PORTARIA CONJUNTA
POLÍCIA CIVIL - SECRETÁRIA DE SEGURANÇA PÚBLICA

PORTARIA CONJUNTA Nº 006/2024-GS/SSP-AM – 20/05/2024

CONSIDERANDO a Constituição Federal de 1988, que assegura o direito à privacidade e à proteção de dados pessoais, bem como o princípio da dignidade da pessoa humana;

CONSIDERANDO o Código de Processo Penal e as legislações esparsas sobre investigações policiais;

CONSIDERANDO a norma de cadeia de custódia de vestígios prevista no Artigo 158 do Código de Processo Penal e na portaria 82/2014 da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública;

CONSIDERANDO a Lei de Proteção de Dados (Lei nº 13.709/2018), que estabelece diretrizes para o tratamento de dados pessoais, garantindo a sua segurança e privacidade;

CONSIDERANDO a necessidade de regulamentar o acesso e o uso de ferramentas computacionais forenses, tais como o "UFED 4PC" e/ou "INSEYETS UFED" - CELLEBRITE, entre outras, de forma a garantir o cumprimento das normas constitucionais e legais mencionadas,

RESOLVE:

Artigo 1º CRIAR a Central Integrada de Extração de Dados de Dispositivos Computacionais Portáteis (CIEX) em ambiente colaborativo, compartilhado e integrado de extração de dados de vestígios cibernéticos entre o Departamento de Polícia Técnico-Científica (DPTC) e o Núcleo de Inteligência de Polícia Judiciária (NIPJ/PCAM).

§ 1º A coordenação administrativa e operacional da CIEX será exercida, de forma cooperativa, pelos titulares do DPTC/SSP e NIPJ/PCAM.

§ 2º O Departamento de Polícia Técnico-Científica (DPTC) atuará na Central Integrada de Extração de Dados de Dispositivos Computacionais Portáteis, por intermédio do Setor de Informática Forense do Instituto de Criminalística assegurada a autonomia técnica, científica e funcional do perito prevista na Lei nº 12030/2009, realizando as extrações dos dispositivos e emitindo os laudos periciais sem análise de dados.

§ 3º O Núcleo de Inteligência de Polícia Judiciária (NIPJ/PCAM) atuará na Central Integrada de Extração de Dados de Dispositivos Computacionais Portáteis, por intermédio do Setor de Inteligência de Dados, tem como objetivo executar o apoio técnico em investigações policiais, nas quais eventualmente exista a necessidade de extração e análise de dados de dispositivos eletrônicos móveis apreendidos, por meio de ferramentas e estratégias atuais, complexas e especializadas no combate ao crime, em apoio as investigações, além de executar precipuamente a atividade de inteligência de polícia judiciária do Estado do Amazonas.

§ 4º Os servidores integrantes da CIEX serão indicados, exclusivamente, pelos titulares do DPTC/SSP e NIPJ/PCAM.

Artigo 2º Os dispositivos computacionais portáteis que serão objeto de extração na Central estão relacionados a seguir:

I. Telefones celulares;

II. Tabletes;

III. Drones.

§ 1º Os demais equipamentos computacionais como: dispositivos de armazenamento (discos rígidos, SSD, pendrives, cartões de memória, mídias ópticas); notebooks; computadores pessoais; storages; entre outros, deverão ser encaminhados para o Setor de Informática Forense no Instituto de Criminalística.

Artigo 3º É atribuição da Autoridade Policial que efetuou a apreensão do dispositivo eletrônico:

I. Restringir a apreensão de dispositivos àqueles itens que guardem relação com o crime investigado e carreguem indícios de sua materialidade de autoria, evitando a apreensão de equipamentos que não guardem interesse direto às investigações, gerando assim volume de trabalho desnecessário e sem objetividade.

II. Zelar pela cadeia de custódia do vestígio eletrônico apreendido, conforme preceitua o Art. 158-A do Código de Processo Penal, no intuito de preservar a prova e sua correta utilização dentro do procedimento judicial;

III. Realizar o translado do equipamento até a CIEX, visando iniciar o processo de extração e eventual análise, ficando desde logo ciente que todos aqueles que foram responsáveis pelo transporte ou que tiveram acesso ao vestígio devem ser registrados em documento pertinente, e qualquer acontecimento atípico ocorrido durante o transporte também deverá ser documentado.

