Diário Eletrônico (apenas matérias ADMINISTRATIVAS) nº 109
Disponibilização: 13/06/2024

SEÇÃO JUDICIÁRIA DE SÃO PAULO
Rua Peixoto Gomide, 768 - Bairro Jardim Paulista - CEP 01409-903 - São Paulo - SP - www.jfsp.jus.br

# NOTA TÉCNICA NI CLISP 21/2024

JUSTIÇA FEDERAL

CENTRO LOCAL DE INTELIGÊNCIA JUSTIÇA FEDERAL EM SÃO PAULO

**CENTRO DE INTELIGÊNCIA DA SECÃO JUDICIÁRIA DE SÃO PAULO - CLISP**

Assunto: Provas digitais em âmbito Criminal

Relatoras: Raecler Baldresca e Flávia Serizawa e Silva

Revisoras: Letícia Mendes Gonçalves Hillen e Milenna Marjorie Fonseca da Cunha

## Sumário



## I - Introdução

O desenvolvimento acelerado do mundo digital tem alterado profundamente as relações sociais entre os indivíduos e a forma pela qual tem se estabelecido o relacionamento entre países de todo o mundo, impactando sobremaneira os institutos jurídicos até então prevalentes.

Especificamente em matéria criminal, não é novidade o aumento exponencial da criminalidade cibernética, assim como da existência de vestígios digitais, presentes em praticamente toda investigação de infrações penais, o que tem se mostrado um desafio aos órgãos de persecução, responsáveis por viabilizar a aplicação da lei penal.

Nesse sentido, chama-se atenção para a promulgação da Convenção de Budapeste pelo Brasil em abril de 2023 (Decreto 11.491/2023), que trata dos crimes cibernéticos, reconhecendo a necessidade de uma *política criminal comum destinada à proteção da sociedade contra o crime cibernético*, bem como da *cooperação internacional como instrumento eficiente para o controle dessa espécie de criminalidade*.

Replicando a fórmula que os acordos internacionais em matéria penal têm utilizado nas últimas décadas, a Convenção de Budapeste também busca uniformizar institutos e procedimentos, além de prever instrumentos de investigação e cooperação entre os órgãos internacionais. Ao aderir ao tratado, os países se comprometem a adotar, em seus respectivos territórios, medidas para enfrentar (i) os crimes praticados contra a confidencialidade, a integridade e a disponibilidade de dados e sistemas de computador; (ii) os crimes informáticos; (iii) os crimes relacionados ao conteúdo da informação; e, finalmente, (iv) a violação de direitos autorais e de direitos correlatos.

Em relação às evidências, o acordo prevê meios para a preservação expedita de dados armazenados e poderes de ordem de exibição e de busca e apreensão de dados de computador para as autoridades locais, com a finalidade de obtenção e preservação de provas digitais.

No que diz respeito à legislação interna, a Lei 12.965/14 (Marco Civil da Internet) caminhou no mesmo sentido, prevendo o dever de Guarda de Registros de Conexão (por pelo menos um ano) e de Registros de Acesso a Aplicações de Internet na Provisão de Conexão (por pelo menos seis meses), podendo tal prazo ser estendido mediante requisição das autoridades competentes, sendo o seu acesso condicionado à autorização judicial. Tais normas também demonstram a preocupação e a necessidade de obtenção e preservação de evidências digitais que possam auxiliar na elucidação de eventual atividade criminosa praticada por meios tecnológicos.

Note-se que, quanto mais ampla e tecnológica a investigação, maior será a complexidade metodológica e científica envolvida e, consequentemente, maior será o debate sobre a prova e sua valoração. Nesse sentido, compreender a metodologia, os instrumentos e a técnica utilizada na captação e análise dos vestígios deixados pelos crimes cibernéticos será tarefa de extrema importância ao processo penal.

