência digital**

cópia de evidência digital que foi produzida para manter a confiabilidade da evidência, incluindo tanto a evidência digital como os meios de verificação no qual o método de verificação pode ser incorporado ou ser independente das ferramentas utilizadas na verificação

#### 3.7

##### **Primeiro Interventor da Evidência Digital**

##### **DEFR**

pessoa que está autorizada, treinada e qualificada para agir primeiro no local do incidente, na execução da coleta e aquisição da evidência digital, responsabilizando-se pelo seu manuseio

NOTA Autoridade, treinamento e qualificação são os requisitos necessários esperados para produzir evidência digital confiável, mas circunstâncias particulares podem resultar em uma pessoa que não siga os três requisitos. Nestes casos, é recomendado que sejam consideradas a legislação local, a política organizacional e as circunstâncias particulares.

#### 3.8

##### **Especialistas em Evidência Digital**

##### **DES**

indivíduo que pode executar tarefas de um DEFR e possui um conhecimento especializado, aptidão e habilidade para lidar com uma ampla gama de questões técnicas

NOTA Um DES pode possuir conhecimentos adicionais de um segmento, por exemplo, rede de aquisições, aquisição de memória RAM, sistemas operacionais ou conhecimento em *Mainframe*.

**3.9****mídia de armazenamento digital**

dispositivo no qual dados digitais podem ser gravados

[Adaptado da ISO/IEC 10027:1990]

**3.10****instalações de preservação de evidências**

ambiente seguro ou um local onde as evidências coletadas ou adquiridas são armazenadas

**NOTA** É recomendado que uma instalação de preservação de evidências não seja exposta a campo magnético, poeiras, vibrações, umidade ou quaisquer elementos ambientais (como extrema temperatura ou umidade) que podem danificar a potencial evidência digital inserida na instalação.

**3.11****valor de hash**

série de bits que são o resultado da função *hash*

[ISO/IEC 10118-1:2000]

**3.12****identificação**

processo envolvendo a busca, reconhecimento e documentação da potencial evidência digital

**3.13****imagem**

processo de criação de uma cópia bit a bit de mídias de armazenamento digital

**NOTA** A cópia bit a bit também é chamada de cópia física.

**EXEMPLO** Quando se faz a imagem de um disco rígido, o DEFR também pode copiar os dados que foram apagados.

**3.14****periférico**

dispositivo anexado a dispositivo digital para expandir a sua funcionalidade

**3.15****preservação**

processo para manter e proteger a integridade e/ou a condição original da potencial evidência digital

**3.16****confiabilidade**

propriedade de resultados e comportamentos pretendidos consistentes

[ISO/IEC 27000:2009]

**3.17****repetibilidade**

propriedade de um processo conduzido para obter os mesmos resultados de testes em um mesmo ambiente de teste (mesmo computador, disco rígido, modo de operação etc.)

**3.18****reprodutibilidade**

propriedade de um processo para obter os mesmos resultados de testes em um diferente ambiente de teste (diferente computador, disco rígido, operador etc.)

**3.19**

**espoliação**

ato de realizar ou permitir alteração(ões) na potencial evidência digital que diminui o seu valor probatório

**3.20**

**tempo de sistema**

tempo gerado pelo relógio do sistema e usado pelo sistema operacional, não o tempo computado pelo sistema operacional

**3.21**

**adulteração**

ato de deliberadamente realizar ou permitir alteração(ões) na potencial evidência digital (isto é, intencionalmente ou espoliação intencional)

**3.22**

**carimbo de tempo**

parâmetro de variação do tempo que indica o momento específico que diz respeito a uma referência de tempo comum

[ISO/IEC 11770-1:1996]

**3.23**

**espaço não alocado**

área na mídia digital, incluindo memória principal, que não foi alocada pelo sistema operacional e que está disponível para o armazenamento de dados, incluindo metadados

**3.24**

**validação**

comprovação, por meio do fornecimento de evidências objetivas, de que os requisitos para um específico uso ou aplicação tenham sido atendidos

[ABNT NBR ISO/IEC 27004:2010]

**3.25**

**função de verificação**

função que é usada para verificar dois conjuntos de dados são idênticos

NOTA 1 Convém que dois conjuntos de dados não idênticos não produzam uma combinação idêntica a partir de uma função de verificação

NOTA 2 Funções de verificação são comumente implementadas utilizando funções *hash* como MD5, SHA1 etc., mas outros métodos podem ser utilizados.

**3.26**

**dados voláteis**

dados que são especialmente propensos a alteração e que podem ser facilmente modificados

NOTA Uma alteração pode se dar pelo desligamento de energia ou por passar por um campo magnético. Dados voláteis também incluem dados que se alteram por alterações do estado do sistema. Exemplos incluem dados armazenados em memória RAM e em endereços de IP dinâmicos.

## 4 Termos abreviados

**AVI** Áudio Vídeo Intercalado

<b>CCTV</b>	Círculo Fechado de Televisão
<b>CD</b>	Disco Compacto
<b>DNA</b>	Ácido Desoxirribonucleico
<b>DEFR</b>	Primeiro Interventor da Evidência Digital
<b>DES</b>	Especialista em Evidência Digital
<b>DVD</b>	Vídeo digital/Disco versátil
<b>ESN</b>	Número Serial Eletrônico
<b>GPS</b>	Sistema Global de Posicionamento
<b>GSM</b>	Sistema Global para Comunicações Móveis
<b>IMEI</b>	Identificação Internacional de Equipamento Móvel
<b>IP</b>	Protocolo de Internet
<b>ISIRT</b>	Grupo de Respostas a Incidentes de Segurança da Informação
<b>LAN</b>	Rede de Área Local
<b>MD5</b>	Mensagem de Resumo, Algarismo 5
<b>MP3</b>	MPEG Camada de Áudio 3
<b>MPEG</b>	Grupo de Especialistas em Imagens com Movimento
<b>NAS</b>	Armazenamento Anexado à Rede
<b>PDA</b>	Assistente Pessoal Digital
<b>PED</b>	Dispositivo Eletrônico Pessoal
<b>PIN</b>	Número de Identificação Pessoal
<b>PUK</b>	Código de Desbloqueio de PIN
<b>RAID</b>	Conjunto Redundante de Discos Independentes
<b>RAM</b>	Memória de Acesso Aleatório
<b>RFID</b>	Identificação por Radiofrequênci
<b>SAN</b>	Rede de Área de Armazenamento
<b>SHA</b>	Algoritmo de <i>Hash</i> Seguro
<b>SIM</b>	Módulo de Identificação de Assinante

<b>USB</b>	<i>Universal Serial Bus</i>
<b>UPS</b>	Fonte de Alimentação Ininterrupta
<b>USIM</b>	Módulo Universal de Identificação de Assinante
<b>UV</b>	Ultravioleta
<b>Wi-Fi</b>	Fidelidade Rede sem Fio

## 5 Visão Geral

### 5.1 Contexto para coleta evidência digital

Pode ser necessário evidência digital para o uso em cenários distintos, sendo que cada cenário possui diferente equilíbrio entre os condutores da qualidade probatória, na análise oportunamente, na restauração do serviço e no custo da coleta da evidência digital. Portanto, será exigido que as organizações tenham um processo de priorização que identifique as necessidades e equilibre a qualidade probatória, a oportunidade e a restauração do serviço antes de atribuir tarefas aos recursos do DEFR. O processo de priorização envolve efetuar uma avaliação do material disponível para determinar o possível valor probatório e a ordem na qual convém que a potencial evidência digital seja coletada, adquirida ou preservada. A priorização é executada para minimizar o risco de a potencial evidência digital ser espoliada e maximizar o seu valor probatório.

### 5.2 Princípios da evidência digital

Em muitas jurisdições e organizações, evidência digital é governada por três princípios fundamentais: relevância, confiabilidade e suficiência. Estes três princípios são importantes para todas as investigações, não apenas para que aquelas evidências digitais sejam admitidas nos tribunais. A evidência digital é relevante quando se destina a provar ou refutar um elemento de um caso específico que está sendo investigado. Embora a definição detalhada de “confiança” altere-se entre jurisdições, o significado geral do princípio “para garantir que a evidência digital seja o que pretende ser” é amplamente defendido. Nem sempre é necessário ao DEFR coletar todos os dados ou realizar uma completa cópia da evidência digital original. Em muitas jurisdições, o conceito de suficiência significa que o DEFR precisa coletar potencial evidência digital suficiente para permitir que elementos da questão sejam adequadamente examinados ou investigados. O entendimento deste conceito é importante para o DEFR priorizar o esforço apropriado quando o tempo ou o custo são preocupações.

**NOTA** É recomendado que o DEFR assegure que a coleta da potencial evidência digital está de acordo com as leis e regulamentos da jurisdição local, bem como com os requisitos das circunstâncias específicas.

Convém que todos os processos a serem utilizados pelo DEFR e DES tenham sido validados antes das suas utilizações. Se a validação é executada externamente, convém que o DEFR ou DES verifique se a validação é apropriada para o uso específico do processo e no meio e nas circunstâncias } em que o processo está prestes a ser utilizado. É recomendado ao DEFR ou ao DES também:

- a) documentar todas as ações;
- b) determinar e aplicar um método para estabelecer a exatidão e confiança da cópia da potencial evidência digital comparada com a fonte original; e
- c) reconhecer que não é possível que o ato de preservação da potencial evidência digital seja sempre não intrusivo.

## 5.3 Requisitos para o manuseio da evidência digital

### 5.3.1 Geral

Os princípios previstos em 5.2 acima podem ser satisfeitos das seguintes maneiras:

- Relevância: É recomendado que seja possível demonstrar que o material adquirido é relevante para a investigação, ou seja, que contém informação de valor no auxílio à investigação de um incidente particular e de que há uma boa razão para ter sido adquirida. Por meio da auditoria e justificação, é recomendado que o DEFR seja capaz de descrever os procedimentos seguidos e esclarecer como a decisão para adquirir cada item foi obtida.
- Confiabilidade: É recomendado que todos os processos utilizados no manuseio da potencial evidência digital sejam passíveis de auditoria e repetições. Convém que os resultados da aplicação destes processos sejam reproduzíveis; Suficiência: É recomendado que o DEFR tenha levado em consideração que material suficiente foi recolhido para permitir a adequada execução da investigação. Convém que o DEFR seja capaz, por meio de auditoria e justificativa, de indicar quanto material, ao todo, foi considerado e quais os procedimentos utilizados para decidir o quanto e qual material foi adquirido.

**NOTA** Os materiais podem ser recolhidos por meio de aquisição e/ou atividades de coleta.

Há quatro aspectos-chave no manuseio da evidência digital: auditabilidade, justificabilidade e repetibilidade ou reproduzibilidade, dependendo das circunstâncias particulares.

### 5.3.2 Auditabilidade

Convém que seja possível para um assistente independente ou outra parte autorizada interessada avaliar as atividades realizadas por um DEFR e DES. Isto se torna possível por meio de adequada documentação de todas as ações realizadas. Recomenda-se que os DEFR e DES sejam capazes de justificar o processo de tomada de decisão para escolha de um determinado curso de ação. É recomendado que os processos realizados pelos DEFR e DES estejam disponíveis para avaliação independente com o intuito de determinar se o método científico, a técnica ou o procedimento foi adequadamente seguido.

### 5.3.3 Repetibilidade

A repetibilidade é estabelecida quando os mesmos resultados de testes são produzidos sob as seguintes condições:

- Utilizando os mesmos procedimentos e métodos de medição;
- Utilizando os mesmos instrumentos e sob as mesmas condições; e
- Pode ser repetido a qualquer tempo depois do teste original.

Convém que um hábil e experiente DEFR seja capaz de realizar todos os processos descritos na documentação e de alcançar os mesmos resultados, sem orientação ou interpretação. É recomendado que o DEFR esteja atento a possíveis circunstâncias em que não será possível repetir o teste, por exemplo, quando um disco rígido original foi copiado e voltou a ser utilizado, ou quando um item envolve memória volátil. Nestes casos, convém que o DEFR assegure que o processo de aquisição é confiável. Para alcançar a repetibilidade, recomenda-se que o controle de qualidade e a documentação do processo estejam em ordem.

### 5.3.4 Reprodutibilidade

A reprodutibilidade é estabelecida quando os mesmos resultados de testes são produzidos sob as seguintes condições:

- Utilizando os mesmos métodos de medição;
- Utilizando diferentes instrumentos e sob diferentes condições; e
- Pode ser reproduzido a qualquer tempo depois do teste original.

As necessidades de reproduzir os resultados variam de acordo com as jurisdições e circunstâncias, então o DEFR ou o indivíduo que está realizando a reprodução necessitará ser informado sobre as condições aplicáveis.

### 5.3.5 Justificabilidade

É recomendado que o DEFR seja capaz de justificar todas as ações e métodos utilizados para o manuseio da potencial evidência digital. A justificativa pode ser alcançada demonstrando que a decisão foi a melhor escolha para obter toda a potencial evidência digital. Qualquer DEFR ou DES poderia, também, demonstrar isto, reproduzindo com sucesso ou validando as ações ou métodos utilizados.

É para o bem da organização empregar um DEFR ou DES que possua habilidades e competências essenciais como descritas no Anexo A desta Norma. Isto assegurará que processos e procedimentos corretos são seguidos no manuseio da potencial evidência digital para garantir a eventual preservação da evidência digital que pode ter valor probatório. Isto também garantirá que organizações sejam capazes de utilizar a potencial evidência digital, por exemplo, em seus procedimentos disciplinares ou facilitando a troca de potencial evidência digital entre jurisdições.

**NOTA** A competência descrita no Anexo A está limitada à função do DEFR, a qual está alinhada com a função do DES, como definido em 3.8.

## 5.4 Processo de manuseio da evidência digital

### 5.4.1 Visão geral

Embora o completo processo de manuseio da evidência digital inclua outras atividades (por exemplo, apresentação, disposição), o escopo desta Norma refere-se somente ao processo inicial de manuseio da evidência digital, o qual consiste na identificação, coleta, aquisição e preservação da potencial evidência digital.

Evidência digital pode ser frágil na sua natureza. Ela pode ser alterada, adulterada ou destruída por manuseio ou exame impróprio. É recomendado que manuseadores da evidência digital sejam competentes para identificar e administrar os riscos e consequências advindos de possíveis linhas de conduta quando tratam com a evidência digital. Falha em manusear dispositivos digitais adequadamente podem tornar a potencial evidência digital contida naqueles dispositivos digitais inutilizáveis.

