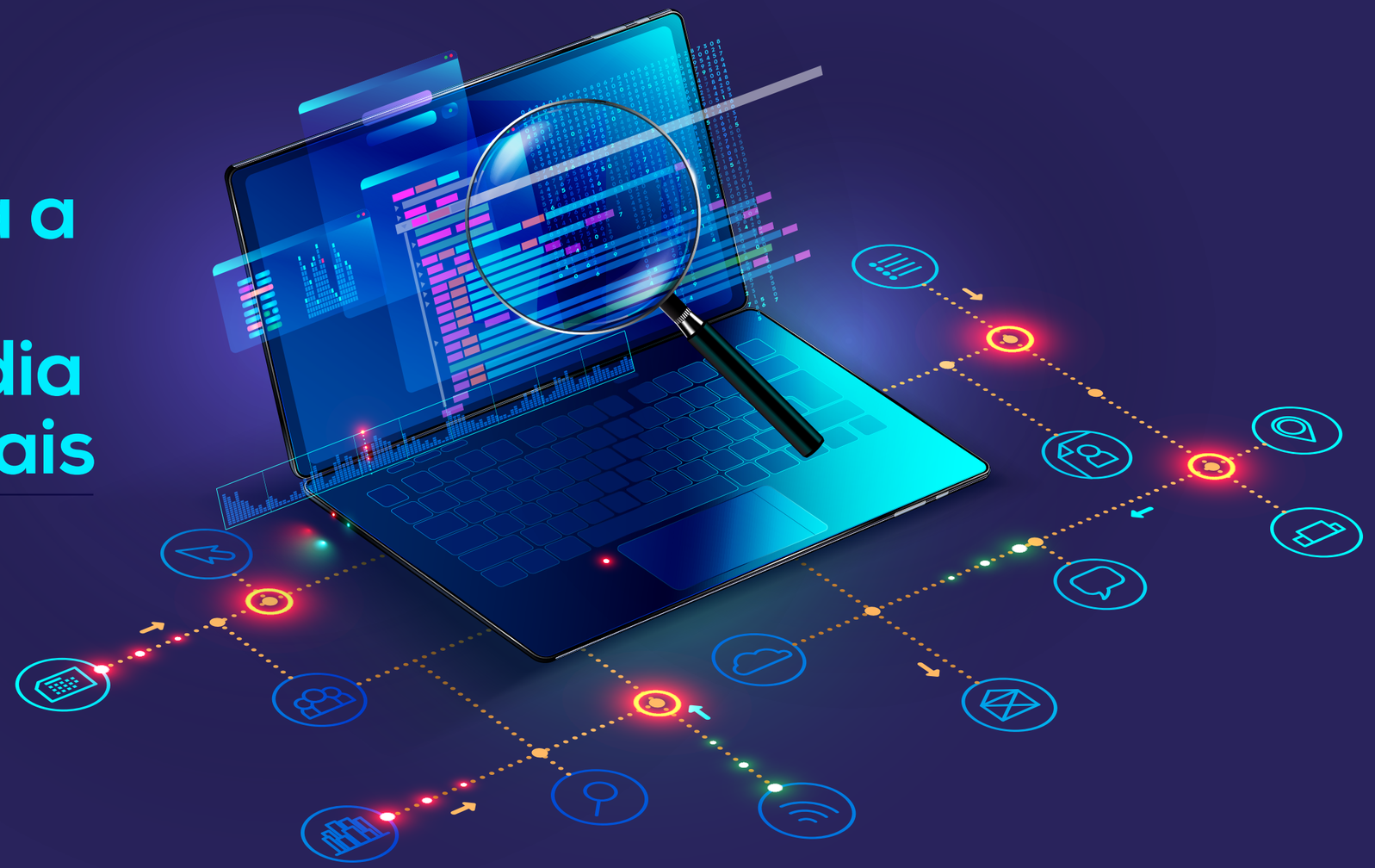
Secretaria de Perícia, Pesquisa e Análise

Orientações para a Preservação da Cadeia de Custódia de Vestígios Digitais

com base na Lei Anticrime nº 13.964/2019



MPF
Ministério Público Federal

Ministério Público Federal
Secretaria de Perícia, Pesquisa e Análise

Orientações para a Preservação da Cadeia de Custódia de Vestígios Digitais

com base na Lei Anticrime nº 13.964/2019

Brasília
MPF
2020

Dados Internacionais de Catalogação na Publicação (CIP)

B823o

Brasil. Ministério Público Federal. Secretaria de Perícia, Pesquisa e Análise. Orientações para a preservação da cadeia de custódia de vestígios digitais : com base na Lei Anticrime nº 13.964/2019 / Ministério Público Federal. Secretaria de Perícia, Pesquisa e Análise. – Brasília : MPF, 2020.