Contudo, por se tratar de uma nova espécie de evidências, há o risco de que os responsáveis pela persecução penal deixem de observar as cautelas que devem ser adotadas em relação às provas digitais, desde o seu reconhecimento até o seu armazenamento, o que muitas vezes dificulta que se assegure a sua integridade (ausência de alteração), precisão, autenticidade e reprodução, podendo inviabilizar a prova.

De fato, a inobservância de um procedimento padrão, especialmente por parte dos primeiros agentes que travam contato com os vestígios digitais e que são os responsáveis por sua coleta, pode prejudicar a segurança e a confiabilidade da prova e, em última análise, gerar impunidade.

Tal constatação se acentuou com a promulgação da Lei 13.964/19, que introduziu em nosso Código de Processo Penal regramento sobre a necessidade de preservação da cadeia de custódia, definindo-a como o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte, bem como disciplinando todas as suas fases.

Quanto ao ponto, a necessidade de um protocolo uniforme e seguro de tratamento dessas provas deve iniciar-se desde o local do crime em que encontrado o vestígio (muitas vezes em cumprimento de mandado de busca e apreensão), com o seu reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte, sendo que eventuais falhas em qualquer parte dessa cadeia podem comprometer a confiabilidade ou a validade da prova.

Em razão disso, o objetivo desta Nota Técnica é reunir as melhores práticas para orientar os trabalhos de todos os envolvidos

na produção da prova digital, desde a sua identificação e desenvolvimento na fase policial até a sua apuração e valoração na fase judicial. Em especial, pretende-se informar os magistrados a respeito dos protocolos nacionais e internacionais existentes sobre o tema e indicar diretrizes para o aperfeiçoamento da atuação jurisdicional nesse contexto.

## II – As provas digitais: considerações gerais sobre a aquisição e preservação

Qualquer informação que tenha sido produzida, armazenada ou transmitida por meios eletrônicos pode constituir prova digital, incluindo os elementos nascidos em formato digital – como os dados de redes sociais, de dispositivos eletrônicos e armazenados em nuvens ou provedores de serviços - e também aqueles originalmente analógicos que foram digitalizados posteriormente.

A principal característica da prova digital é a sua imaterialidade, uma vez que, embora se revele necessariamente por um suporte transportador, consiste em uma informação de dados em bits sequenciais, daí a sua volatilidade e fragilidade.

Em razão dessas peculiaridades, exige-se cautela suplementar em sua aquisição e manipulação, a fim de garantir a integridade e a autenticidade da prova, além da preservação da confidencialidade das informações às quais o agente público tenha acesso[1].

A integridade e a autenticidade garantem que a prova foi coletada em sua integralidade e sem qualquer modificação, contaminação ou parcialidade, permitindo inclusive a repetição de todos os procedimentos feitos pelos peritos oficiais, salvaguardando, dessa forma, a cadeia de custódia e viabilizando o contraditório digital.

Quanto à sua preservação, a prova digital pode ser obtida tanto a partir da apreensão de dispositivos físicos, quanto do acesso remoto a informações mantidas de forma online, via sistema digital, nuvem ou rede. Na primeira hipótese, é necessário utilizar métodos para reter e preservar dados – realizando cópias espelho e cálculo da função *hash*[2] – bem como atentar para a cadeia de custódia e o registro dos equipamentos apreendidos e das informações coletadas. Para acesso às informações mantidas em sistemas digitais, nuvem ou rede, é fundamental o conhecimento de ferramentas tecnológicas e a obtenção de chaves de acesso que permitam o alcance das informações armazenadas.

Ressalte-se que, em qualquer caso, é preciso evitar a contaminação do material obtido e atentar para o fato de que poderá haver questionamentos a respeito do procedimento adotado na aquisição e no método científico utilizado no exame. Daí ser imperiosa a elaboração de relatórios diligenciais que permitam verificar como ocorreu o recolhimento das evidências, atestar o cumprimento dos procedimentos de preservação e afastar a possibilidade de contaminação.