Convém que os DEFR e DES sigam os procedimentos documentados para garantir que a integridade e a confiabilidade da potencial evidência digital sejam mantidas. É recomendado que os procedimentos incluam diretrizes de manuseio para fontes de potencial evidência digital e que incluam os seguintes princípios fundamentais:

- Minimizar o manuseio do dispositivo digital original ou da potencial evidência digital;

- Considerar quaisquer alterações e documentar ações tomadas (na medida em que um especialista seja capaz de formar uma opinião sobre a confiabilidade);
- Estar de acordo com as regras de evidência locais; e
- Não é recomendado que os DEFR e DES adotem ações além de suas competências.

Ao cumprir os princípios fundamentais e requisitos para o manuseio da potencial evidência digital, recomenda-se que a evidência seja preservada. Especificamente nos casos em que é recomendado que alterações inevitáveis sejam realizadas, é necessário que todas as ações e análises racionais sejam documentadas. Cada processo de manuseio da evidência digital, por exemplo, identificação, coleta, aquisição e preservação, é discutido com mais detalhes nas seções que seguem.

#### **5.4.2 Identificação**

Evidência digital é representada na forma física e lógica. A forma física inclui a representação de dados dentro de um dispositivo tangível. A forma lógica da potencial evidência digital refere-se à representação virtual dos dados dentro do dispositivo.

O processo de identificação envolve a pesquisa, reconhecimento e documentação da potencial evidência digital. Convém que o processo de identificação identifique o armazenamento da mídia digital e os dispositivos de processamento que podem conter a potencial evidência digital relevante para o incidente. Este processo também inclui uma atividade para priorizar a coleta da evidência baseada em sua volatilidade. Recomenda-se que a volatilidade dos dados seja identificada para garantir a correta ordem dos processos de coleta e aquisição para minimizar o dano à potencial evidência digital e para obter a melhor evidência. Adicionalmente, convém que o processo identifique a possibilidade de uma potencial evidência digital oculta. Recomenda-se que os DEFR e DES estejam atentos que nem todos os tipos de mídia de armazenamento digital podem ser facilmente identificados e localizados, por exemplo, computação em nuvem, NAS e SAN – todos adicionam um componente virtual ao processo de identificação.

É recomendado que o DEFR execute sistematicamente uma pesquisa completa dos itens que podem conter potencial evidência digital. Diferentes tipos de dispositivos digitais podem conter potenciais evidências digitais que, por sua vez, podem facilmente passar despercebidos (por exemplo, devido ao pequeno tamanho), disfarçadas ou mescladas entre outros materiais irrelevantes.

Em 6.1 e 6.6 são fornecidas mais informações sobre a cadeia de custódia, acondicionamento e aspectos de rotulagem da identificação da evidência digital. A Seção 7 especifica diretrizes relevantes para instâncias específicas de identificação, coleta, aquisição e preservação da evidência digital.

#### **5.4.3 Coleta**

Uma vez que os dispositivos digitais que podem conter potencial evidência digital são identificados, convém que os DEFR e DES decidam se efetuam a coleta ou aquisição durante o próximo processo. Há uma série de fatores de decisão para isso, que é discutida em mais detalhes na Seção 7. É recomendado que a decisão seja baseada em circunstâncias.

Coleta é um processo que integra o processo de manuseio da evidência digital, no qual dispositivos que podem conter potencial evidência digital são removidos de sua localização original para um laboratório ou outro ambiente controlado para posterior aquisição e análise. Dispositivos contendo potencial evidência digital podem estar em um dos dois estados: quando o sistema está ligado ou quando o sistema está desligado. Diferentes abordagens e ferramentas são necessárias, dependendo do estado do dispositivo. Procedimentos locais podem ser aplicáveis às abordagens e ferramentas utilizadas para o processo de coleta.

Este processo inclui a documentação de toda abordagem, bem como o acondicionamento destes dispositivos antes do transporte. É importante aos DEFR e DES coletar qualquer material que possa estar relacionado à potencial informação digital (por exemplo, papel com senhas anotadas, suporte e conectores de energia para dispositivos de sistemas embutidos). A potencial evidência digital pode ser perdida ou danificada se cuidados razoáveis não forem aplicados. Convém que os DEFR e DES adotem o melhor método de coleta possível, baseado na situação, custo e tempo, e documentem a decisão para o uso de um método particular.

NOTA 1 A remoção da mídia de armazenamento digital nem sempre é recomendada, e convém que o DEFR esteja seguro de que é competente para remover a mídia de armazenamento e reconhecer quando é apropriado e permitido para tanto.

NOTA 2 É recomendado que detalhes sobre dispositivos digitais não coletados sejam documentados com justificativas para sua exclusão, de acordo com requerimentos aplicáveis na jurisdição.

#### 5.4.4 Aquisição

O processo de aquisição envolve a produção da cópia da evidência digital (por exemplo, disco rígido completo, partição, arquivos selecionados) e documentação de métodos usados e atividades realizadas. Recomenda-se que o DEFR adote métodos adequados de aquisição baseados na situação, custo e tempo, e documente apropriadamente a decisão para o uso de um método ou ferramenta particular.

É recomendado que os métodos utilizados para adquirir uma potencial evidência digital sejam claramente documentados em detalhes e, o quanto antes possível, sejam reproduzíveis ou verificáveis por um DEFR competente. Convém que um DEFR ou um DES adquira a potencial evidência digital de modo menos intrusivo para evitar introdução de alterações quando possível. Na execução deste processo, recomenda-se que o DEFR considere o método mais apropriado para uso. Se o resultado de um processo for uma alteração inevitável do dado digital, convém que as atividades realizadas sejam documentadas para descrever as alterações no dado.

Convém que o método de aquisição utilizado produza uma cópia de evidência digital da potencial evidência digital ou do dispositivo digital que pode conter a potencial evidência digital. Recomenda-se que ambas as fontes originais e a cópia da evidência digital sejam verificadas com uma função de verificação comprovada (comprovada precisão, naquele determinado momento) que é aceitável para o indivíduo que utilizará a evidência. É recomendado que a fonte original e cada cópia de evidência digital produzam o mesmo resultado de função de verificação.

Em circunstâncias em que não é possível que o processo de verificação seja realizado, por exemplo, ao adquirir um sistema em execução, a cópia original contém erros setoriais ou o período de tempo de aquisição é limitado. Em tais casos, convém que o DEFR use o melhor método possível disponível e seja capaz de justificar e defender a escolha do método. Se não for possível verificar a imagem, isto precisa ser documentado e justificado. Se necessário, recomenda-se que o método de aquisição utilizado seja capaz de obter o espaço alocado e não alocado.

NOTA 1 Quando não é possível que o processo de verificação seja executado de forma completa, devido a erros na fonte, então a verificação utilizando as partes da fonte que podem ser lidas com segurança pode ser utilizada.

Pode haver casos em que não é viável ou permitida a produção de uma cópia da evidência digital a partir uma fonte de evidência, por exemplo, quando a fonte for muito grande. Nestes casos, o DEFR pode realizar uma aquisição lógica, que tem como alvo somente tipos de dados específicos, diretórios ou locais. Isto geralmente ocorre em um arquivo e nível de divisão. Durante a aquisição lógica, arquivos ativos e arquivos não baseados em espaço alocado da mídia de armazenamento digital podem ser

copiados; não é permitido que arquivos excluídos e espaço não alocado sejam copiados, dependendo do método utilizado. Outros casos em que este método pode ser útil são quando sistemas de missão crítica estão envolvidos e não é possível que sejam desligados.

**NOTA 2** Algumas jurisdições podem exigir tratamento especial para dados; por exemplo, lacrá-los na presença do proprietário dos dados. É recomendado que a vedação seja feita de acordo com as exigências locais (legislativas e processuais).

#### 5.4.5 Preservação

Convém que a potencial evidência digital seja preservada para garantir sua utilidade na investigação. Ela é importante para proteger a integridade da evidência. O processo de preservação envolve a guarda da potencial evidência digital e do dispositivo digital que pode conter a potencial evidência digital contra espoliação ou adulteração. Recomenda-se que o processo de preservação seja iniciado e mantido durante o processo de manuseio da evidência digital, começando da identificação do dispositivo digital que contém a potencial evidência digital.

No melhor cenário, recomenda-se que não haja espoliação aos dados em si ou a quaisquer metadados associados a ele (por exemplo, registro de data e horário). Convém que o DEFR seja capaz de demonstrar que a evidência não foi modificada, desde que ela foi coletada ou adquirida, ou de fornecer os fundamentos e ações documentadas se alterações inevitáveis foram feitas.

**NOTA** Em alguns casos, a confidencialidade da potencial evidência digital é uma exigência, seja um requisito de negócio seja requisito legal (por exemplo, privacidade). É recomendado que a potencial evidência digital seja preservada de modo a garantir a confidencialidade dos dados.

## 6 Principais componentes de identificação, coleta, aquisição e preservação de evidência digital

### 6.1 Cadeia de custódia

Em qualquer investigação, é recomendado que o DEFR seja capaz de descrever todas as aquisições de dados e dispositivos que, no momento, estiverem sob custódia do DEFR. O registro de cadeia de custódia é um documento identificando a cronologia de movimento e do manuseio da potencial evidência digital. Recomenda-se que seja instituído a partir do processo de coleta ou aquisição. O registro será tipicamente alcançado traçando a história do item a partir do momento em que foi identificado, coletado ou adquirido pela equipe de investigação até o momento e localidade atual.

O registro de cadeia de custódia é um documento, ou uma série de documentos relacionados, que detalha a cadeia de custódia e os registros de quem foi o responsável pelo manuseio da potencial evidência digital, seja na forma de dado seja na forma de dado digital ou em outros formatos (como notas de papel). O propósito de manter o registro de cadeia de custódia é para possibilitar a identificação do acesso e movimento da potencial evidência digital a qualquer tempo. O registro de cadeia de custódia em si pode compreender mais do que um documento, por exemplo, para a potencial evidência digital é recomendado que exista um documento contemporâneo registrando a aquisição de dados digitais para um determinado dispositivo, o movimento deste dispositivo e a documentação registrando subsequentemente extratos ou cópias da potencial evidência digital para análise ou outros propósitos. Convém que o registro de cadeia de custódia contenha no mínimo as seguintes informações:

- Identificador único da evidência;
- Quem acessou a evidência e o tempo e local em que ocorreu;

- Quem checou a evidência interna e externamente nas instalações de preservação da evidência e quando isto ocorreu;
- Motivo de a evidência ter sido verificada (qual caso e propósito) e a autoridade relevante, se aplicável; e
- Quaisquer alterações inevitáveis da potencial evidência digital, assim como o nome do indivíduo responsável para tanto e a justificativa para a introdução da alteração.

Recomenda-se que a cadeia de custódia seja mantida durante todo tempo de vida da evidência e preservada por certo período de tempo depois do fim da evidência – este período de tempo pode ser definido de acordo com a jurisdição local da coleta e aplicação da evidência. Convém que ela seja estabelecida a partir do momento em que o dispositivo digital e/ou a potencial evidência digital são adquiridos e que não seja comprometida.

**NOTA** Algumas jurisdições podem possuir exigências especiais em relação à cadeia de custódia. Convém que o DEFR siga tais exigências.

## 6.2 Precauções no local do incidente

### 6.2.1 Generalidades

É recomendado que o DEFR realize atividades para assegurar e proteger o local da potencial evidência digital tão logo chegue ao local. Convém que as atividades apoiem o seguinte, sujeitas à lei local:

- Assegurar e assumir o controle da área que contém os dispositivos;
- Determinar quem é o indivíduo responsável pelo local;
- Garantir que indivíduos estão afastados dos dispositivos e fontes de energia;
- Documentar qualquer pessoa que tenha acesso ao local e qualquer pessoa que possa ter motivo para estar envolvido com a cena do incidente;
- Se o dispositivo estiver ligado, não desligá-lo; se o dispositivo estiver desligado, não ligá-lo.
- Se possível, documentar (por exemplo, por desenho, fotografia ou vídeo) a cena, todos os componentes e cabos na sua posição original. Se não houver câmera fotográfica ou videocâmera disponível, desenhar um plano de esboço do sistema e rotular as portas e cabos de forma que este sistema possa ser validado e reconstruído posteriormente; e
- Se permitido, pesquisar as áreas para itens como notas, diários, papéis, computadores portáteis ou manuais de *hardware* e *software* com detalhes cruciais sobre os dispositivos, como senhas e PIN.

**NOTA 1** Algumas jurisdições podem possuir exigências especiais para admissão de evidência no formato de fotografias e vídeo. Convém que o DEFR siga tais exigências.

**NOTA 2** DEFREs precisam estar cientes de que a potencial evidência digital pode não estar sempre em locais óbvios, como meios de armazenamento distribuídos ou virtualizados.

É recomendado que o DEFR primeiramente conheça todos os riscos envolvidos na realização de todos os processos durante a investigação. Convém levar em consideração a proteção às pessoas e à potencial evidência digital no cenário do incidente.

### 6.2.2 Pessoal

Conduzir a análise de riscos em relação à segurança de pessoal antes de iniciar o processo é importante, uma vez que a segurança das pessoas envolvidas no processo é vital. Questões a serem consideradas na análise de riscos às pessoas incluem, mas não se limitam a, o seguinte:

- O(s) indivíduo(s) investigado(s) estará(ão) presente(s)? Se presente(s), ele(s) é(são) propenso(s) à violência?
- Durante qual período do dia a operação será conduzida?
- A cena do incidente pode ser isolado de transeuntes?
- Há armas na área?
- Há qualquer perigo físico com relação ao(s) indivíduo(s) presente(s)?
- Algo nas proximidades, incluindo o dispositivo, poderia ter sido configurado para causar perigos físicos se manuseado de modo inapropriado, por exemplo, armadilha oculta?
- O material a ser coletado possui qualquer indício para causar dano ou ofensa psicológica?
- A cena do incidente pode ser considerada insegura?
- A área circundante possui um impacto sobre risco potencial?

### 6.2.3 Potencial evidência digital

É recomendado que o DEFR tenha cuidado ao usar ferramentas específicas para coletar ou adquirir potencial evidência digital. Não calcular os riscos antes de agir pode ocasionar a perda de algumas ou todas as potenciais evidências digitais devido à tecnologia aplicada durante a coleta ou aquisição. Convém que os riscos sejam analisados para reduzir a exposição a pedidos de indenização.

A análise de risco envolve a avaliação sistemática de riscos e do potencial impacto que eles podem ter sobre a investigação da evidência digital. Aspectos a considerar durante a análise de risco da potencial evidência incluem, mas não se limitam a, o seguinte:

- Qual método de coleta/aquisição será aplicado?
- Quais os equipamentos que poderão ser necessários no local?
- Qual o nível de volatilidade dos dados e informações relacionados à potencial evidência digital?
- É possível o acesso remoto à qualquer dispositivo digital e isso oferece uma ameaça à integridade da evidência?
- O que acontece se um dado/equipamento está danificado?
- Um dado poderia ter sido comprometido?
- Um dispositivo digital poderia ter sido configurado para destruir (por exemplo, usando uma bomba lógica), espoliar ou ofuscar um dado se desligado ou acessado de forma descontrolada?