14 p.

Disponível em: <http://intranet.mpf.mp.br/areas-tematicas/gabinete-pgr/pericia-pesquisa-e-analise/publicacoes-e-manuais/relatorios-1>.

1. Evidência digital – preservação. 2. Cadeia de custódia – preservação. 3. Prova criminal. 4. Ministério Público Federal – manual. I. Autor. II. Título.

CDD 387.544

Elaborado por Juliana de Araújo Freitas Leão – CRB 1/2596

Coordenação e Organização

Secretário de Perícia, Pesquisa e Análise

Pablo Coutinho Barreto

Secretário de Perícia, Pesquisa e Análise Adjunto

Paulo Rubens Carvalho Marques

Normalização bibliográfica

Coordenadoria de Biblioteca e Pesquisa (Cobip)

Planejamento visual e diagramação

Bianca Prado / Secom

Revisão

Ana Paula Rodrigues de Azevedo / Secom

Fernanda Souza / Secom

Procuradoria-Geral da República

SAF Sul, Quadra 4, Conjunto C

CEP 70050-900 – Brasília, DF

Tel.: (61) 3105-5100

www.mpf.mp.br

Sumário

Apresentação

A Lei nº 13.964/2019, vigente desde 23 de janeiro de 2020, alterou a legislação penal e processual penal, disciplinando, entre outros temas, a cadeia de custódia e perícias em geral.

A cadeia de custódia é fundamental para garantir a higidez e a rastreabilidade dos vestígios, físicos ou digitais. Diante da relevância e da transversalidade do tema, a Secretaria de Perícia, Pesquisa e Análise (Sppea/PGR), por meio da Assessoria Nacional de Perícia em Tecnologia da Informação e Comunicação (Anptic), tem orientado os integrantes do Ministério Público Federal a observarem determinadas cautelas básicas para preservação da integridade dos vestígios, sobretudo os digitais.

Esses cuidados se aplicam não apenas a equipamentos eletrônicos apreendidos ou mídias disponibilizadas por colaboradores ou provedores de internet, mas também a dados disponibilizados em nuvem para *download*.

Nesse contexto, a presente publicação procurou registrar conceitos básicos e situações práticas que possam orientar membros e servidores do MPF no dia a dia de seu trabalho, permitindo a identificação de riscos à integridade das evidências. Tal iniciativa não desnatura a elaboração, pela Sppea/PGR, de outros materiais, com maior nível de detalhamento.

O que é cadeia de custódia?

"Considera-se cadeia de custódia 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."

(Art. 158-A da Lei nº 13.964/2019)

O que é vestígio?

"Vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal."

(§ 3º do art. 158-A da Lei nº 13.964/2019)

O que é vestígio digital?

"Vestígio digital, ou vestígio cibernético, é qualquer informação de valor probatório que tenha sido armazenada ou transmitida em meio digital e que pode ser utilizada para comprovação de um crime."

(VELHO, 2016)

Cadeia de custódia

O art. 158-B da Lei nº 13.964/2019 definiu as seguintes etapas na cadeia de custódia:

- Reconhecimento;
- Isolamento;
- Fixação;
- Coleta;
- Acondicionamento;
- Transporte;
- Recebimento;
- Processamento;
- Armazenamento; e
- Descarte.

Os mais importantes são detalhados a seguir:

• Isolamento

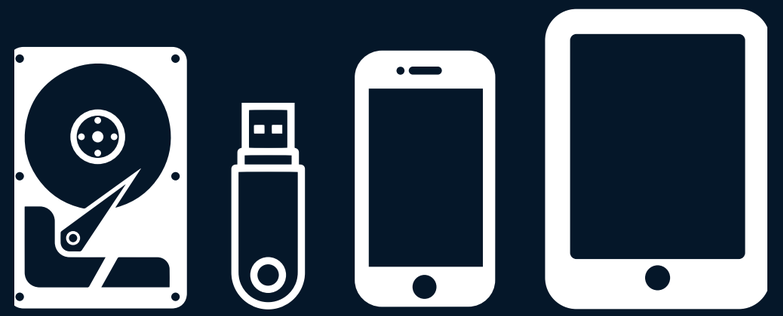
DEFINIÇÃO: ato de evitar que se altere o estado dos vestígios digitais, devendo isolar e preservar o ambiente.