Portanto, tais procedimentos devem ser observados desde o local em que encontrado o equipamento, especialmente nos casos de cumprimento de mandado de busca e apreensão, devendo, nesse caso, a autoridade judicial determinar as cautelas necessárias à obtenção e preservação das evidências, até a realização do exame pericial em si, com a elaboração de laudo pericial e posterior valoração.

## III – Padrões Metodológicos

Com vistas à observância da integridade e preservação das provas digitais, foram desenvolvidos internacionalmente padrões metodológicos e científicos para garantia do correto procedimento em investigações e análises de evidências digitais. Embora exista mais de um protocolo a esse respeito, todos eles levam em consideração as etapas da cadeia de custódia na produção da prova, nos seguintes termos:

- **ETAPA 1 – Recolha:** identificação e coleta de fontes de prova relevantes no material disponível.
- **ETAPA 2 – Autenticação:** criação da cópia da fonte de prova digital, protegendo-a de alterações, confirmando sua integralidade e validando sua autenticidade, o que pode ser feito com a utilização da função *hash*.

- **ETAPA 3 – Exame e Preservação:** identificação e separação das fontes de prova relevantes ao processo, armazenamento e transporte das fontes de prova e registro cronológico.
- **ETAPA 4 – Relatório:** relatório pericial, com linguagem acessível e descrição dos procedimentos.
- **ETAPA 5 – Arquivamento do material**

Em âmbito internacional, em 1995, foi criada a IOCE – *International Organization on Computer Evidence* – para fornecer às agências internacionais um fórum para troca de informações sobre investigações de delitos informáticos. Nesse contexto, foi realizada em 1999 a Conferência Internacional de Ciência da Saúde e Forense – que aprovou as seguintes diretrizes:

- Ao aproveitar a evidência digital, as ações adotadas não devem alterar essas evidências;
- Quando é necessário que uma pessoa tenha acesso a provas digitais originais, essa pessoa deve ser competente na análise forense;
- Todas as atividades relacionadas à apreensão, acesso, armazenamento ou transferência de evidências digitais devem ser totalmente documentadas, preservadas e disponíveis para revisão;
- Um indivíduo é responsável por todas as ações tomadas em relação à evidência digital enquanto a evidência está em sua posse;
- Qualquer entidade que seja responsável por aproveitar, acessar, armazenar ou transferir evidências digitais é responsável pelo cumprimento desses princípios.

Tais diretrizes foram fundamentais para a elaboração dos procedimentos nacionais de coleta, preservação e análise das provas digitais, que deram origem aos seguintes protocolos:

- Norma ISO (Organização Internacional de Padronização), em conjunto com a IEC (Comissão Eletrotécnica Internacional) 27037/2013 = estabelece diretrizes sobre identificação, coleta, aquisição e preservação da evidência digital - ABNT NBR ISO/IEC.

- PROCEDIMENTO OPERACIONAL PADRÃO DA SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA MINISTÉRIO DA JUSTIÇA (POP SENASP/MJ) = estabelece metodologia padrão para realização de perícia informáti forense envolvendo perícias em mídia de armazenamento computacional, em equipamentos computacionais portáteis, em local de informática e em local de internet.

De acordo com o POP, toda evidência digital válida deve apresentar três características fundamentais: relevância, confiabilidade e suficiência.

## IV - Recomendações para a Busca e Apreensão

Em regra, as diligências que envolvem acesso a fontes de prova digitais devem ser realizadas por agentes policiais especializados nesse tipo de operação e que possuam conhecimentos específicos em Ciência Forense Digital, ou ao menos, que tenham sido submetidos a treinamento para análise de equipamento no local da busca e a melhor forma de preservação dos dados nele contidos.

Contudo, não há como se afastar a possibilidade de que, durante o cumprimento de alguma busca e apreensão, o responsável pela diligência desconheça as cautelas necessárias, razão pela qual deve o magistrado indicar um protocolo de busca em sua decisão e incluir diversas recomendações no respectivo mandado.