### 6.3 Papéis e responsabilidades

O papel do DEFR envolve a identificação, coleta, aquisição e preservação da potencial evidência digital no cenário do incidente. Isso inclui o desenvolvimento do relato da coleta e aquisição, mas não necessariamente o relato da análise. O papel do DEFR também envolve assegurar a integridade e autenticidade da potencial evidência digital. Em atendendo ao seu papel, convém que o DEFR tenha experiência adequada, habilidades e conhecimento no manuseio da potencial evidência digital. Isto é fundamental porque a potencial evidência digital pode ser facilmente espoliada.

O DEFR também pode requisitar assistência de pessoal de suporte técnico em áreas relacionadas. O papel do DES envolve fornecer suporte técnico ao DEFR na identificação, coleta, aquisição e preservação da potencial evidência digital no cenário do incidente. O DES fornece habilidade especializada ao DEFR. A matriz de competências para o DEFR (vide em Anexo A) serve como um guia para identificar os níveis de sua relevante competência.

**NOTA** No contexto de tratamento do incidente em que uma ISIRT existe, os papéis do DEFR e/ou DES como um membro da equipe de ISIRT são discutidos na ISO/IEC 27035:2011.

### 6.4 Competência

É recomendado que o DEFR e/ou DES possuam relevante competência técnica e jurídica (por exemplo, aquelas no Anexo A) e que sejam capazes de demonstrar que eles são devidamente treinados e que têm técnica e entendimento jurídico suficiente para manusear apropriadamente a potencial evidência digital. Isto inclui uma compreensão dos processos e métodos apropriados para o manuseio das potenciais fontes da evidência digital. Uma formação adequada permitirá aos DEFR manusear os dispositivos digitais que contêm potenciais evidências digitais. Ter o melhor conjunto de ferramentas não garantirá a qualidade da evidência digital se o DEFR não for competente na realização das tarefas.

Algumas jurisdições têm prescrito como é recomendado que DEFR estabeleçam suas qualificações. É responsabilidade dos DEFR garantir que sejam devidamente informados sobre como fazer isso nas jurisdições relevantes. Quando requisitados, convém que o DEFR e/ou DES sejam capazes de demonstrar que eles são competentes para manusear a potencial evidência digital utilizando as ferramentas e métodos selecionados para realizar as tarefas. Também é exigido que os DEFR sejam capazes de fornecer provas de suas competências continuadamente.

Alguns dos pré-requisitos para o DEFR são:

- Convém que eles sejam devidamente e adequadamente treinados para manusear dispositivos digitais no contexto das atividades investigativas;
- Convém que eles demonstrem e mantenham suas habilidades e competências para autoridades apropriadas na área relevante de manuseio da potencial evidência digital; e
- É de responsabilidade do(s) indivíduo(s) e do empregador garantir que eles estejam adequadamente treinados e que as habilidades e competências estejam mantidas.

**NOTA** Competência de um DEFR pode variar de uma jurisdição para outra.

### 6.5 Utilizar cuidado razoável

Evitar quaisquer ações que possam conduzir para espoliação das potenciais evidências digitais que estão armazenadas em dispositivos digitais devido a ações intencionais ou não. Por exemplo, exposição a campos magnéticos podem espoliar a potencial evidência digital contida na mídia de armazenamento magnético. Convém que o DEFR não acesse dispositivos digitais, como conduzir o despejo de memória a partir de um dispositivo digital ativo, a menos que ele tenha competência necessária, e com a utilização de processos confiáveis e validados.

Existem algumas circunstâncias em que é impraticável a coleta ou aquisição de potencial evidência digital. É recomendado que o DEFR considere as circunstâncias seguintes, que não se limitam a somente estas:

- Se não há permissão legal ou autorização para coletar o dispositivo digital;
- Se há uma obrigação para uso de outros métodos (por exemplo, para evitar interrupção de uma atividade empresária);
- Se o DEFR quer capturar o método de operação de um suspeito durante o abuso de um sistema;
- Se é recomendado que a coleta ou aquisição ocorra em segredo, se considerado legal pela jurisdição;
- Se é um dispositivo digital de missão crítica, que não é possível que tolere qualquer tempo de inatividade;
- Se o tamanho físico do dispositivo digital é muito grande, como um servidor em um centro de dados ou sistema RAID;
- Se é um dispositivo digital de segurança crítica que colocaria em risco a vida se desativado; e
- Se é um dispositivo digital que também serve partes inocentes.

## 6.6 Documentação

Documentação é crucial quando manuseando dispositivos digitais que podem conter potencial evidência digital. Recomenda-se que o DEFR siga os seguintes pontos durante a documentação:

- Convém que toda atividade tomada seja documentada. Isto é para garantir que nenhum detalhe foi deixado de lado durante os processos de identificação, coleta, aquisição e preservação. Pode também ser útil em uma investigação transfronteiriça quando a potencial evidência digital coletada em outra parte do globo pode ser rastreada adequadamente.
- Convém que o DEFR seja sensível à hora e data se os dispositivos digitais estiverem ligados. Comparar o tempo configurado com uma fonte de tempo confiável, como o tempo que está sincronizado com uma fonte de tempo confiável e rastreável. Recomenda-se que essas configurações do tempo sejam documentadas e anotadas se quaisquer diferenças estiverem presentes. Alguns sistemas requerem interação com o usuário para obter a configuração de hora e data. Convém que o DEFR seja cauteloso para não modificar o sistema. É recomendado que somente pessoal devidamente treinado restabeleça essas configurações.
- Convém que o DEFR documente qualquer coisa visível na tela do dispositivo digital: programas e processos ativos, bem como os nomes dos documentos abertos. Recomenda-se que esta documentação inclua uma descrição do que é visível, pois alguns programas maliciosos podem mascarar programas de computador altamente conhecidos.
- Convém que qualquer movimento dos dispositivos digitais seja documentado de acordo com as exigências locais.
- Documentar todos os identificadores exclusivos dos dispositivos digitais e as partes associadas, como números seriais e marcas únicas.

Exemplos do conjunto mínimo de documentação para troca interjurisdicional de potencial evidência digital estão elencados no Anexo B.

NOTA Consultar a seção de gestão de documentos e seção de gestão de registros da ABNT NBR ISO/IEC 17025 para maiores informações sobre documentação.

## 6.7 Instruções

### 6.7.1 Geral

É essencial que o DEFR e DES sejam adequadamente instruídos pela autoridade competente antes da realização de suas tarefas, ao mesmo tempo respeitando leis de confidencialidade e restrições (ou seja, precisa conhecer a base). É importante ter uma seção formal de instrução para o entendimento do incidente, o que esperar e não esperar durante a investigação e um lembrete contra adulteração e espoliação. Convém que as instruções sejam suficientes para os membros estarem bem preparados no desempenho de suas funções e responsabilidades; deste modo, assegurando a extração de todas as potenciais evidências digitais relevantes.

### 6.7.2 Evidência digital específica

Uma seção de instrução focada explicitamente em orientações específicas para evidência digital é necessária para informar os DEFR sobre detalhes pertencentes à investigação. Durante a seção de instrução, é recomendado que o DEFR e o DES sejam providos com informações relevantes e instruções detalhadas relacionadas à potencial evidência digital a ser coletada ou adquirida. Isso pode incluir:

- Tipo do incidente (se conhecido);
- Data e horário do incidente (se conhecido);
- Plano de investigação (coleta e/ou aquisição, conhecimento das atividades de rede, conhecimento da volatilidade dos dados requeridos etc.);
- Considerar onde e como a potencial evidência digital será armazenada/transportada depois da coleta ou aquisição;
- Especificar ferramentas necessárias para adquirir a potencial evidência digital;
- Potencial evidência digital que está relacionada com tipos específicos da investigação;
- Equipamentos e manuais relacionados aos dispositivos digitais;
- Relembrar membros da equipe para desligar qualquer *Bluetooth* ou rede sem fio de seus telefones/computadores de tal modo que eles não interajam, inadvertidamente, com os dispositivos digitais, exceto para telefones/computadores utilizados para detectar as conexões;
- Importância de documentar durante a investigação; e
- Fatores legais aplicados, ou outros, que podem proibir a coleta de quaisquer dispositivos e da potencial evidência digital neles contida.

Esta seção de instruções específicas pode formar parte de uma seção de instruções gerais como descrito em 6.7.1.

### 6.7.3 Pessoal específico

Uma seção de instrução focada explicitamente em orientações específicas de pessoal é necessária para informar os DEFR sobre aspectos relacionados às partes envolvidas na investigação. Durante a seção de instruções, o pessoal de investigação será provido com instruções relativas ao pessoal. Isso pode incluir:

- Atribuições, papéis e responsabilidades dos membros da equipe de investigação no cenário do incidente;
- Se outras autoridades (pessoal médico, investigadores de biologia forense etc.) são esperadas para serem envolvidas na investigação;
- Exigência de os membros da equipe não aceitarem assistência técnica de quaisquer indivíduos não autorizados; e
- Exigência de os membros da equipe seguirem estritamente os procedimentos na minimização de riscos de espoliação da potencial evidência digital, como evitar o uso de quaisquer ferramentas ou materiais que podem produzir ou emitir eletricidade estática ou campo magnético, uma vez que estes podem danificar ou destruir a potencial evidência digital.

Esta seção de instruções específicas pode formar parte da seção de instruções gerais como descrito em 6.7.1.

### 6.7.4 Incidentes em tempo real

É altamente desejável que a investigação de um incidente seja planejada com antecedência, mas existem circunstâncias (por exemplo, quando um incidente está em desenvolvimento e sendo respondido em tempo real) em que o planejamento completo pode não ser possível. Nessas situações, convém que a equipe seja instruída sobre as estratégias e táticas iniciais para a investigação e autorizada a desenvolver novas estratégicas e táticas em resposta às condições que prevaleçam. É recomendado que informações sobre o incidente, enquanto se desenvolve, sejam compartilhadas entre a equipe tão rápido quanto possível para garantir que decisões sobre ações a serem tomadas possam ser realizadas eficientemente e com a devida consideração da necessidade de justificativa.

### 6.7.5 Outras informações nas instruções

Além da evidência digital e equipe, outras instruções importantes a serem informadas à equipe de investigação incluem:

- Designação da área sob investigação, incluindo o nome da organização, endereço e localização no mapa (se disponível);
- Mandado de investigação;
- Detalhes dos mandados de busca e outras autoridades aplicáveis para a investigação, incluindo os limites da busca e apreensão;
- Aspectos e implicações legais;
- Prazo de investigação;
- Equipamento necessário para ser levado ao cenário do incidente para a investigação;

- Informação logística; e
- Potencial conflito de interesses.

É recomendado que o DEFR evite situações nas quais acusações de inerente parcialidade podem ser feitas. Um exemplo de inerente parcialidade é quando o DEFR copia um computador e não outro (o qual, posteriormente, passa-se a descobrir que contém evidência excludente) baseado na percepção formada pelas instruções.

## 6.8 Priorizando coleta e aquisição

Na priorização de coleta ou aquisição da potencial evidência digital é imperativo para o DEFR entender o motivo da razão em coletar ou adquirir a potencial evidência digital. Como um princípio geral, recomenda-se que o DEFR tente maximizar a quantidade dos dados preservados pelas ações de coleta e aquisição. No entanto, pode ser necessário priorizar itens pela volatilidade e/ou pelo seu valor probatório quanto à(ao) relevância/potencial. Itens de valor probatório de alta relevância/potencial são aqueles que são mais prováveis de conter dados relativos diretamente ao incidente sob investigação.

Priorizar pela volatilidade é somente aplicável se circunstâncias específicas do caso investigado requererem isto. A potencial evidência digital pode ser dividida em duas categorias: voláteis e não voláteis. Dados voláteis podem ser facilmente destruídos ou perdidos para sempre se o devido cuidado na proteção dos dados não for aplicado. Por exemplo, remover uma fonte de energia de um dispositivo digital pode resultar em perda de dados voláteis. Dados não voláteis permanecem na mídia mesmo se a fonte de energia for removida. Uma vez que alguns tipos de evidência digital podem ter curto tempo de vida, a potencial evidência digital pode ser facilmente adulterada ou espoliada. Onde não é claro se os dispositivos digitais contêm potencial evidência digital, ou quais itens são de maior relevância em comparação a outros, pode ser necessário examiná-los antes da coleta utilizando-se de um processo para determinar prioridade. Dispositivos digitais a serem considerados para a coleta incluem, mas não estão limitados a: equipamentos de TI e mídias de armazenamento digital, sistemas CFTV, os PED, sistemas automotivos, sistemas de controle e eletrônicos improvisados. Adquirir primeiro a potencial evidência digital mais volátil, como RAM, espaço de troca, processos em execução etc. Recomenda-se que o DEFR tenha um conhecimento razoável para priorizar de acordo com a volatilidade.

Após a identificação, é recomendado ao DEFR:

- Priorize a potencial evidência digital que pode ser perdida para sempre se a fonte de energia for removida; e
- Tome ações rápidas para coletar e adquirir este dado com métodos validados.

**NOTA 1** Alguns dados voláteis podem se alterar devido a fatores que incluem, mas não se limitam a, o local, tempo e alterações ao redor dos dispositivos digitais – garantir que este dado está preservado antes de mover o dispositivo.

**NOTA 2** Dispositivos digitais contendo potencial evidência digital podem ser uma fonte de evidência física (por exemplo, impressões digitais, DNA etc.). Os DEFR precisam tomar cuidado para não espoliar a evidência e coordenar com os coletores de evidências relevantes antes de prosseguir para as próximas atividades.

**NOTA 3** Quando há suspeita de criptografia ou de um programa malicioso, é desejável o examinar o dado volátil.

Nestas circunstâncias, tempo pode ser um fator de limitação durante uma investigação. Nestes casos, é recomendado que seja dada preferência à potencial evidência digital identificada como relevante para o incidente específico.

## 6.9 Preservação da potencial evidência digital

### 6.9.1 Visão geral

Na preservação da potencial evidência digital adquirida e de dispositivo digital coletados durante o acondicionamento, é importante garantir estes itens de um modo que seja eliminada espoliação ou adulteração. Espoliação pode resultar de uma degradação magnética, degradação elétrica, temperatura elevada, exposição à alta ou baixa umidade, bem como choques e vibrações. Adulteração pode resultar de um ato intencional de adulterar ou permitir mudança da potencial evidência digital. Por esse motivo, é crucial proteger a potencial evidência digital da melhor forma possível e utilizar o dado original o mínimo possível. É importante que o DEFR esteja familiarizado com os requisitos específicos de acondicionamento relacionados à jurisdição relevante.