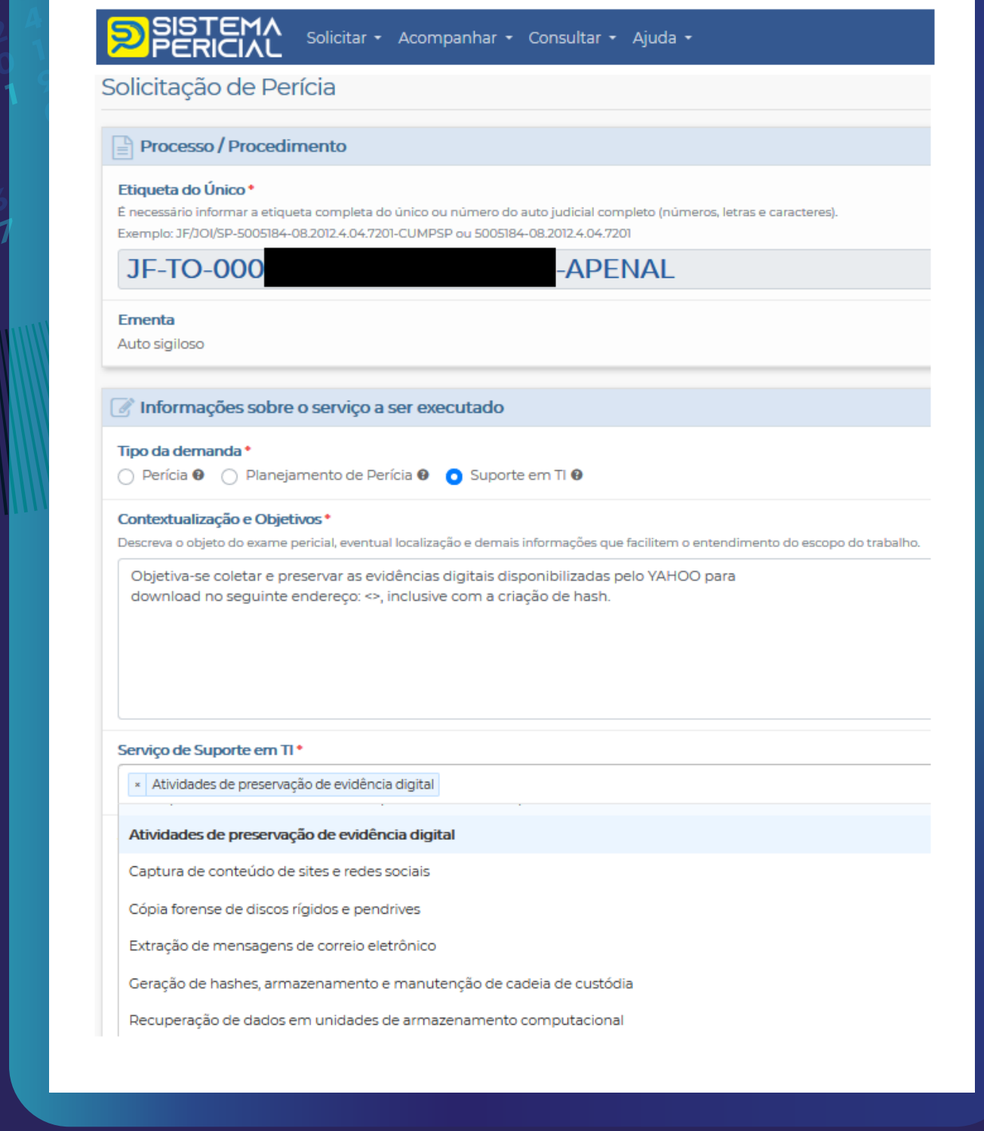
Um isolamento inadequado pode invalidar todo o objeto probatório.

• Coleta

DEFINIÇÃO: ato de recolher o vestígio que será submetido à análise pericial.

Cada dispositivo possui um procedimento específico adequado às suas características.





A coleta de vestígios digitais deverá ser ser realizada, preferencialmente, por servidor indicado pela Sppea, após solicitação do serviço de Suporte em TI via Sistema Pericial.