Recomenda-se a identificação dos possíveis crimes praticados, bem como do que deve possivelmente ser apreendido (foco), determinando desde logo a sua identificação e devido isolamento, fixação (de preferências com fotos), coleta, acondicionamento e transporte, com o registro de todo esse procedimento.

Também se sugere a determinação de cópia de segurança para a análise e outra cópia selada para a defesa, bem como que

se evite a apreensão do equipamento, exceto se o pedido justificar o contrário (análise do crime investigado).

A principal questão que pode invalidar a utilização de determinada prova digital diz respeito à sua recolha, sendo preferível que se realize em modo off-line, o que assegura que não ocorra a alteração de dados até que seja feita uma cópia de segurança para a devida análise. Contudo, quando não for possível apreender ou desligar o sistema alvo ou se não for possível conectar às estações de processamento, a apreensão pode ser realizada em modo on-line, sendo importante, porém, a utilização de ferramentas de geração de cópias em tempo real.

Finalmente, quanto à preservação, também é de fundamental importância o acionamento, quando necessário, do Sistema de plantão 24 por 7, previsto na Convenção de Budapeste, que consiste em uma rede para contato disponível 24 horas por dia, 7 dias por semana, de modo a assegurar a assistência imediata para investigações ou procedimentos relacionados a crimes de computador e de dados, ou para a obtenção de provas eletrônicas de uma infração penal.

Tal assistência incluirá a facilitação, ou, se permitido pelas leis e costumes jurídicos locais, a adoção direta das seguintes medidas: fornecimento de suporte técnico, conservação de dados, coleta de provas, fornecimento de informação jurídica e localização de suspeitos.

Levando-se em consideração tais diretrizes, tem-se as seguintes cautelas na busca e apreensão das provas digitais:

(i) Sob o ponto de vista do objeto/material a ser apreendido:

- Busca de aparelhos e dispositivos de armazenamento de informação (off-line) e acesso às informações de um sistema digital por busca remota (on-line);
- Busca das fontes de provas digitais, ou seja, de cópia integral do dispositivo para a realização da triagem (do que é relevante para a investigação).

(ii) Quanto aos princípios que devem orientar a apreensão e o processamento das fontes de prova digital (ou conduta dos agentes):

- os agentes não podem adotar nenhum procedimento que possa alterar os dados de um dispositivo;
- apenas devem acessar os dados armazenados em um dispositivo agentes qualificados a extrair provas e explicar os procedimentos adotados;
- devem registrar todos os procedimentos do dispositivo e do recolhimento da fonte de prova de modo que um terceiro alcance o mesmo resultado ao adotá-lo;
- devem garantir que os princípios anteriores sejam cumpridos.

Ainda, é importante atentar para que seja observado:

- não basta a apreensão dos dispositivos, mas também é preciso utilizar métodos para reter e preservar dados (cópias espelho e cálculo da função *hash*);
- tecnologias de acesso remoto e obtenção de chaves de acesso aos repositórios de dados;
- quanto aos dispositivos móveis, a cadeia de custódia sobre o equipamento e sobre os dados coletados.

Resumindo, recomenda-se que o mandado de busca e apreensão envolvendo crimes ou provas digitais contenham o seguinte:

a) A devida explicitação dos possíveis crimes praticados e do que deve possivelmente ser apreendido;
b) A determinação:
   a. Para que se evite a apreensão do equipamento, exceto se o pedido justificar o contrário (análise do crime investigado).
   b. Em caso de apreensão, para que se proceda ao registro de todo o procedimento envolvendo o material custodiado, indicando: sua identificação, isolamento, fixação (de preferência com fotos), coleta,

acondicionamento e transporte.

c. Para confecção de cópia de segurança para análise e de cópia selada para a defesa.

d. Para que a recolha da prova digital seja, preferencialmente, realizada em modo off-line, a fim de assegurar a integridade dos dados até a realização de cópia de segurança para análise;

e. Em caso de apreensão on-line (diante da impossibilidade de apreensão ou desligamento do sistema alvo ou de conexão às estações de processamento), que sejam utilizadas ferramentas de geração de cópias em tempo real.

f. Para atentem à existência do Sistema de plantão 24 por 7, quando necessário.