### 6.9.2 Preservando a potencial evidência digital

Convém que todo dispositivo digital coletado e potencial evidência digital adquirida sejam protegidos tanto quanto possível de perdas, adulteração ou espoliação. A atividade mais importante no processo de preservação é manter a integridade e autenticidade da potencial evidência digital e sua cadeia de custódia.

Convém que o dispositivo digital coletado e a potencial evidência digital adquirida sejam armazenados em uma instalação de preservação de provas que aplica controle de segurança física, como sistema de controle de acessos, sistemas de vigilância ou sistemas de detecção de intrusão ou outro controle de ambiente para preservação da evidência digital. Os principais objetivos da segurança física são proteger e prevenir perdas, danificações e adulterações, bem como garantir a auditabilidade.

É recomendado que o dispositivo digital coletado seja embrulhado ou colocado em embalagem apropriada para a natureza do dispositivo para evitar contaminação do dispositivo digital antes de transportá-lo para outro local. Uma embalagem resistente a choques pode ser utilizada para evitar danificação física a quaisquer componente(s) do dispositivo.

- Recomenda-se que o DEFR considere a sensibilidade do dispositivo digital à eletricidade estática. Se isto é uma preocupação, é recomendado que o dispositivo seja protegido em uma embalagem antiestática.
- As principais unidades do sistema e computadores portáteis precisam ser protegidas em recipiente, para evitar adulteração ou espoliação da potencial evidência digital que pode residir neste.

**NOTA** A utilização de uma embalagem de Faraday, ou outra embalagem blindada de radiofrequência, pode aumentar a drenagem da bateria do telefone móvel. Isto pode exigir fornecimento de energia auxiliar para o dispositivo enquanto no interior da embalagem, se os recursos permitirem.

### 6.9.3 Acondicionando dispositivos digitais e potencial evidência digital

#### 6.9.3.1 Atividades de base: acondicionando potencial evidência digital

Recomenda-se que atividades de base sejam conduzidas, a menos que exista uma boa razão para que não sejam realizadas. Isto também pode ser referido como o mínimo de ações a serem tomadas. Durante o acondicionamento, convém ao DEFR observar e atender às seguintes atividades de base:

- Não tocar em fita magnética, mas pegá-la por sua própria capa protetora ou áreas que são conhecidas por não conter dados (por exemplo, bordas de discos óticos). É recomendado que isto seja feito somente se o DEFR utilizar luvas livres de partículas.

**NOTA** As áreas específicas das mídias de armazenamento que são conhecidas por não conterem dados dependem do tipo de mídia. É de responsabilidade do DEFR conhecer a tecnologia atual e estar familiarizado com o manuseio de mídias de armazenamento.

- Para assegurar a identificação correta, recomenda-se que o DEFR rotule toda potencial evidência digital. Algumas jurisdições têm exigências específicas em relação ao formato na rotulação do material probatório. É recomendado que o DEFR esteja familiarizado, e em conformidade, com as exigências aplicáveis no assunto em questão. Convém que o DEFR rotule toda potencial evidência digital, dispositivo digital coletado e qualquer parte de hardware associada ao dispositivo com invólucro inviolável. Recomenda-se que o rótulo não seja colocado diretamente sobre as partes mecânicas do dispositivo digital e não cubra ou oculte importantes informações identificadas. Recomenda-se que toda potencial evidência digital em dispositivo coletado seja adquirida e armazenada de modo a garantir a integridade da evidência.
- Recomenda-se que, quando possível, dispositivos digitais com aberturas e componentes móveis sejam selados com rótulos invioláveis que sejam apropriados para os dispositivos e é recomendado que o DEFR assine o selo.
- Recomenda-se que dispositivos que são ligados a baterias, e que contêm dados voláteis, sejam checados regularmente para garantir que os dispositivos sempre tenham energia suficiente.
- Identificar e proteger dispositivos digitais em um recipiente apropriado para a natureza do dispositivo contra potenciais ameaças.
- Recomenda-se que computadores e dispositivos digitais sejam acondicionados de tal forma a prevenir danos provenientes de choques, vibrações, alta altitude, calor e exposição à radiofrequência durante o transporte.
- Recomenda-se que mídias de armazenamento magnético sejam armazenadas em embalagem inerte magneticamente, antiestática e livre de partículas.
- Dispositivos digitais podem também conter evidências latentes, traçáveis ou biológicas. Assim, atividades apropriadas precisam ser realizadas para preservar a potencial evidência digital. Recomenda-se que a imagem da evidência digital seja realizada após os processos de coleta de evidências latentes, traçáveis ou biológicas haverem sido conduzidos sobre os dispositivos. No entanto, convém que a decisão para priorizar a coleta da evidência seja cuidadosamente avaliada para preservar a evidência.

#### **6.9.3.2 Atividades adicionais: acondicionando potencial evidência digital**

Atividades adicionais referem-se a atividades que são fortemente recomendadas a serem executadas. Durante o acondicionamento, é recomendado que o DEFR observe e atenda às seguintes atividades adicionais, quando aplicáveis:

- Utilizar luvas livres de partículas e assegurar que as mãos estejam limpas e secas.
- Proteger os dispositivos digitais da influência de fontes eletromagnéticas (por exemplo, rádios de polícia, alto-falantes, máquinas de raios X). É recomendado que o ambiente da embalagem esteja livre de eletricidade estática.
- É recomendado que o ambiente da embalagem esteja livre de poeira, gordura e poluentes químicos que promovam a deterioração oxidativa e condensação da umidade sobre a camada magnética.
- Minimizar a possibilidade de impressão direta (a transferência de um sinal a partir do espiral da fita para o seu espiral adjacente), que pode ocorrer quando fitas são armazenadas por longos períodos sem uso ativo, resultando em má qualidade de sinal.

- Recomenda-se que, onde for necessário, as áreas de acondicionamento estejam livres de luz UV. UV pode causar degradação do DNA ou danificar alguns tipos de mídia. Convém que o DEFR considere se UV apresenta um risco para a potencial evidência digital antes de selecionar uma área de acondicionamento.
- Recomenda-se que os dispositivos digitais sejam fortemente protegidos de choques térmicos.

#### **6.9.4 Transportando potencial evidência digital**

Durante o transporte, é recomendado que o DEFR preserve o dispositivo digital coletado e a potencial evidência digital adquirida. Não é recomendado que a potencial evidência digital seja deixada desatendida durante o processo de transporte. Convém que o DEFR mantenha a cadeia de custódia durante o processo de transporte para prevenir possível adulteração ou espoliação e mantenha a integridade e autenticidade do dispositivo digital e da potencial evidência digital. Se a potencial evidência digital não for transportada pelo DEFR ou pelo DES, é recomendado que a criptografia seja utilizada.

**NOTA** Recomenda-se que o DEFR assegure que a coleta de informações sensíveis ou pessoais está de acordo com as leis e regulamentos da jurisdição local para a proteção dos dados.

Durante o acondicionamento e transporte, o DEFR precisa estar atento à possível presença de descarga eletrostática que pode danificar o valor probatório da potencial evidência digital. Recomenda-se que o DEFR garanta que computadores e dispositivos digitais estão acondicionados de modo seguro durante o transporte para prevenir danificações decorrentes de choques e vibrações.

É recomendado que o processo de transporte permita um ambiente propício e controlado. Recomenda-se que o nível de transpiração, umidade do ar e do dispositivo digital e a temperatura sejam apropriados ao dispositivo digital. Evitar manter a potencial evidência digital e o dispositivo digital no veículo de transporte por prolongados períodos, e evitar que ambos fiquem na presença de UV.

Em algumas jurisdições, quando as circunstâncias não permitem, o DEFR é incapaz de acompanhar a evidência. Em tais casos, a utilização apropriada e autorizada de mecanismos de transporte pode ser aplicada para assegurar a segurança adequada da evidência durante o transporte. Convém que documentos da transportação e verificação da integridade da embalagem tornem-se parte da cadeia de custódia.

## **7 Instâncias de identificação, coleta, aquisição e preservação**

### **7.1 Computadores, dispositivos periféricos e mídias de armazenamento digital**

#### **7.1.1 Identificação**

##### **7.1.1.1 Pesquisa e documentação do cenário físico do incidente**

No contexto desta seção, computadores são considerados como dispositivos digitais autônomos que recebem, processam e armazenam dados e produzem resultados. Estes dispositivos computacionais não estão conectados a uma rede, mas podem ser conectados a dispositivos periféricos como impressoras, digitalizadores, *webcams*, *MP3 players*, sistemas GPS, dispositivos RFID, e assim por diante. É recomendado que um dispositivo digital que tem uma rede de interface, mas, no momento da coleta ou aquisição, não está conectado, seja considerado (para o propósito desta Norma) como um computador autônomo. Quando há um computador com uma interface de rede, mas sem conexão óbvia encontrada, convém que as atividades sejam realizadas para identificar dispositivos que podem ter sido conectados em um passado recente.

Usualmente, cenários de incidente conterão vários tipos de mídia de armazenamento digital. A mídia de armazenamento digital é usada para armazenar dados de dispositivos digitais e varia em capacidade de memória. Exemplos de mídia de armazenamento digital incluem, mas não se limitam a, discos rígidos portáteis externos, *pen drives*, *CD*, *DVD*, discos *Blu-ray*, disquetes, fitas magnéticas e cartões de memória.

Antes de qualquer aquisição ou coleta ser feita, aspectos de segurança da potencial evidência digital precisam ser considerados. Esses aspectos estão descritos em 6.2.1 e 6.2.2. Recomenda-se que o DEFR tenha cuidado, no entanto, para se assegurar de que um dispositivo aparentemente autônomo não foi recentemente conectado em uma rede. Se há suspeita que um dispositivo aparentemente autônomo foi recentemente desconectado, recomenda-se dar a ele o tratamento de um dispositivo de rede para, assim, assegurar que outras partes da rede sejam tratadas corretamente. Convém ao DEFR observar e atender a pelo menos o seguinte:

- É recomendado que o DEFR documente o tipo e a marca de qualquer dispositivo digital usado e identificar todo computador e dispositivos periféricos que talvez necessitem ser adquiridos ou coletados durante este estágio inicial. Recomenda-se que os números de série, números de licença e outras marcas identificadoras (incluindo danos físicos) sejam documentados sempre que possível.
- No estágio de identificação, é recomendado que os estados dos computadores e dos dispositivos periféricos remanesçam como ali estão. Se os computadores ou dispositivos periféricos estiverem desligados, não ligá-los. Se os computadores ou dispositivos periféricos estiverem ligados, recomenda-se que o DEFR não os desligue, pois pode espoliar a potencial evidência digital.
- Se os computadores estiverem ligados, recomenda-se que o DEFR fotografe ou elabore um documento por escrito do que está exibido nas telas. Convém que qualquer documento escrito inclua a descrição do que exatamente é visível (por exemplo, posições aproximadas das janelas, títulos e conteúdos).
- Um dispositivo que tenha bateria sujeita a acabar precisa ser carregado para assegurar que a informação não seja perdida. O DEFR precisa identificar e coletar potenciais carregadores de bateria e cabos durante esta fase.
- É recomendado que o DEFR considere o uso de detector de sinal de rede sem fio para detectar e identificar sinais de rede sem fio a partir de dispositivos de rede sem fio que podem estar escondidos. Pode haver casos em que um detector de sinal de rede sem fio não seja usado devido a restrições de custo e tempo, e recomenda-se que o DEFR documente isto. Se qualquer dispositivo de rede for encontrado, recomenda-se que o DEFR continue com o processo de manuseio da evidência como descrito em 7.2.2.2 deste documento. Onde o exame ativo (ou seja, transmissão e/ou sondagem) para dispositivos de rede sem fio é usado, é recomendado que os dispositivos de exame sejam desligados até que a avaliação sobre as possibilidades de o dispositivo interagir com outros dispositivos no local seja determinada. Convém que membros da equipe recordem que certos dispositivos no local podem detectar a presença de dispositivos de exame ativa, e o uso de exame ativa pode provocar ações que podem espoliar a potencial evidência digital, e pode, em extremas circunstâncias, resultar na ativação de armadilhas ocultas.

**NOTA 1** Em algumas jurisdições, é permitido ligar dispositivos digitais no local para determinar sua relevância para a investigação, se há muitos dispositivos digitais presentes. Isto é feito considerando o tempo de processamento e custo que pode incorrer se dispositivos digitais não relevantes forem adquiridos. Se um dispositivo for ligado para avaliação no local, é recomendado que o DEFR assegure que anotações exaustivas das ações tomadas são mantidas durante o processo.

**NOTA 2** Em preservando o estado de energia do dispositivo digital, convém que os resultados dos processos de priorização por volatilidade e relevância sejam considerados. Se a decisão tomada é de que a informação crucial é a informação não volátil em disco, então o sistema em execução pode fotografar a tela do console e o cabo de energia puxado. Se a informação volátil na memória é relevante, então é crucial deixar o sistema ligado para permitir a sua aquisição.

### 7.1.1.2 Coleta de evidência não digital

É recomendado que o DEFR considere a coleta de evidência não digital. Convém que, para permitir isso, o líder da equipe identifique os indivíduos responsáveis pelas instalações no local. Este indivíduo pode fornecer informação e documentação adicional, como senhas para os dispositivos digitais e outros detalhes relevantes. O DEFR precisa documentar o nome e a designação desses indivíduos.