Artigo 4º Considerando a proteção de sigilo relacionada a quaisquer dados contidos em dispositivos computacionais portáteis, o serviço de protocolo da CIEX somente receberá tais equipamentos nas seguintes condições:

§ 1º Acompanhados de ordem ou decisão judicial autorizadora da quebra de sigilo com extração e análise de dados, devendo constar EXPRESSAMENTE os seguintes termos:

I. Autorização para o procedimento de acesso e extração de dados de dispositivo móvel de seu conteúdo, IMEI´S e CHIP´S, podendo manusear e acessar todos os aplicativos vinculados ao terminal existente no SIM card e do aparelho, tais como agenda telefônica, registros de chamadas, áudios, vídeos e imagens, além de conteúdo de aplicativos de trocas de mensagens instantâneas, a exemplo do WhatsApp e Telegram, e outras redes sociais existentes, como Instagram, Facebook, entre outras, e todo conteúdo necessário, a ser realizado pelo Centro Integrado de Extração de Dispositivos Computacionais Portáteis;

II. Autorização para que o agente responsável pela extração de dados, parte integrante do CIEX, possa romper o lacre do recipiente que contém o (s) dispositivo (s), atendendose ao artigo 158-D, do CPP;

III. Autorização para compartilhamento dos dados extraídos com a perícia do Instituto de Identificação Criminal – IC, com o Núcleo de Inteligência de Polícia Judiciária – NIPJ e com a respectiva Unidade Policial demandante, responsável pelas investigações. Observação: No caso dos requisitos citados acima não constarem de forma expressa na Ordem Judicial autorizadora, o Requerimento Informacional será indeferido por este CIEX, podendo a Autoridade Policial requerer ao juiz, a retificação da mesma, para inclusão expressa dos requisitos supra. Nesse caso, o requerimento será reapreciado para fins de deferimento.

§ 2º Acompanhados de termo de autorização do proprietário do aparelho ou de parentes próximos em casos de aparelhos pertencentes à vítimas de homicídios, além do auto de exibição e apreensão assinado pela Autoridade Policial. Os responsáveis deverão assinar termo de autorização, cujo modelo será disponibilizado pela CIEX.

§ 3º Casos excepcionais serão analisados e avaliados pelos titulares do DPTC/SSP e NIPJ/PCAM.

Artigo 5º A Autoridade Policial, após a devida autorização judicial, deverá fazer o Requerimento por meio de memorando via SIGED à CIEX, com solicitação de acesso a extração e análise de dados nos aparelhos celulares, tabletes ou drones, juntamente com a cópia da decisão judicial que concedeu a autorização de extração e eventual do aparelho em questão, além do auto de exibição e apreensão correspondente, para fins de correta individualização do aparelho.

Artigo 6º As extrações de dados serão realizadas conforme a fila de prioridade, de acordo com o previsto em lei (Lei nº 8.069/1990, Lei nº 10.741/2003, Lei 11.340/2006, Art. 429 do Decreto Lei nº 3.689/1941 e Lei n° 8.072/1990) e em ordem cronológica do encaminhamento do material (os mais antigos são atendidos primeiros). A fila de prioridade seguirá os seguintes critérios de classificação:

I. Cobranças judiciais;

II. Casos envolvendo crianças, adolescentes e idosos;

III. Casos em que a legislação prevê prioridade, como naqueles que envolvem réus presos,Tribunal do Júri, casos enquadrados na lei Maria da Penha, crimes hediondos, entre outros.

Artigo 7º Somente será realizada a fase de **análise pericial dos vestígios** por peritos criminais quando a requisição apresentar quesitos específicos que demandem conhecimentos especializados de computação forense para interpretação do vestígio cibernético.

§ 1º São exemplos de exames que requerem conhecimento especializado em computação forense a análise de arquivos de log, análise de metadados de arquivos, análise de conteúdo de bancos de dados, análise de conteúdos apagados, análise de arquivos de sistema, análise de arquivos criptografados, análise de malware, análise de aplicativos antiforenses, análise de protocolos de comunicação e análise de invasão de sistemas informáticos.