## V - Recomendações na Realização de Exame Pericial

No que diz respeito aos exames periciais em si, o Ministério da Justiça, em consonância com seus congêneres de países estrangeiros[3], providenciou, desde 2013, o Procedimento Operacional Padrão em Perícia Criminal[4], incluindo a perícia em informática forense, justamente com a finalidade de conferir tratamento uniforme e seguro às perícias forenses em tal matéria.

Para tanto, são determinadas regras básicas para análise da prova, tais como a utilização de métodos para reter e preservar dados (cópia espelho e função *HASH*), afastar a possibilidade de contaminação por terceiros, bem como garantir a possibilidade de sua reprodução, de forma também a viabilizar a sua posterior submissão ao contraditório.

Referido procedimento abrange as perícias em (i) mídia de armazenamento computacional; (ii) equipamento computacional portátil (incluindo aparelhos celulares); (iii) local de informática; e (iv) local de internet, cujos principais pontos passam a ser destacados:

(i) Perícia Criminal em Mídia de Armazenamento Computacional

O procedimento inicia com a identificação e individualização de todo o material, a necessidade de duplicação dos dados contidos na mídia original para análise, devendo o exame ser efetuado na cópia, para evitar o risco de alteração de dados. O processamento dos dados inclui a recuperação de arquivos apagados, a expansão de arquivos compactados, o cálculo de *hashes* e a indexação de dados. Quanto à análise dos dados, pode ser feita via extração direta de arquivos (em que o objetivo é a obtenção do universo de arquivos existentes em determinada mídia) ou elucidação técnico-pericial (em que o objetivo é o esclarecimento sobre alguma questão técnico-pericial pontual sobre o material encaminhado). Finalmente, tem-se a elaboração de laudo, com todos os seus tópicos recomendáveis, bem como a anexação de mídia, se entender necessário.

(ii) Perícia Criminal em Equipamento Computacional Portátil

O procedimento inicia com a identificação e individualização de todo o material e a remoção do cartão SIM ou Micro SD. Em seguida, extraem-se os dados do equipamento portátil para uma mídia de trabalho, devendo iniciar-se com a clonagem do cartão SIM com ferramenta que desabilite as suas funções de comunicação com a rede de telefonia.

Caso exista uma senha não fornecida pelo proprietário, pode-se tentar o desbloqueio com programas forenses para tal finalidade, ou utilizando-se a senha padrão da operadora de telefonia, hipótese em que será necessária a expedição de ofício para que a forneça.

Nesse tipo de equipamento, geralmente é possível extrair os seguintes dados: informações de usuário, mensagens eletrônicas, informações de internet, de localização e de conexões, sendo ainda possível a recuperação de arquivos apagados. Também é necessário o cálculo de *hashes* dos arquivos selecionados. Finalmente, tem-se a elaboração de laudo, com todos os seus tópicos recomendáveis, bem como a anexação de mídia, se entender necessário.

(iii) Perícia Criminal em Local de Informática

O procedimento inicia com o isolamento físico do local de acesso dos equipamentos de informática, devendo ser fotografado o ambiente. Muitas vezes é necessária a análise de arquivos no local de crime devido à volatilidade dos vestígios computacionais, restrições de apreensão de equipamentos e constatação de flagrante delito. Tal exame pode ser classificado em dois tipos: *live* ou *post mortem*.

O exame *live* é recomendado se a máquina estiver ligada, especialmente se forem constatados documentos abertos, conversações online, armazenamento remoto de dados, criptografia de dados, programas em execução, proteção por criptografia, devendo ser efetuada cópia de seu conteúdo integral ou parcialmente, a depender do interesse.