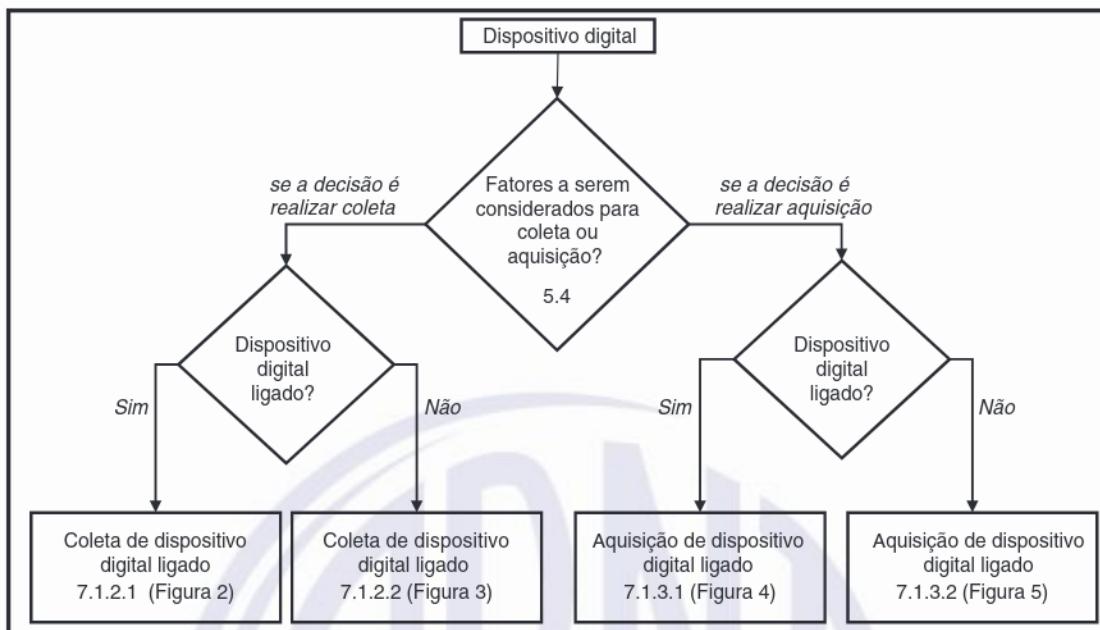
O DEFR pode também precisar coletar algumas evidências por entrevistas com indivíduos que podem ter informações úteis ou relevantes sobre a potencial evidência digital ou sobre o dispositivo digital a ser coletado. É recomendado que quaisquer respostas sejam documentadas com precisão. Estes indivíduos podem incluir o administrador do sistema, o proprietário do dispositivo e usuários do computador e dispositivos periféricos. Durante a coleta desta evidência verbal, o DEFR pode requerer informação como a configuração do sistema e senha do administrador/root. Estas informações adicionais podem ser úteis no estágio de análise da potencial evidência digital. Recomenda-se que estas conversações sejam documentadas para garantir a precisão dos detalhes e garantir que o depoimento documentado não seja alterado. O DEFR precisa estar familiarizado com as exigências jurisdicionais relevantes para a coleta de evidências não digitais.

### 7.1.1.3 Processo para tomada de decisão para coleta ou aquisição

Ao decidir pela coleta de um dispositivo digital ou aquisição de potencial evidência digital, convém que vários fatores sejam considerados, que incluem, mas não estão limitados a, os seguintes:

- volatilidade da potencial evidência digital, que foi discutida em 5.4.2 e 6.8,
- existência de criptografia completa de disco ou de volumes criptografados onde senhas ou chaves podem residir como dado volátil em RAM, fichas externas, smart cards, outros dispositivos ou mídias.
- criticidade do sistema, que foi discutida em 5.4.4, 7.2.1.2 e 7.1.3.4,
- exigências legais de uma jurisdição, e
- recursos como tamanho de armazenamento necessário, disponibilidade de pessoal, limitações de tempo.

A Figura 1 ilustra a visão geral do processo de tomada de decisão para coleta ou aquisição.



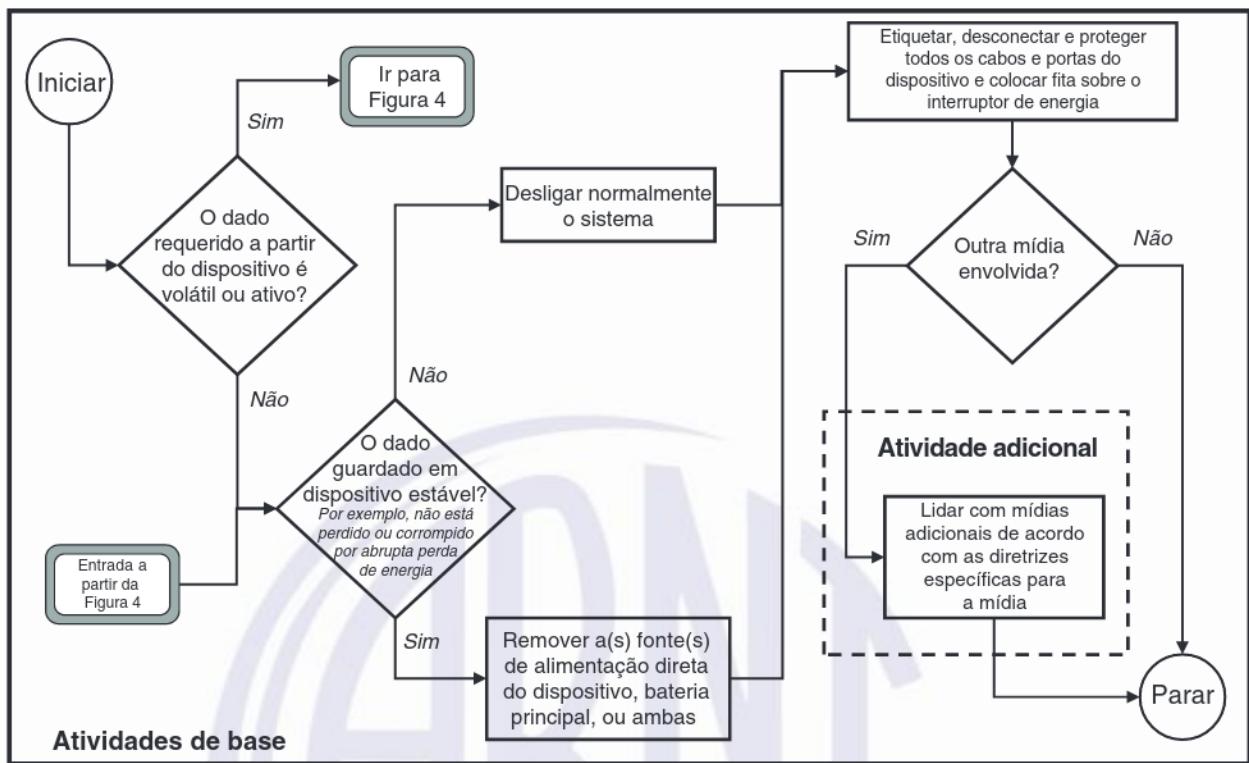
**Figura 1 – Diretrizes para tomada de decisão para coleta ou aquisição da potencial evidência digital**

## 7.1.2 Coleta

### 7.1.2.1 Dispositivos digitais ligados

#### 7.1.2.1.1 Visão geral

O DEFR pode seguir uma série de diretrizes para a coleta quando o dispositivo digital estiver ligado. Nem todas as diretrizes são ideais e apropriadas para quaisquer casos; algumas orientações são relevantes somente para casos específicos. Consequentemente, as orientações podem ser categorizadas como de base ou adicionais. Recomenda-se que as atividades de base sejam aplicadas em todas as circunstâncias, enquanto convém que as atividades adicionais sejam aplicadas quando forem relevantes e aplicáveis, dependendo do dispositivo único ou das circunstâncias. A Figura 2 ilustra as atividades de base e adicionais aplicáveis ao dispositivo digital ligado.



**Figura 2 – Diretrizes para coleta de dispositivo digital ligado**

**NOTA** É recomendado que todas estas atividades estejam em conformidade com as leis e regulamentos da jurisdição local.

É do DEFR a responsabilidade de conhecer a tecnologia atual e estar familiarizado com as orientações para o manuseio/tratamento da mídia de armazenamento.

#### 7.1.2.1.2 Atividades de base: coleta de dispositivo digital ligado

Recomenda-se que as seguintes atividades de base sejam seguidas pelo DEFR em todos os casos envolvendo potencial evidência digital. Estas orientações aplicam-se quando o DEFR decide que um dispositivo digital ligado seja coletado:

- Considerar a aquisição de um dado de um dispositivo digital volátil e o estado atual antes de desligar o sistema. Chaves de criptografia e outros dados cruciais podem residir na memória ativa ou na memória inativa que ainda não foi limpa. Considerar uma aquisição lógica quando há suspeita de criptografia. Neste caso, ter em mente que o sistema operacional local pode não ser confiável, então considerar a utilização de ferramentas apropriadas que sejam confiáveis e validadas.
- A configuração do dispositivo digital pode determinar se o DEFR precisa desligar o dispositivo por meio de procedimentos administrativos normais ou se é recomendável que o plugue do dispositivo seja retirado da tomada. O DEFR pode precisar consultar o DES para determinar a melhor abordagem a ser dada às circunstâncias específicas. Se a decisão é para retirar o plugue da tomada, o DEFR precisa remover primeiro a extremidade do cabo de energia ligado ao dispositivo digital, e não a extremidade do cabo ligada à tomada. Estar ciente de que um dispositivo conectado em uma UPS pode ter dados alterados se o cabo de energia for removido da parede e não do dispositivo.

**NOTA 1** Se a energia é removida a partir de um dispositivo digital ligado, qualquer potencial evidência digital armazenada em volumes criptografados estará inacessível, a menos que a chave para decriptar

seja obtida. Dados ativos potencialmente valiosos podem também ser perdidos, como dados corporativos ou dispositivos digitais que controlam equipamentos médicos. Como tal, é recomendado que o DEFR assegure que dados voláteis foram coletados antes de removida a fonte de energia.

**NOTA 2** Há dispositivos de *hardware* que permitem que dispositivos ligados sejam desconectados da rede elétrica e transferidos para UPS portáteis, sem interromper a energia do dispositivo. Há também *mouse-jigglers* que podem ser usados para prevenir que o protetor de tela seja ativado. Ambos os dispositivos fornecem ferramentas úteis quando se lida com dispositivos ligados em que criptografia pode estar ativa. Quando um dispositivo coletado está ligado de tal forma que a energia é mantida, convém que o acondicionamento e o transporte do sistema em execução abordem questões relacionadas com a provisão de resfriamento, proteção contra choques mecânicos etc.

- Rotular, desconectar e proteger todos os cabos do dispositivo digital e rotular as portas de modo que o sistema possa ser reconstruído em um estágio posterior.
- Colocar fita sobre o interruptor de energia, se necessário, para prevenir a alteração de estado. Considerar se o estado do interruptor foi corretamente documentado antes de lacrado ou movimentado.

#### 7.1.2.1.3 Atividades adicionais: coleta de dispositivo digital ligado

Seguem as atividades adicionais que são relevantes dependendo da configuração do dispositivo digital específico.

- Se há um computador portátil, assegurar que o dado volátil é adquirido antes de removida a bateria. É recomendado que o DEFR remova primeiro a principal fonte de energia da bateria, em vez de pressionar o botão de energia do computador portátil para desligá-lo. Convém que o DEFR tome nota se um adaptador de energia está presente e, se sim, remova o adaptador de energia depois de removida a bateria.

**NOTA 1** A ação de pressionar o botão de energia do dispositivo digital pode estar configurada para iniciar um documento que pode alterar ou excluir informação do sistema antes de ser desligado ou alertar sistemas conectados sobre a ocorrência de um evento inesperado de modo que pode apagar dados de valor probatório antes de serem identificados. Pode também ser configurado para acionar um dispositivo destinado a causar dano físico ao DEFR ou a outras pessoas presentes.

- Colocar fita sobre a entrada de disquete, se presente.
- Certificar-se de que as unidades de bandejas de CD ou DVD estão retraidas no lugar; observar se estas unidades de bandejas estão vazias, contêm discos ou não foram verificadas; e colocar uma fita sobre a abertura da unidade fechada para evitar a sua abertura.

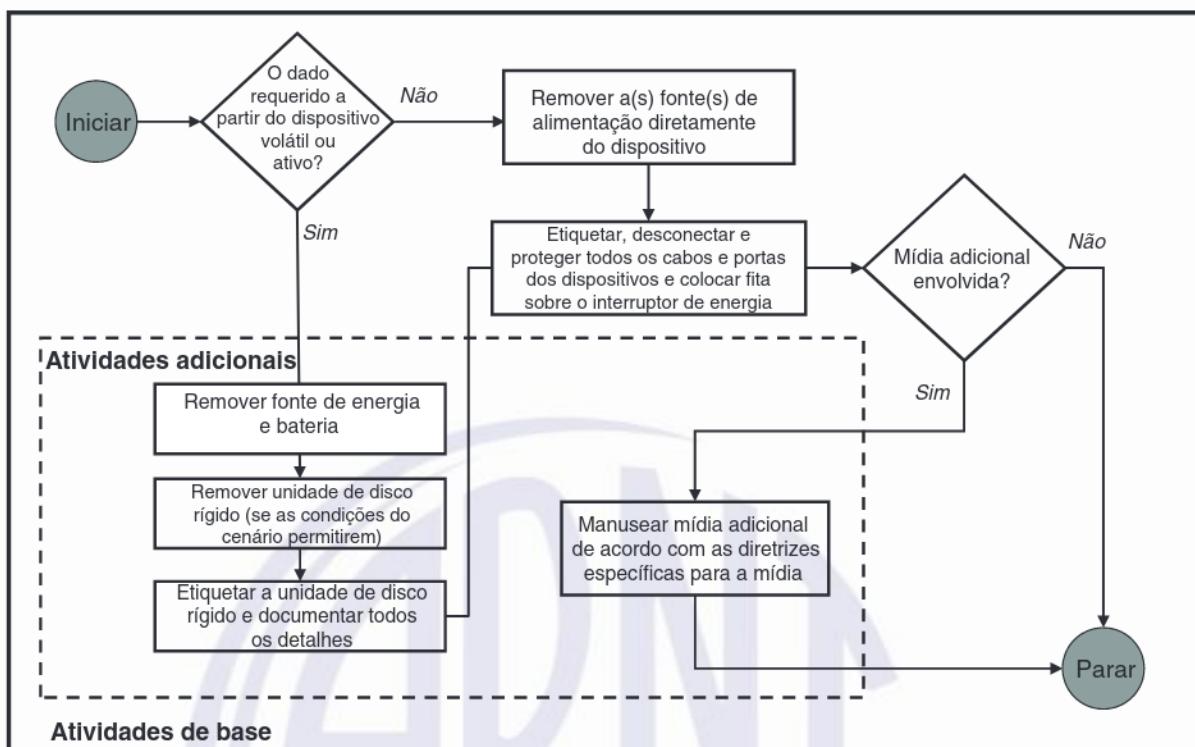
**NOTA 2** Se qualquer mídia sujeita à inicialização é deixada, então, quando a máquina for ligada em seguida, poderá inicializar a partir da mídia em vez de disco rígido (ou ferramentas forenses *pen-drives*), dependendo das configurações BIOS do computador.

Recomenda-se que o DEFR conduza a coleta de evidência não digital em conformidade com as leis processuais para garantir a admissibilidade de qualquer evidência.

#### 7.1.2.2 Dispositivos digitais desligados

##### 7.1.2.2.1 Visão geral

O DEFR pode seguir uma série de orientações para coleta quando o dispositivo digital estiver desligado. Nem todas as atividades contidas nestas orientações são relevantes em todas as circunstâncias. Assim, uma distinção há de ser feita entre aquelas atividades que se aplicam a todos os casos (atividades de base) e aquelas que se aplicam somente em alguns casos (atividades adicionais). Figura 3 ilustra as atividades de base e adicionais aplicáveis para coleta de dispositivo digital desligado.



**Figura 3 – Diretrizes para coleta de dispositivo digital desligado**

É do DEFR a responsabilidade de conhecer a tecnologia atual e estar familiarizado com as orientações para o manuseio da mídia de armazenamento.