As coletas e cópias forenses deverão ser efetuadas seguindo os procedimentos definidos pela Sppea em documentos complementares ou, na ausência destes, deverão observar as melhores metodologias de forense digital.

Regras essenciais para o isolamento e a coleta

Jamais conecte um vestígio diretamente ao computador, exceto se o ambiente hospedeiro estiver devidamente configurado.

De modo algum ligue um dispositivo que estiver desligado, a não ser que esteja realizando um procedimento controlado.

De modo algum desligue um dispositivo que esteja ligado antes que tenha a garantia de que os dados voláteis e criptografados tenham sido capturados.

Sempre atue de forma a manusear a evidência original o mínimo necessário.

Informação complementar

Hashes são uma importante parte da manutenção de integridade, pois podem garantir que um vestígio não foi alterado.

Uma função *hash* é um algoritmo matemático que mapeia dados de comprimento variável para dados de comprimento fixo.

Um *hash* (resultado da função *hash*) poderá ser inadvertidamente alterado caso a evidência seja incorretamente manuseada.

Cabe, preferencialmente, ao perito ou perito eventual de TIC calcular o *hash* do vestígio digital sempre que possível.

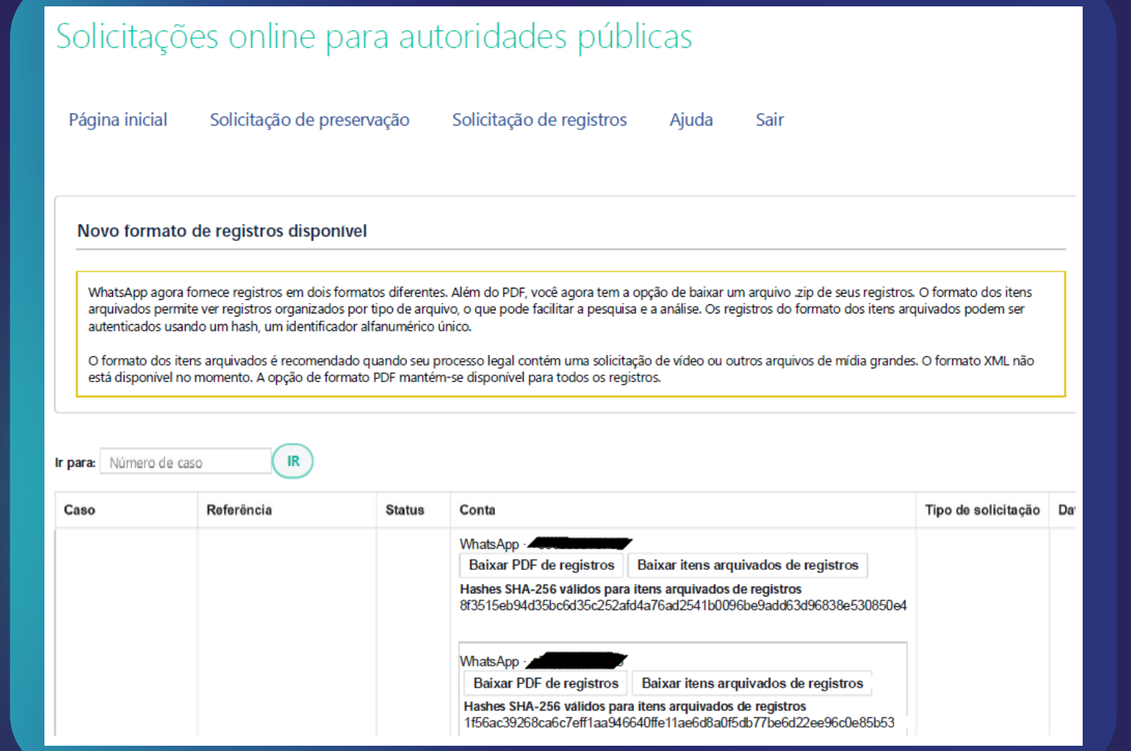
Dados disponibilizados pelo provedores

Em cumprimento a ordens judiciais, os provedores de aplicações de internet têm disponibilizado evidências[1] por meio de (I) mídias físicas, (II) links para *download* ou em (III) ambientes restritos no interior de portais criados para o atendimento a determinações estatais, chamados de *Law Enforcement Request System (Lers)*.