O exame *post mortem* se destina a equipamentos desligados, sendo possível acessar a mídia sem efetuar alteração de seu conteúdo pelo uso de bloqueadores de escrita ou por meio de inicialização controlada.

Após, tem-se a extração de dados, a elaboração de laudo, com todos os seus tópicos recomendáveis, bem como a anexação de mídia, se entender necessário.

(iv) Perícia Criminal em Local de Internet

O exame de local de internet consiste na utilização de técnicas e ferramentas para coletar vestígios deixados pela prática de infração penal com utilização da internet, dividindo-se em a) exame de IPs e nomes de domínio; b) exames de mensagens de correio eletrônico e c) exames de páginas de internet.

Em relação ao exame de IPs e nomes de domínio, geralmente é possível a verificação de dados cadastrais de registros em sites especializados, rastreamento de rotas de tráfego e informações sobre localização geográfica. No exame de mensagem de correio eletrônico, o objetivo é determinar a real origem de uma mensagem eletrônica, sendo necessário para tanto o cabeçalho completo da mensagem. Finalmente, o exame de páginas da internet visa à preservação do conteúdo de um sítio na Internet, devendo ser salvo o seu conteúdo em formato digital original, preferencialmente.

Finalmente, tem-se a elaboração de laudo, com todos os seus tópicos recomendáveis, bem como a anexação de mídia, se entender necessário.

Nesse mesmo sentido, tem-se ainda a norma ABNT NBR ISO/IEC 27037:2013com o propósito de padronizar o tratamento de evidências digitais – compreendendo as fases de identificação, coleta, aquisição e preservação – a fim de preservar sua integridade e autenticidade, de modo a assegurar sua admissibilidade, força probatória e relevância em processos judiciais ou disciplinares[5].

Possui como princípios fundamentais: (i) minimizar o manuseio dos dispositivos digitais originais ou das evidências digitais; (ii) considerar quaisquer alterações e documentar ações tomadas; e (iii) a limitação da atuação dos agentes dentro de suas competências.

Verifica-se ainda especial atenção à cadeia de custódia, com a documentação do procedimento desde o processo de coleta ou aquisição, possibilitando a identificação, acesso e movimento da evidência digital a qualquer tempo, com a existência de identificador único da evidência, e o registro de todas as pessoas que acessaram a evidência, com data, hora e local, bem como registro de quaisquer alterações.

Dessa forma, recomenda-se que os responsáveis pela análise das evidências digitais sigam e documentem seus procedimentos segundo as normas contidas no Procedimento Operacional Padrão em Perícia Criminal e ABNT NBR ISO/IEC 27037:2013, de modo a viabilizar a análise precisa da cadeia de custódia, bem como a validade dos exames periciais realizados.

## VI – A atividade jurisdicional em face das provas digitais

Embora as orientações tratadas neste documento sejam dirigidas a todos os atores do sistema de justiça criminal, não há dúvidas de que a observância dos protocolos expostos pretende garantir segurança e imparcialidade à atividade jurisdicional nos casos que envolvem as provas digitais.

Nesse sentido, o magistrado deve proceder com especial atenção quanto à determinação de colheita e preservação das evidências (o que será efetivado por meio da busca e apreensão), bem como em relação à análise das provas digitais (realização de perícia), sob pena de eventual prejuízo à sua utilização processual.

Para tanto, recomendável que nas decisões judiciais que influirão na preservação, colheita e análise da prova em sede investigatória, sejam fixados os parâmetros ou orientações específicas para as evidências digitais, inclusive com a citação das normas técnicas a serem observadas, caso se entenda necessário, tendo em vista a volatilidade desse tipo de vestígio.