#### 7.1.2.2.2 Atividades de base: coleta de dispositivo digital desligado

A seguir, estão as atividades de base recomendadas para coleta quando o dispositivo digital estiver desligado:

- Remover o cabo de energia removendo primeiro a extremidade ligada ao dispositivo digital e não a extremidade ligada à tomada.
- Desconectar e proteger todos os cabos do dispositivo digital e etiquetar as portas de modo que o sistema possa ser reconstruído em um estágio posterior.
- Colocar fita sobre o interruptor de energia, se necessário, para prevenir a alteração de estado. Considerar se o estado do interruptor foi corretamente documentado antes de lacrado ou movimentado.

**NOTA** Na maioria dos casos, não é recomendado que a mídia de armazenamento seja removida do dispositivo digital até que seja adquirida, uma vez que removida aumenta o risco de danificá-la ou confundi-la com outra mídia de armazenamento. Recomenda-se que procedimentos locais em relação à necessidade de remover mídia de armazenamento de dispositivos digitais sejam desenvolvidos e seguidos.

#### 7.1.2.2.3 Atividades adicionais: coleta de dispositivo digital desligado

Seguem as atividades adicionais que são relevantes para a coleta de dispositivo digital desligado, dependendo da configuração do dispositivo digital específico:

- Primeiro, garantir que o computador portátil está de fato desligado, uma vez que alguns podem estar em modo de espera. Ter cautela, pois alguns computadores portáteis podem ser ligados pela abertura da tampa. Em seguida, proceder para remover a principal fonte de energia da bateria do computador portátil.

- Se as condições de campo requerem que o disco rígido seja removido, convém ao DEFR ter cuidado para aterrarr o dispositivo digital para prevenir que a eletricidade estática danifique o disco rígido. De outro lado, recomenda-se que o disco rígido não seja removido no campo. Etiquetar o disco rígido como um disco suspeito e documentar todos os detalhes, como fabricante, nome do modelo, número de série e tamanho do disco rígido.
- Colocar fita sobre o disquete, se presente.
- Certificar-se de que as unidades de bandejas de CD ou DVD estão retraídas no lugar; observar se estas unidades de bandejas estão vazias, contêm discos ou não foram verificadas; e colocar uma fita na unidade fechada para evitar que ela se abra.

**NOTA** Se qualquer mídia sujeita à inicialização é deixada, então quando a máquina for ligada em seguida, poderá inicializar a partir de mídia em vez de disco rígido (ou ferramentas forenses flash drive), dependendo das configurações do BIOS do computador.

### 7.1.3 Aquisição

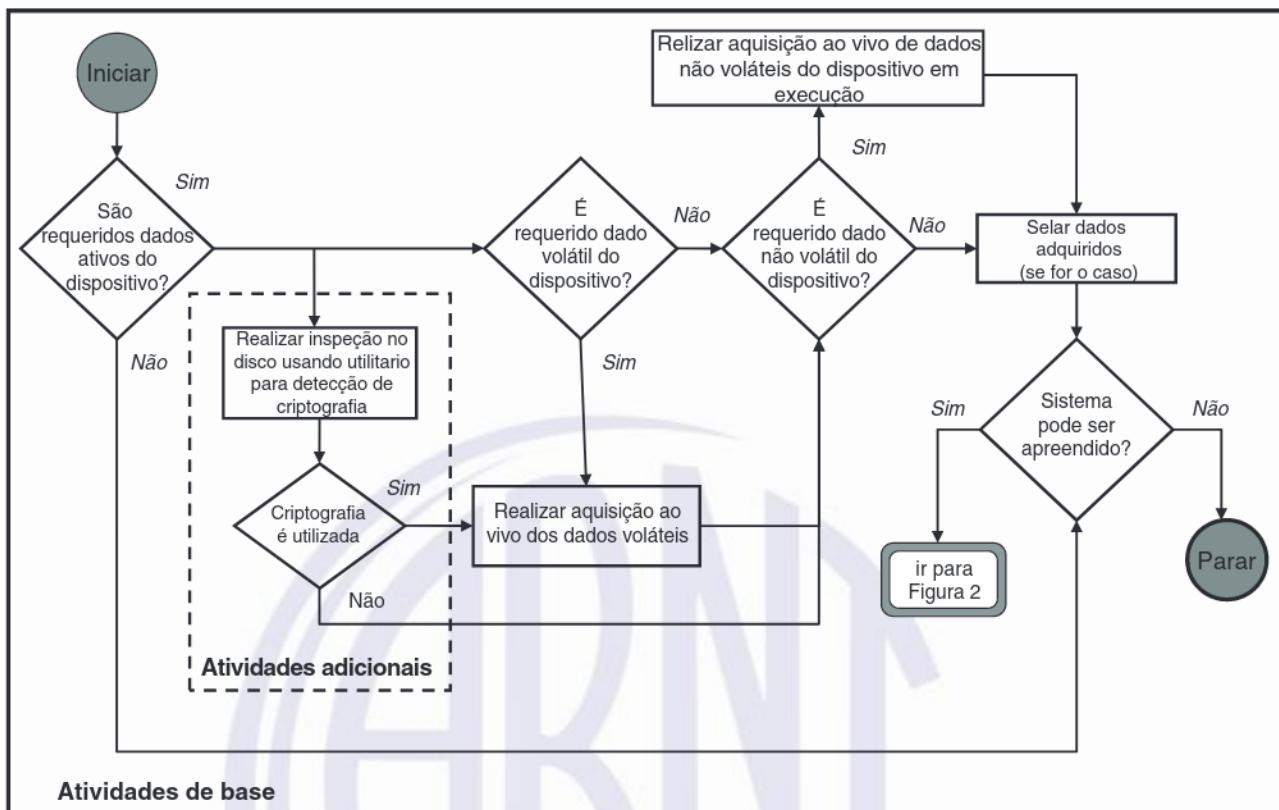
#### 7.1.3.1 Dispositivos digitais ligados

##### 7.1.3.1.1 Visão geral

Existem três cenários em que a aquisição pode ser necessária para ser conduzida: quando os dispositivos digitais estiverem ligados, quando os dispositivos digitais estiverem desligados e quando os dispositivos digitais estiverem ligados mas não é recomendado que sejam desligados (como dispositivos digitais de missão crítica). Em todos estes cenários é necessário que o DEFR faça uma cópia precisa da evidência digital que está na mídia de armazenamento dos dispositivos digitais suspeitos de conter potencial evidência digital.

Se não é possível que uma imagem seja obtida, cópias precisas dos arquivos específicos, suspeitos de conter potencial evidência digital, podem ser adquiridas. Idealmente, convém que tanto uma cópia-mestre verificada quanto cópias de trabalho sejam produzidas. Não é recomendado que a cópia-mestre seja usada novamente, a menos que isso seja requerido para verificação do conteúdo da cópia de trabalho ou produção de uma cópia de trabalho substitutiva à primeira cópia de trabalho outrora danificada.

O DEFR pode seguir uma série de orientações para aquisição quando o dispositivo digital é encontrado ligado. Nem todas as orientações são ideais e apropriadas para todos os casos; algumas orientações são somente relevantes para casos específicos. Consequentemente, as orientações podem ser categorizadas como de base ou adicionais. É recomendado que se considere a possibilidade de um sistema ligado poder entrar em modo de proteção de tela ou auto-lock e se há implicações para qualquer esforço para impedir isso. Por exemplo, o uso de um mouse-jiggler requererá uma porta de entrada USB no registro e modificações provavelmente ocorrerão independentemente das ações tomadas. Recomenda-se que a utilização de métodos confiáveis minimize as implicações destas ações. A Figura 4 ilustra as atividades de base e adicionais aplicáveis para aquisição de dispositivo digital ligado.



**Figura 4 – Diretrizes para aquisição de dispositivo digital ligado**

#### 7.1.3.1.2 Atividades de base: aquisição de dispositivo digital ligado

Convém que as atividades de base a seguir sejam seguidas pelo DEFR em todos os casos envolvendo aquisição de potencial evidência digital em dispositivos digitais ligados:

- Primeiro, considerar a aquisição de potencial evidência digital que pode, de outro modo, ser perdida se o dispositivo digital é desligado. Isto também é conhecido como dado volátil, como dado armazenado em memória RAM, processos em execução, conexões de rede e configurações de data/tempo. Em circunstâncias quando é necessária a aquisição de dado não volátil de dispositivos digitais que estão ainda sendo executados, convém que seja considerada a realização de uma aquisição sobre um sistema ligado.
- É necessário realizar aquisição imediata para adquirir dados ativos de dispositivos que estão ainda sendo executados. Aquisição imediata de dado volátil em memória RAM pode permitir a recuperação de informação valiosa, como estado do trabalho em rede, descriptografar aplicações e senhas. Aquisição imediata pode ser conduzida sobre o console ou remotamente por meio da rede. Os processos são diferentes e requerem o uso de conjuntos diferentes de ferramentas.
- Convém que o DEFR nunca confie nos programas dos sistemas. Por esta razão, ferramentas confiáveis obtidas pelo DEFR (binários estáticos) são recomendadas sempre que possível. Recomenda-se que o DEFR seja competente para utilizar as ferramentas validadas e ser competente para descrever os efeitos que tais ferramentas possam ter sobre o sistema (por exemplo, deslocamento da potencial evidência digital, conteúdo da memória expirar quando o programa está sendo carregado etc.). Convém que todas as ações realizadas e os resultados das mudanças realizadas sobre a potencial evidência digital sejam documentadas e entendidas.

Se não for possível determinar o provável efeito da introdução de ferramentas no sistema ou se não é possível que alterações resultantes sejam determinadas com convicção, convém que isto também seja documentado.

- Ao adquirir dado volátil, é recomendado que o DEFR adote o uso de receptáculo de arquivo lógico, quando possível, e documente o valor de *hash*, uma vez que contém arquivo com dado volátil. Quando isso não for possível, convém que um receptáculo, como um arquivo ZIP, seja usado e, em seguida, recomenda-se que este arquivo seja colocados em *hash* e o valor seja documentado. É recomendado que os receptáculos de arquivos resultantes sejam armazenados em uma mídia de armazenamento digital que tenha sido preparada para este propósito, ou seja, formatada.
- Executar o processo de imagem no armazenamento vivo não volátil utilizando-se de ferramentas de imagem validadas. É recomendado que a cópia da evidência digital resultante seja armazenada sobre uma mídia de armazenamento digital preparada para este propósito. Enquanto é preferível utilizar uma nova mídia de armazenamento digital, o uso de cópias da evidência digital a partir de processos validados assegura a integridade do dado quando reconstruído. Portanto, uma armazenamento digital que foi esterilizado será suficiente. Se a imagem tem de ser armazenada em um receptáculo de arquivo lógico, convém que o DEFR assegure que a imagem não pode ser corrompida ou danificada.

**NOTA** Em situações onde o dispositivo está bloqueado, acesso físico pode ser conduzido mediante outros meios que têm permissão de acesso direto à memória, por exemplo interface *Firewire*.

#### 7.1.3.1.3 Atividades adicionais: aquisição de dispositivo digital ligado

Seguem as atividades adicionais que são relevantes para a aquisição de dispositivo digital ligado, dependendo da configuração do dispositivo digital específico:

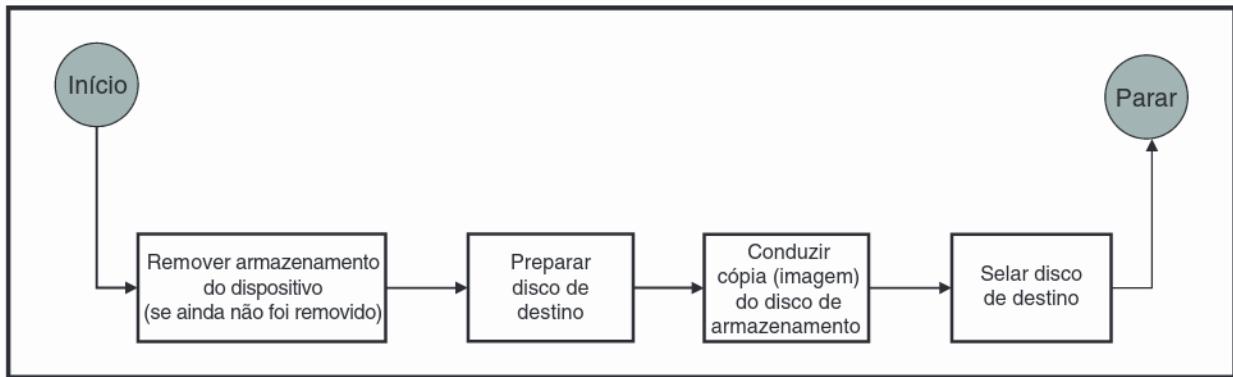
- Considerar aquisição de dado volátil em memória RAM quando o uso de criptografia é suspeitado. Primeiro, checar se este é o caso inspecionando o disco bruto (*raw disk*) ou usando algum serviço útil de detecção de criptografia. Se este é o caso, ter em mente que o sistema operacional local pode não ser confiável e considerar a utilização de ferramentas confiáveis apropriadas e validadas.
- Utilizar uma fonte de tempo confiável e documentar o tempo de cada ação realizada.
- Pode ser apropriado associar o DEFR com a potencial evidência digital, utilizando assinaturas digitais, biometrias e fotografias.

**NOTA** A ação de pressionar o botão de energia do dispositivo digital pode estar configurada para iniciar um documento que pode alterar ou excluir informação do sistema antes de ser desligado ou alertar sistemas conectados sobre a ocorrência de um evento inesperado de modo que pode apagar dados de valor probatório antes de serem identificados. Pode também ser configurado para acionar um dispositivo destinado a causar dano físico ao DEFR ou a outras pessoas presentes.

#### 7.1.3.2 Dispositivos digitais desligados

##### 7.1.3.2.1 Visão geral

É mais fácil manusear/tratar um dispositivo digital desligado comparado a um dispositivo digital ligado porque não há necessidade de aquisição de dado volátil. A Figura 5 ilustra as atividades que são aplicáveis à aquisição de dispositivo digital desligado



**Figura 5 – Diretrizes para aquisição de dispositivo digital desligado**

#### 7.1.3.2.2 Aquisição de dispositivo digital desligado

A seguir, estão as atividades para aquisição de dispositivo digital quando é encontrado desligado:

- Assegurar-se de que o dispositivo está de fato desligado.
- Se apropriado, remover o armazenamento a partir do dispositivo digital desligado, se já não foi removido. Rotular o armazenamento como um armazenamento suspeito e documentar todos os detalhes, como fabricação, nome do modelo, número de série e tamanho do armazenamento.
- Executar o processo de imagem utilizando ferramentas de imagem validadas para a criação de uma cópia da evidência digital do disco suspeito.