§ 2º A requisição pericial dos vestígios com quesitos que demandem conhecimento especializado em computação forense deverá conter, necessariamente, a tipificação dos delitos e os detalhes do objeto a ser analisado, por exemplo: a identidade do proprietário do equipamento examinado (caso ela seja conhecida), alvos, suspeitos, vítimas, alcunhas, palavras chaves, datas ou faixa de datas específicas e locais.

§ 3º Será realizada a fase de análise pericial dos vestígios nos equipamentos computacionais portáteis relacionados a crimes hediondos, invasão de dispositivo informático e crimes prioritários segundo Parágrafo Único do Art. 158 do Código de Processo Penal.

§ 4º Quando os quesitos tratarem exclusivamente de extração de dados, as requisições de perícia serão atendidas por meio de **exame pericial sem fase de análise de dados**, realizados exclusivamente por peritos criminais oficiais.

Artigo 8º Os agentes responsáveis pela apreensão dos dispositivos computacionais portáteis deverão adotar os seguintes procedimentos com vistas a garantia da integridade da prova pericial:

I. Caso o dispositivo esteja desligado, como regra geral, ele deve ser mantido desligado;

a. Caso o proprietário forneça a senha do dispositivo, ele deve ser ligado, a senha deve ser testada e documentada. Na sequência, os passos sobre dispositivo eletrônico móvel ligado e desbloqueado devem ser seguidos;

II. Caso o dispositivo eletrônico móvel esteja ligado e desbloqueado:

a. Colocar o aparelho em modo avião, assim como desativar os serviços de Bluetooth, geoposicionamento e wi-fi;

b. Verificar a presença de senhas específicas de aplicativos de interesse à investigação (WhatsApp, Telegram, Wickr, etc.) e também descrevê-las nos documentos de apreensão dos materiais;

c. Desabilitar a configuração de descanso ou travamento automático de tela;

d. Desabilitar todos os seus alarmes, pois em alguns modelos o dispositivo é ligado automaticamente no horário programado;

e. Caso seja possível, verificar se existem outros métodos de desbloqueio através de agentes de confiabilidade (extend unlock / smart lock), por exemplo, quando conectado a uma rede sem fio pré-estabelecida (Wi-Fi ou Bluetooth), desbloqueio por proximidade ou quando o celular estiver em um determinado local. Se estes métodos de bloqueio estiverem ativos, devem ser desativados;

f. Dispositivos da fabricante Apple como iPhones e iPads devem ter desativada a localização off-line.

III. Caso o dispositivo esteja ligado e bloqueado:

a. Acondicionar o aparelho em uma bolsa Faraday, com sua entrega para extração de dados com a maior brevidade possível, conectado a bateria portátil. Podem ser utilizados materiais alternativos para isolamento de sinal. A bateria portátil deve ser acondicionada juntamente com o aparelho, nunca fora da embalagem.

IV. Os tópicos seguintes referem-se a orientações gerais durante o processo de coleta do equipamento:
a. Caso o proprietário esteja utilizando o aparelho, deve-se tentar realizar a apreensão do dispositivo antes que seja possível efetuar o bloqueio;

b. Não sendo possível essa apreensão imediata e o proprietário não forneça a senha, deve se verificar se outras pessoas na residência têm conhecimento da senha do aparelho em questão ou de outros aparelhos e dispositivos móveis;

c. Obtendo-se a senha do aparelho e desabilitando-a, deverá se proceder conforme os passos detalhados no item II;

d. Sempre que possível, os dispositivos eletrônicos móveis apreendidos devem ser fotografados e/ou filmados, identificados, embalados corretamente e entregues à Central de Extração com a maior brevidade possível;

e. Os dados armazenados nesses dispositivos, como regra geral, não devem ser acessados ou sofrer quaisquer alterações, sendo proibido o manuseio aleatório do aparelho após sua apreensão, visando prevenir a maculação de eventuais indícios/provas nele contidos. Caso seja imprescindível a manipulação do aparelho, a justificativa deve ser registrada, incluindo quem realizou (nome e matrícula), data, hora e local;

Observação: A SSP e PCAM envidarão esforços visando a aquisição de ferramentas para coleta dos vestígios, como por exemplo: bolsas de Faraday, malotes, sacos de evidência, lacres, entre outros, que serão disponibilizados oportunamente às unidades da Polícia Civil responsáveis pelas apreensões dos equipamentos.