Quanto ao contraditório diferido, caso já realizada prova pericial em sede de Inquérito Policial, desnecessária, em regra, a repetição da perícia na fase judicial, notadamente levando-se em consideração a possibilidade de acesso integral aos suportes probatórios, bem como repetição dos procedimentos periciais, o que deve estar devidamente documentado. De toda forma, nada impede que a defesa formule quesitos *a posteriori*, que devem ser respondidos pelos peritos, ou ainda solicite a repetição do exame, desde que haja indícios de violação da preservação das evidências.

Quanto à produção de prova testemunhal, interessante que o magistrado formule perguntas de modo a verificar o *íter* da cadeia de custódia, especialmente quando ouvidos como testemunhas os agentes responsáveis pela efetivação da busca e apreensão, de modo a aferir que foram observados os protocolos que visam à integridade e preservação das provas digitais, ainda que não tenham sido documentados.

Finalmente, também é necessário destacar que eventual inobservância de alguma das etapas recomendáveis na cadeia de custódia das provas digitais não conduzirá inexoravelmente à sua nulidade, tendo em vista a possibilidade de aproveitamento parcial da prova, ou ainda de sua repetição, caso não haja indícios de sua contaminação, o que deve ser analisado caso a caso pelo magistrado, à luz do princípio da instrumentalidade das formas.

## VII – Conclusões:

A busca da verdade a partir dos elementos de prova do processo penal sempre foi uma tarefa que exigiu enorme empenho das partes e do magistrado em face da dificuldade de se reconstituir fatos cuja memória sofre o inevitável desgaste provocado pelo decurso do tempo.

Entretanto, a atual realidade tecnológica evidencia um paradoxo em relação à atividade probatória: se de um lado o mundo digital se desenvolve com extrema celeridade, tornando obsoletos certos instrumentos e criando outros capazes de dificultar as investigações criminais, de outro lado, os sistemas eletrônicos auxiliam sobremaneira a persecução penal, na medida em que permitem o registro de operações e a origem da conduta criminosa, facilitando a tarefa de percorrer o caminho trilhado durante a infração penal para identificar seu autor e as circunstâncias do delito.

Ao magistrado cabe, portanto, zelar para que a atividade probatória seja realizada pelas partes de modo responsável e eficiente. Nesse ponto repousa a importância de se atentar para os protocolos e as orientações expostos nesta Nota Técnica, a fim de garantir a segurança e a integridade da prova e, em última análise, alcançar a aplicação da lei penal com justiça.

[1] Quanto à confidencialidade, os dispositivos digitais podem conter, para além dos dados relevantes para a investigação, outras informações pessoais protegidas pela confidencialidade, sendo necessária a triagem dos elementos relevantes pelos agentes públicos, não obstante a necessária preservação de sua integridade.

[2] Trata-se de um algoritmo aplicado a um arquivo que gera um resultado normalmente expresso em números ou letras, permitindo verificar a sua integridade, uma vez que qualquer alteração no arquivo implica em alteração do código *hash* original.

[3] No âmbito internacional, destacam-se: a) Information technology – Security techniques. Guidelines for identification, collection, acquisiton, and preservation of digital evidence. Switzerland, 2012; b) U.S. DEPARTMENT OF JUSTICE. Eletronic Crime Scene Investigation: a guide for first responders. 2 ª Ed. Washington, 2008.

[4] Disponível em https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/pop/procedimento_operacional_padrao-pericia_criminal.pdf

[5] Disponível em https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/

Documento assinado eletronicamente por **Flávia Serizawa e Silva**, **Juíza Federal Relatora**, em 11/06/2024, às 12:15, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Letícia Mendes Gonçalves**, **Juíza Federal Revisora**, em 11/06/2024, às 13:18, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Milenna Marjorie Fonseca da Cunha**, **Juíza Federal Revisora**, em 11/06/2024, às 14:25, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Raecler Baldresca**, **Juíza Federal Relatora**, em 11/06/2024, às 17:48, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.trf3.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **10949192** e o código CRC **40257BF6**.