**NOTA** Na maioria dos casos, não é recomendado que a mídia de armazenamento seja removida do dispositivo digital até a sua aquisição já que, uma vez removida, aumenta o risco de danificá-la ou confundi-la com outras mídias de armazenamento. Convém que sejam desenvolvidos e seguidos procedimentos locais em relação à necessidade de remover discos rígidos.

#### 7.1.3.3 Dispositivos digitais de missão crucial

Em alguns casos, não é possível que dispositivos digitais sejam desligados devido à natureza crucial dos sistemas. Nestes sistemas, servidores em centros de dados que podem também servir clientes de serviços inocentes, sistemas de vigilância, sistemas médicos e muitos outros, podem ser crucialmente afetados se forem interrompidos ou desligados. Recomenda-se cuidado especial ao lidar com tais sistemas.

Quando não for possível que o dispositivo digital seja desligado, conduzir a aquisição imediata e/ou aquisição parcial, como discutido em 7.1.3.1.2 e 7.1.3.4.

#### 7.1.3.4 Aquisição parcial

Aquisição parcial pode ser realizada devido a várias razões, como:

- O sistema de armazenamento é muito grande para ser adquirido (por exemplo, servidor de banco de dados);
- Um sistema é muito crucial para ser desligado;
- Quando somente dados selecionados a serem adquiridos contêm outros dados irrelevantes dentro do mesmo sistema; ou

- Quando compelido por autoridade legal, como um mandado de busca, que limita o escopo da aquisição.

Quando a decisão é para a realização de aquisição parcial, convém que as atividades para aquisição incluam, mas não se limitem a, os seguintes:

- Identificação de pasta(s), arquivo(s) ou qualquer outro relevante sistema proprietário disponível para aquisição do dado desejado,
- Condução da aquisição lógica nos dados identificados.

#### **7.1.3.5 Mídia de armazenamento digital**

Vários tipos de mídia de armazenamento digital podem ser encontrados no cenário de um incidente. Geralmente estes são os tipos menos voláteis de dados e podem ser de menor prioridade durante a coleta e aquisição. Isso não significa que não são importantes porque, em muitos casos, mídias de armazenamento digital externas contêm a evidência que os analistas estão procurando. O DEFR precisa garantir o seguinte:

- Checar e documentar a localização (por exemplo, bandejas de entrada de CD ou DVD, cabo e conector, porta de USB etc.), fabricante, marca, modelo e número de série (se algum) de cada mídia de armazenamento digital encontrada.
- Decidir pela coleta da mídia de armazenamento digital identificada ou conduzir uma aquisição no local. Recomenda-se que a decisão seja baseada na natureza do incidente e recursos disponíveis. A fim de conduzir a aquisição no local da mídia de armazenamento digital (principalmente disco rígido), referir-se à Figura 4.
- Se o DEFR decide e é permitido coletar a mídia de armazenamento digital, é recomendado que a mídia coletada seja embrulhada ou colocada em embalagem apropriada.
- Rotular toda mídia de armazenamento digital e quaisquer partes associadas a ela. Não é recomendado que rótulos de evidências sejam colocados diretamente sobre as partes mecânicas da mídia digital, nem que cubram ou ocultem informações importantes, como o número de série, número do modelo e número da peça. Convém que toda mídia coletada seja adquirida e armazenada de modo a garantir sua integridade. Quando possível, recomenda-se que a evidência seja selada com selos invioláveis, e convém que o DEFR ou pessoa responsável assine na etiqueta.
- É recomendado que a mídia de armazenamento digital coletada seja armazenada em um ambiente adequado para preservação do dado.
- Diferentes mídias de armazenamento digital têm diferentes capacidades de retenção de dados. Recomenda-se que o DEFR esteja ciente do período de tempo máximo aceitável especificado pela jurisdição relevante, no que diz respeito à capacidade de retenção de dados da mídia de armazenamento digital.

#### **7.1.4 Preservação**

Depois que o processo de aquisição é completado, é recomendado que o DEFR sele o dado adquirido usando funções de verificação ou assinaturas digitais para determinar que as cópias das evidências digitais são equivalentes ao original. Além disso, os aspectos de segurança requerem controles que aplicam os princípios da preservação da confidencialidade, integridade e disponibilidade da potencial

evidência digital. A fim de proteger contra espoliação, convém que os aspectos do ambiente sejam considerados com medidas apropriadas. O DEFR precisa assegurar o seguinte:

- Uso de uma apropriada função de verificação para fornecer evidência de que os arquivos copiados são equivalentes aos originais.
- Pode ser apropriada a associação do DEFR com a potencial evidência digital adquirida usando de assinaturas digitais, biometrias e fotografias.

Todos os dispositivos digitais coletados precisam ser apropriadamente preservados. Diferentes tipos de dispositivos digitais podem requerer diferentes métodos de preservação. A potencial evidência digital precisa ser preservada durante toda a sua vida útil, que pode variar por meio de jurisdições e políticas organizacionais.

**NOTA** Como uma alternativa para vedação do dado adquirido com funções de verificação ou assinaturas digitais, o DEFR também pode usar características biométricas. A biometria utiliza características físicas e comportamentais para determinar a identidade de um indivíduo. Ao anexar a característica biométrica à evidência adquirida, pode-se assegurar que a evidência não seja adulterada sem comprometer a característica biométrica.

## 7.2 Dispositivos de rede

### 7.2.1 Identificação

#### 7.2.1.1 Visão geral

No contexto desta seção, dispositivos de rede são considerados como computadores ou outros dispositivos digitais que estão conectados à rede no modo com fio ou sem fio. Estes dispositivos de rede podem incluir *mainframes*, servidores, computadores de mesa, pontos de acesso, interruptores, *hubs*, roteadores, dispositivos móveis, PDA, PED, dispositivos de *Bluetooth*, sistemas CFTV e muitos outros. Notar que se os dispositivos digitais estiverem conectados a rede, é difícil de determinar onde a potencial evidência digital sendo procurada está armazenada. O dado pode ser localizado em qualquer lugar da rede.

A identificação de um dispositivo digital inclui componentes como logotipo do fabricante, número de série, apoios e adaptadores de energia. O DEFR pode considerar os seguintes aspectos como meios de identificação:

- Características do dispositivo: O modo de fabricação e o fabricante de um dispositivo digital podem, às vezes, ser identificados pelas características observáveis, particularmente se existirem elementos únicos de *design*.
- Interface do dispositivo: O conector de energia é frequentemente específico a um fabricante e a um auxílio confiável para a identificação.
- Etiqueta do dispositivo: Para dispositivos móveis desligados, informações obtidas do interior da cavidade da bateria podem ser reveladoras, particularmente quando acoplado com uma base de dados apropriada. Por exemplo, a IMEI é um número de 15 dígitos que indica a fabricação, tipo do modelo e país de aprovação para dispositivos GSM; o ESN é um identificador exclusivo de 32 bits documentado pelo fabricante no *chip* protegido de um telefone móvel – os primeiros 8-14 bits identificam o fabricante e os bits remanescentes identificam o número de série atribuído.
- Pesquisa reversa: No caso de telefones móveis, se o número do telefone é conhecido, a pesquisa reversa pode ser utilizada para identificar o operador de rede.

Devido ao pequeno tamanho dos dispositivos móveis em geral, o DEFR precisa ter cuidado extra para identificar todos os tipos de dispositivos digitais que podem ser relevantes para o caso. O DEFR precisa proteger o cenário do incidente suspeito e assegurar que nenhum indivíduo ou quaisquer outros dispositivos digitais sejam removidos do cenário. É recomendado que dispositivos digitais que podem conter evidências digitais sejam protegidos de acessos não autorizados.

**NOTA** Em alguns casos, não é recomendado que a comunicação seja interrompida. Informar os indivíduos autorizados sobre possíveis problemas (por exemplo, não alertar indivíduos desconhecidos sobre o desligamento do dispositivo).

### 7.2.1.2 Pesquisa do cenário físico do incidente e documentação

Antes que qualquer aquisição ou coleta possa ser feita, convém que o cenário do incidente seja documentado de forma visual, seja fotografando, filmando ou desenhando a aparência do cenário, logo após a entrada. Recomenda-se que a escolha do método da documentação seja ponderada com as circunstâncias, custo, tempo, recursos disponíveis e prioridades. É recomendado que o DEFR documente todos os outros itens do cenário que possam conter potenciais materiais relevantes, como notas rabiscadas, anotações, agendas etc.

- É recomendado que o DEFR documente o tipo, marca, modelo e números de série de quaisquer dispositivos digitais utilizados e identifique todos os dispositivos digitais que talvez sejam necessários serem adquiridos ou coletados durante este estágio inicial. Convém que todos os dispositivos móveis e os itens associados, como cartões de memórias, cartões SIM, carregadores e apoios encontrados no cenário, seus números de série associados e quaisquer características identificadoras sejam documentados e coletados, se requerido. Também tentar encontrar as embalagens originais dos telefones móveis; estes podem conter notas com códigos PIN e PUK.
- Se o dispositivo estiver em rede, convém que o DEFR identifique os serviços prestados pelos dispositivos para compreender as dependências e para apurar a crucialidade dos dispositivos ligados às redes antes de decidir sobre desconectar o dispositivo da rede. Isto é importante se os dispositivos estão servindo para funções de missão crítica que não podem tolerar qualquer tempo de inatividade ou para evitar destruição da potencial evidência digital. No entanto, se parecer haver ameaças em andamento à rede-base do dispositivo, o DEFR pode ter que decidir acerca da desconexão do dispositivo da rede para proteger a potencial evidência digital.
- Se o dispositivo em rede é um sistema CFTV, é recomendado que o DEFR anote os números de câmeras conectadas ao sistema, bem como qual destas câmeras estão em operação ativa. Convém que o DEFR também anote o modo de fabricação, modelo e configurações básicas do sistema, como configurações de exibição, configurações de registro em execução e o local de armazenamento, de modo que se alterações tiverem de ser feitas para facilitar o processo de coleta e aquisição, será possível retornar o sistema ao seu estado original.
- Na medida do possível, convém que o estado dos dispositivos digitais permaneçam como encontrado. Geralmente, se os dispositivos digitais estiverem desligados, não é recomendado que o DEFR ligue-os, e, se estiverem ligados, não é recomendado que o DEFR desligue-os. Isto pode prevenir espoliação desnecessária da potencial evidência digital. Um dispositivo que possui baterias que podem acabar precisa ser carregado para garantir que a informação não seja perdida. O DEFR precisa identificar potenciais carregadores de mídia e cabos durante esta fase. Se é recomendado que um dispositivo seja transportado e examinado em data futura indeterminada, pode ser apropriado desligá-lo para minimizar potencial dano ao dado contido no dispositivo.
- Recomenda-se que o DEFR também considere a utilização de detector de sinal de rede sem fio para detectar e identificar sinais de rede sem fio a partir de dispositivos de rede sem fio que podem estar escondidos. Pode haver casos em que um detector de sinal de rede sem fio não seja usado devido a restrições de custo e tempo, e convém que o DEFR documente isto.

## 7.2.2 Coleta, aquisição e preservação

### 7.2.2.1 Visão geral

O DEFR precisa decidir se coleta ou adquire a potencial evidência digital dos dispositivos digitais. A escolha precisa ser ponderada com as circunstâncias, custo, tempo, recursos disponíveis e prioridades.

Se o DEFR decidiu por desconectar os dispositivos, os processos para coleta ou aquisição da potencial evidência digital segue o descrito em 5.4. No caso em que não é possível que os dispositivos sejam desconectados da rede devido à crucialidade de sua função ou da probabilidade de destruição da potencial evidência digital, é recomendado que o DEFR conduza prontamente a aquisição de imediato enquanto os dispositivos permanecem em rede.

**NOTA** É importante ter os procedimentos-padrão razoáveis que empreguem ferramentas validadas, acopladas com uma boa documentação e um DEFR experiente e treinado.

A coleta e a aquisição da potencial evidência digital a partir de dispositivos móveis conectados à rede são complicadas porque podem existir em múltiplos estados e modos de interação, como *Bluetooth*, radiofrequência, *touch screen* e infravermelho. Além disso, diferentes fabricantes de dispositivos móveis utilizam diferentes tipos de sistemas de operação, exigindo diferentes métodos de aquisição da evidência. Existe também uma vasta gama de cartões de memória que são utilizados com dispositivos móveis, e remover estes cartões de memória de dispositivos móveis ligados pode interferir nos processos em execução.

Geralmente, dispositivos móveis, como os PDA e telefones móveis, precisam ser ligados a fim de que seja adquirida a potencial evidência digital. Estes dispositivos podem continuamente alterar o seu ambiente operacional enquanto ligados, por exemplo, o temporizador pode ser atualizado. O problema associado é que não é possível que duas cópias de evidência digital do mesmo dispositivo passem pelas funções-padrão de verificação, como o *hash*. Nesta situação, funções alternativas de verificação que identificam áreas em comum e/ou diferentes podem ser mais apropriadas.

É importante que o DEFR não introduza dispositivos de rede sem fio ou *Bluetooth* na cena que possa alterar o nivelamento da informação nos potenciais dispositivos digitais. Isto é particularmente importante se o investigador necessita conhecer quais dispositivos foram conectados.

Se o DEFR decidiu por seguir um processo de aquisição, é recomendado que os dispositivos de rede sejam mantidos em funcionamento para maior análise para determinar outros dispositivos conectados à rede de dispositivos. Convém que o DEFR considere a possibilidade de sabotagem pela suspeita de uma rede ativa conectada e decida pelo monitoramento do sistema ou por desconectá-lo.

### 7.2.2.2 Diretrizes para coleta de dispositivos de rede

Em algumas circunstâncias, pode ser apropriado deixar os dispositivos de rede conectados de forma que sua atividade possa ser monitorada e documentada pelo DEFR e/ou DES com poderes apropriados. Onde isto não é necessário, recomenda-se que os dispositivos sejam coletados como descrito abaixo:

- É recomendado que o DEFR isole o dispositivo da rede, quando estiver certo de que dados não relevantes serão substituídos por esta ação e nenhum mau funcionamento ocorrerá nos sistemas importantes (como instalações de gestão de sistema em hospitais). Isto pode ser feito desconectando as redes com fio do sistema de telefone ou portas de rede ou pela desativação dos pontos de acesso da rede sem fio.
- Antes da desconexão das redes com fio, é recomendado que o DEFR trace as conexões até os dispositivos digitais e rotule as portas para futura reconstrução de toda a rede. Um dispositivo pode ter mais de um método de comunicação. Por exemplo, um computador pode ter os LAN com

fio de rede, um *modem* de rede sem fio e cartões telefônicos móveis. Os PED podem também ser conectados à rede por meio de rede sem fio, conexões *Bluetooth* ou conexões de rede de telefone móvel. Recomenda-se que o DEFR tente identificar todos os métodos de comunicação e realizar atividades apropriadas para proteger a potencial evidência digital contra destruição.