Conforme a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), os provedores têm a obrigação de garantir a segurança e a integridade das provas eletrônicas por eles apresentadas.

Desse modo, como solução ideal, sugere-se que os membros do MPF exijam dos provedores que disponibilizem os códigos *hashes* correspondentes à coleta dos dados.

Caso os *hashes* sejam disponibilizados por meio de PORTAL LERS (vide imagem ao lado), o membro do MPF deverá copiá-los em arquivo de texto, bem como diligenciar a impressão das respectivas telas e juntá-las aos autos. Isso porque os arquivos e as informações disponibilizados em tais portais ficam disponíveis apenas por determinado lapso de tempo.



Por fim, caso os *hashes* não sejam disponibilizados pelos provedores e não seja conveniente obrigá-los a fazê-lo, o Sistema Pericial poderá ser acionado para a realização do serviço de Suporte em TI. Nessa hipótese, poder-se-á afiançar a integridade do vestígio digital apenas desde o momento do cálculo e aplicação dos *hashes* pelo profissional de TI do MPF.

1 Caixas de e-mails dos investigados, postagens em redes sociais, dados de aplicativos de mensagens instantâneas etc.

• Acondicionamento

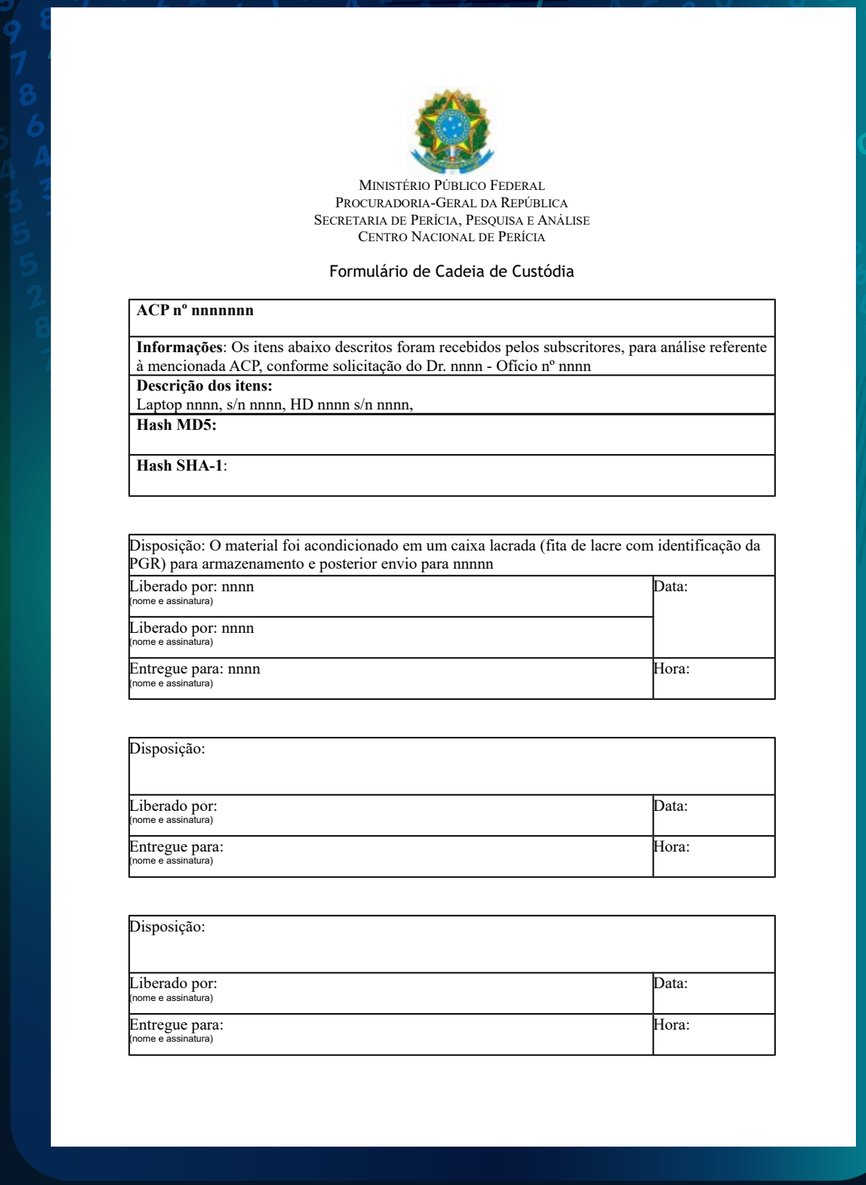
DEFINIÇÃO: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada.