- Estar ciente de que remover energia de dispositivos de rede neste ponto pode destruir um dado volátil, como um processo em execução, conexões de rede e dados armazenados na memória. O sistema operacional local pode ser não confiável e reportar falsa informação. É recomendado que o DEFR capture esta informação usando métodos confiáveis verificados antes de remover a energia dos dispositivos. Uma vez que o DEFR está certo de que nenhuma potencial evidência digital será perdida como resultado, as conexões dos dispositivos digitais podem ser removidas.
- Se a coleta antecede a aquisição e sabe-se que o dispositivo contém memória volátil, recomenda-se que o dispositivo seja constantemente conectado a uma fonte de energia.
- Se o dispositivo móvel está desligado, acondicionar cuidadosamente, selar e etiquetar o dispositivo. Isto é para evitar qualquer operação acidental ou deliberada nas chaves ou botões. Como precaução, convém que o DEFR também considere utilizar caixas *Faraday* ou blindadas.
- Sob algumas circunstâncias, é recomendado que os dispositivos móveis sejam desligados no momento da coleta para prevenir que dado seja alterado. Isto pode acontecer por meio da conexão de entrada e de saída ou de comandos que podem causar a destruição da potencial evidência digital.
- Subsequentemente, cada dispositivo digital pode ser tratado como um dispositivo independente (referência a 7.1) até que seja examinado. Durante o exame, convém considerar como um dispositivo de rede.

**NOTA** É possível implementar uma forma de rede utilizando dispositivos de armazenamento removíveis como mídia de transmissão. Recomenda-se que o DEFR considere se os dispositivos que estão sendo coletados podem ter sido usados deste modo e busque informação sobre outros dispositivos, como um *sneakernet*.

#### 7.2.2.3 Diretrizes para aquisição de dispositivos de rede

Em situações em que dispositivos estão conectados a uma rede, há a possibilidade de que os dispositivos estejam conectados a mais de uma (1) rede física e/ou virtual. Por exemplo, um dispositivo que parece ter uma (1) rede visível física de conexão pode, de fato, estar executando uma Rede Virtual Privada (VPN) e máquina virtual com mais de um (1) endereço de IP. Como tal, recomenda-se que, antes de desconectar o dispositivo da rede, o DEFR conduza uma aquisição lógica de dado relacionado à conexão de rede lógica (por exemplo, conectividade com a *internet*). O dado relacionado inclui, mas não está limitado à, configuração de IP e tabelas de roteamento.

Para um dispositivo de rede que necessita estar constantemente ligado, convém que o dispositivo esteja impedido de interagir com rede de rádio sem fio, incluindo dispositivos de GPS habilitados. Recomenda-se que o DEFR utilize métodos permitidos pela legislação local para isolar sinais de rádio. É recomendado cuidado, no entanto, para garantir que o dispositivo tenha uma adequada fonte de energia, já que métodos de isolamento podem causar a ele o uso de energia adicional ao tentar contactar uma rede. Métodos de isolamento podem incluir, mas não estão limitados a, o seguinte:

- Utilizar um dispositivo de interferência que seja capaz de bloquear transmissão por meio da criação de forte interferência quando o dispositivo emite sinais no mesmo alcance de frequência que os dispositivos móveis usados.

**NOTA 1** Utilizar dispositivos de interferência pode violar requisitos legais em algumas jurisdições.

NOTA 2 Utilizar dispositivos de interferência pode afetar negativamente o comportamento de dispositivos eletrônicos, como equipamentos médicos.

- Utilizar uma área de trabalho protegida para conduzir exames com segurança em um local fixo. A proteção pode ser feita para a área inteira de trabalho ou por meio da criação de um abrigo de *Faraday* que permite portabilidade. Alimentar cabos para dentro do abrigo é problemático, no entanto, uma vez sem o isolamento adequado, eles podem comportar-se como uma antena, anulando o propósito do abrigo. O espaço de trabalho pode ser também muito restrito.
- Utilizar uma área de trabalho protegida para conduzir os exames com segurança em um local fixo. Uma blindagem contra frequência de rádio no espaço de trabalho ou receptáculo (uma gaiola *Faraday*) pode ser utilizada para prevenir conexões à rede de trabalho.

NOTA 3 É recomendado que todos os métodos de bloqueio de acesso às redes de trabalho sejam validados para uso nas frequências apropriadas. Convém que esta validação estenda-se para cabos que passam pela blindagem.

- Utilizar um (U)SIM substituto que imite a identidade do dispositivo original e previna o acesso à rede de trabalho pelo dispositivo. Estes cartões são capazes de induzir em erro o dispositivo a aceitá-los como o (U)SIM original e permitir que exames sejam conduzidos com segurança em qualquer local. Recomenda-se que o (U)SIM seja validado para o dispositivo e rede de trabalho antes da utilização.
- Desabilitar os serviços da rede de trabalho, organizando com a operadora de serviço móvel e identificando detalhes nos serviços a serem desabilitados (por exemplo, o identificador do equipamento, identificador do assinante ou número de telefone). No entanto, tais informações não estão sempre prontamente disponíveis quando o processo de coordenação e confirmação pode impor atraso.

É recomendado que o DEFR conduza a aquisição imediata do dispositivo móvel antes de remover a bateria (por exemplo, para acessar o cartão SIM). Isto pode ser feito a fim de prevenir perda da potencial informação importante na memória RAM do telefone ou para acelerar o processo de exame (por exemplo, onde se acredita que o dispositivo pode estar protegido por um código PIN e/ou PUK que tomaria uma significante parte do tempo para obtê-lo).

NOTA 4 Convém que o DEFR assegure que a coleta e aquisição da potencial evidência digital está de acordo com a leis e regulamentos da jurisdição local, como requerido com base nas circunstâncias específicas.

#### **7.2.2.4 Diretrizes para preservação de dispositivos de rede**

Devido à natureza dos dispositivos digitais e da potencial evidência digital, as diretrizes para preservação de dispositivos de rede são similares à preservação de computadores, dispositivos periféricos e mídias de armazenamento digital. Referir-se a 7.1.4 para diretrizes detalhadas na preservação de dispositivos.

## Anexo A

(informativo)

### DEFR — Competências essenciais e descrição de competências

**Tabela A.1 – Exemplos de descrição de competências**

Nº	Habilidades fundamentais	Descrição das habilidades fundamentais	Descrição de competências		
			Conscientização (1)	Conhecimento (2)	Habilidade (3)
1	Identificação da evidência digital	Caracterizar dispositivo digital, componentes, informações que podem auxiliar a investigação e leis relevantes para manuseio da potencial evidência digital e crimes cibernéticos. Identificar requisitos de ferramentas para coleta e aquisição de dados e dispositivos e avaliação de riscos.	Uso geral de TI e administração de múltiplos tipos de dispositivos de TI e dispositivos de rede; procedimentos investigativos no cenário do crime; determinação do estado do dispositivo; avaliação da informação como evidência; dispositivos e informação relacionados a redes forenses.	Registros e configuração da aplicação/ identificação do sistema e aplicação de registros de entradas, incluindo registros de entradas em <i>email</i> , <i>web</i> , registros de acessos, arquivos de senhas, arquivos <i>sysconfig</i> , informação de IP local; funcionalidade do dispositivo e dependências; habilidade para compreender impactos sobre evidências voláteis e não voláteis.	Análise especial; interpretação de registros para detecção de intrusão na identificação de outros sistemas afetados (algumas jurisdições requerem confirmação da presença da evidência antes da coleta); identificar senhas necessárias para os respectivos dispositivos antes da coleta; identificar diagrama de rede e mecanismos de controles de acessos para compreender as dependências; endereços de <i>link</i> de IP e endereços de <i>MAC</i> para confirmação do dispositivo.

Tabela A.1 (continuação)

Nº	Habilidades fundamentais	Descrição das habilidades fundamentais	Descrição de competências		
			Conscientização (1)	Conhecimento (2)	Habilidade (3)
2	Coleta da evidência digital	Requisitos de ferramentas e implementação de acondicionamento de evidência digital, proteção contra ameaças ambientais. Áreas protegidas incluem segurança da informação.	Segurança na coleta de dados gerais; princípios e estrutura das ferramentas básicas; determinar o melhor método de coleta para preservar ao máximo a informação relevante para o incidente.	Formular e executar o processo de coleta; coletar evidência; gerar documentos probatórios; cadeia de custódia da evidência; processo de controle de qualidade da evidência; entrevista com suspeitos.	Otimização do processo de coleta; documentar a evidência que não é possível que seja adquirida devido a várias restrições; coletar senhas, chaves, <i>dongles</i> , e outras informações necessárias para conduzir a análise em laboratório.
3	Aquisição da evidência digital	Aplicar os requerimentos da aquisição da potencial evidência digital na forma lógica, assegurando a repetibilidade, auditabilidade, reproduzibilidade e justificabilidade. Áreas abrangidas são a aquisição realizada sobre um sistema ligado, a aquisição realizada sobre um sistema desligado e rede forense.	Compreender a informação disponível nos dispositivos digitais, bancos de dados, documentos gerados pelo sistema, dados gerados pelo usuário e dados voláteis; estruturas de arquivos dos sistemas Unix e Windows e aplicações; ter ciência dos impactos sobre dados voláteis.	Saber como determinar requisitos para armazenamento; executar procedimentos de aquisição de imagens (por exemplo, aquisição de mídia de armazenamento parcial e integral); aquisição realizada sobre um sistema ligado, aquisição realizada sobre um sistema desligado; geração de valor de <i>hash</i> .	Habilidade para conduzir aquisição de mídia de armazenamento digital incluindo RAID, bancos de dados, aplicações e dispositivos miniaturizados; compreender dependências e impactos sobre diferentes métodos de aquisição.

**Tabela A.1** (continuação)

Nº	Habilidades fundamentais	Descrição das habilidades fundamentais	Descrição de competências		
			Conscientização (1)	Conhecimento (2)	Habilidade (3)
4	Preservação da evidência digital	Aplicar e avaliar os requerimentos para preservação da potencial evidência digital, compreender fatores e parâmetros que influenciam a sua exatidão. Áreas abrangidas são a metodologia, manutenção da cadeia de custódia, manuseio de dispositivos de computador e manuseio de mídias digitais armazenadas.	Compreender as exigências e procedimentos para manutenção da cadeia de custódia contra requerimentos legais; impactos ambientais tais como umidade, temperatura e choques em direção ao dispositivo digital; compreender as opções de acondicionamento, requisitos de transporte e armazenamento.	Saber como gerar documentos da evidência auditáveis; definir parâmetros para os documentos; segurança da informação, ameaças, vulnerabilidades controles da evidência digital.	Aplicar medidas para proteger a evidência digital sob a forma de grandes dispositivos para dispositivos miniaturizados portáteis; procedimento para documentar detalhes da evidência.

**Tabela A.2 – Definição de competências**

1	Conscientização – Reconhecer, identificar – perguntar quando houver necessidade de auxílio
2	Conhecimento – Adquirir por meio de instrução formal ou trabalho em equipe. Contribuir, participar – fazer com auxílio
3	Experiência – Experiência comprovada por meio da aplicação no ambiente de trabalho. Trabalhos sem supervisão. Aplicar, demonstrar – fazer sem auxílio.

NOTA      Competência de um DEFR pode variar de uma jurisdição para outra.

## Anexo B

(informativo)

### **Requisitos mínimos de documentação para transferência de evidência**

Recomenda-se que o DEFR seja responsável pelos dados adquiridos e dispositivos digitais durante todo o tempo em que eles estão sob custódia do DEFR. A fim de manter este controle, o DEFR precisa estar apropriadamente autorizado, treinado e qualificado. No entanto, uma vez que a legislação local é um fator determinante na habilidade do DEFR para aderir a todos os três requisitos esperados, a competência de um DEFR pode variar de uma jurisdição para outra. Como resultado, é possível que a documentação requerida para transferência interjurisdicional da evidência digital não seja igual em jurisdições diferentes.

Portanto, um conjunto mínimo de requisitos documentais precisa ser especificado para facilitação da transferência interjurisdicinal da potencial evidência digital. Esses requisitos documentais precisam ser considerados com os pontos de documentação mencionados em 6.6. Uma vez que esta Norma não substitui os requisitos legais específicos de qualquer jurisdição, ela serve como um guia prático para transferência de potencial evidência digital por meio das fronteiras jurisdicionais.

A documentação mínima a ser comunicada é:

- o nome e endereço da autoridade relevante;
- a confirmação da autorização, instrução e qualificações do DEFR;
- o propósito da verificação;
- quais ações foram executadas;
- quem fez o quê e quando;
- a cadeia de custódia pertencente à investigação específica;
- lista descritiva da potencial evidência digital e da mídia de armazenamento digital coletada e adquirida; e
- informações relativas a quaisquer exames, testes ou investigações utilizadas para produzir a cópia da evidência.

Os requisitos específicos de jurisdições podem incluir o seguinte:

- Se a evidência é considerada assim por uma opinião de especialista, reconhecimento de relevante testemunha especialista em Código de Conduta; e
- uma ordem judicial que especifica a documentação necessária para transferência e a razão para a transferência.

## Bibliografia

- [1] ILAC-G19:2002. *Guidelines for forensic science laboratories*. Disponível em: [www.ilac.org/documents/g19\\_2002.pdf](http://www.ilac.org/documents/g19_2002.pdf)
- [2] IOCE, *G8 proposed principles for the procedures relating to digital evidence*. Disponível em: <http://ioce.org/core.php?ID=5>
- [3] ISO/IEC 15489:2001, *Information and Documentation – Records Management*
- [4] ABNT NBR ISO/IEC 17024:2003, *Avaliação de conformidade – Requisitos gerais para organismos que realizam certificação de pessoas*
- [5] ABNT NBR ISO/IEC 17043:2010, *Avaliação de conformidade – Requisitos gerais para ensaios de proficiência*
- [6] ABNT NBR ISO/IEC 27001, *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos*
- [7] ABNT NBR ISO/IEC 27002, *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Código de prática para a gestão da segurança da informação*
- [8] ISO/IEC 24760-1, *Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts*
- [9] ISO/IEC 27031:2010, *Information technology – Security techniques – Guidelines for ICT readiness for business continuity*
- [10] ISO/IEC 27035:2011, *Information technology – Security techniques – Information security incident management*
- [11] *Forensic Science Society Academic Accreditation Standards & CPD*. Disponível em: <http://www.forensic-science-society.org.uk>
- [12] *Guidelines for evidence collection and archiving*. Disponível em: <http://www.ietf.org/rfc/rfc3227.txt>