Os vestígios digitais deverão ser acondicionados em sacolas do MPF seladas com lacre, com numeração individualizada, bem como data, hora, nome, matrícula e assinatura do responsável.

Após cada rompimento de lacre, deve se fazer constar do Formulário de Cadeia de Custódia o nome e a matrícula do responsável, a data e o local referentes ao novo acondicionamento.

O FORMULÁRIO DE CADEIA DE CUSTÓDIA deve sempre acompanhar o vestígio digital devidamente acondicionado.

O lacre, sempre que rompido, ou o próprio saco de evidência, deverá ser acondicionado no interior do novo recipiente.



MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA-GERAL DA REPÚBLICA
SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE
CENTRO NACIONAL DE PERÍCIA

Formulário de Cadeia de Custódia

ACP nº nnnnnnn
Informações: Os itens abaixo descritos foram recebidos pelos subscritores, para análise referente à mencionada ACP, conforme solicitação do Dr. nnnn - Ofício nº nnnn
Descrição dos itens: Laptop nnnn, s/n nnnn, HD nnnn s/n nnnn,
Hash MD5:
Hash SHA-1:

Disposição: O material foi acondicionado em um caixa lacrada (fita de lacre com identificação da PGR) para armazenamento e posterior envio para nnnnn	
Liberado por: nnnn (nome e assinatura)	Data:
Liberado por: nnnn (nome e assinatura)	
Entregue para: nnnn (nome e assinatura)	Hora:

Disposição:	
Liberado por: (nome e assinatura)	Data:
Entregue para: (nome e assinatura)	Hora:

Disposição:	
Liberado por: (nome e assinatura)	Data:
Entregue para: (nome e assinatura)	Hora:

ACESSE AQUI O FORMULÁRIO DE CADEIA DE CUSTÓDIA

Transporte

DEFINIÇÃO: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas, de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse.

Durante o transporte, os vestígios deverão estar devidamente acondicionados e não deverão ficar suscetíveis a altas temperaturas ou próximos a campos magnéticos.

Processamento

DEFINIÇÃO: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo, parecer ou relatório técnico produzido por perito.

A solicitação de execução de qualquer perícia deverá acontecer via Sistema Pericial, por meio de novo pedido (serviço pericial).

Armazenamento

DEFINIÇÃO: procedimento referente à guarda, em condições adequadas, do material a ser processado, para realização de contraperícia, ao descarte ou ao transporte, com vinculação ao número do laudo correspondente.

O local de armazenamento deve ser seguro de tal forma que acessos não autorizados sejam detectados.

Descarte

DEFINIÇÃO: procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.

Não cabe aos peritos e peritos eventuais do MPF realizar o descarte dos vestígios, o qual será posteriormente definido em Instrução de Serviço ou por membro solicitante.

Glossário

BLOQUEADOR DE HARDWARE: dispositivo forense computacional que limita o acesso à mídia digital em modo de somente leitura, não permitindo a escrita e garantindo a sua integridade.

DADOS VOLÁTEIS: dados que são perdidos quando o computador ou dispositivo é desligado.

HASH: conteúdo gerado por algoritmos criptográficos, os quais são utilizados na forense computacional para verificar se um conteúdo ou imagem é idêntico à sua origem. Uma simples alteração (pode ser um único bit) em um arquivo gera uma grande mudança no *hash* (ou resumo/sumário). Não é possível recriar um arquivo a partir do *hash*.

IMAGEM OU ESPELHAMENTO: cópia digital criada utilizando-se de um processo forense.

Referências

ASSESSORIA NACIONAL DE PERÍCIA EM TIC DO MPF. Formulário de Cadeia de Custódia. Disponível em: https://goo.gl/H27DMd.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal (e suas atualizações). Disponível em: https://tinyurl.com/ybsp72ak.

BREZINSKI, Dominique; KILLALEA, Tom. RFC 3227: Guidelines for Evidence Collection and Archiving. fev. 2002. Disponível em: https://www.ietf.org/rfc/rfc3227.txt.

VELHO, Jesus. Tratado de Computação Forense. Campinas-SP: Editora Millenium, 2016.

MPF

Ministério Público Federal