Artigo 9º Descrever cada dispositivo apreendido de forma a identificá-lo unicamente. Recomenda-se, para cada dispositivo apreendido, registrar os seguintes dados:

I.Tipo do dispositivo (aparelho celular, tablete, drone);

II.Marca e modelo;

III.Item individualizador (IMEI e número de série do aparelho, ICCID do cartão SIM);

IV.Estado em que foi encontrado (ligado, desligado, avarias , etc.);

V.Dados de segurança (senha de acesso, PIN, etc.);

VI.Informações adicionais (como, por exemplo, a quem pertence).

Observação: Quando não for possível informar o item individualizador do aparelho, as características particularizadas e visíveis do equipamento devem ser descritas, evitando a manipulação do aparelho para a obtenção do IMEI.

Artigo 10º O responsável pelo Recebimento dos dispositivos na CIEX, deverá realizar os registros de entrada do material, procedendo à documentação exigida em lei, e realizar conferências:

I. Cada equipamento recebido pela CIEX terá associado um Documento de Recebimento de Equipamento (DRE), onde serão registrados todos os dados do procedimento desta etapa;

II. Durante a abertura da embalagem para conferência, sugere-se que o procedimento seja filmado e/ou fotografado;

III. Deverá ser conferido se os materiais entregues para extração estão acompanhados de autorização judicial da extração e auto de apreensão dos aparelhos, além dos demais documentos que solicitam a extração (requisição de perícia, memorando, ofício, etc.);

IV. Deverá ser conferida se a descrição contida nos documentos encaminhados pelo requerente corresponde ao efetivamente recebido, sobretudo quanto ao elemento identificador (número de série, IMEI, ICCID, etc) associado aos dispositivos;

V. Antes do deslacre, o recebedor deve conferir a numeração dos lacres, o estado dos lacres e embalagens do vestígio e reportar qualquer problema encontrado;

VI. Deslacrar, realizar nova conferência no material com sua descrição na documentação associada, identificar e individualizar todos os itens;

VII. Preferencialmente remover o cartão SIM, caso esteja presente no equipamento;

VIII. Realizar a remoção de mídia de armazenamento computacional (memória MicroSD ou similares) do dispositivo apenas para fins de identificação e individualização reinserindo novamente para a realização dos exames;

IX. Caso observe qualquer problema que inviabilize o recebimento do equipamento, fotografar e emitir Documento de não Conformidade (DNC), devolvendo o vestígio ao requisitante.

Deve ser priorizado o recebimento de vestígios que demandam procedimento de extração urgente, como no caso de aparelhos ativos, mas sem a senha de desbloqueio, ou bloqueados e recebidos ligados (em powerbank), que deverão ser imediatamente encaminhados à perícia para providências.

Artigo 11º Após o recebimento dos dispositivos computacionais móveis, eles são encaminhados para a Extração de dados.

I. Todas as etapas das extrações serão registradas em um Documento de Acompanhamento de Extração (DAE);

II. Se o dispositivo estiver com defeitos que impeçam a extração dos dados ou quando não for possível realizar a extração de dados através de equipamento forense, deve-se comunicar a autoridade requisitante através do Documento de Devolução do Equipamento Sem Extração (DDE);

III. Sempre que possível, os dispositivos devem ser colocados em modo avião. Verificar se todas as conexões foram efetivamente desabilitadas (Wi-Fi, Bluetooth, rede de telefonia móvel, etc.);

IV. Priorizar sempre a extração mais completa possível (física para dispositivos sem criptografia ou com criptografia de disco, ou sistema de arquivos completa para dispositivos com criptografia baseada em arquivos);

V. Após o fim da extração, ela deve ser distribuída para um perito criminal oficial, que realizará a emissão do Laudo Pericial sem análise de dados.

Artigo 12º A etapa de Elaboração do Laudo Pericial sem análise de dados envolve a descrição pormenorizada dos vestígios periciados, de forma que possa ser individualizado, além do detalhamento das extrações efetuadas e a apresentação clara e sucinta dos procedimentos e métodos utilizados, esclarecendo os temas relevantes para a compreensão das extrações, além da relação de todos os dados extraídos do dispositivo computacional móvel.

§ 1º O resultado do exame pericial em equipamentos computacionais portáteis sem fase de análise de seus dados deverá ser acompanhado de ferramenta de indexação e busca nos relatórios dos anexos eletrônicos.

§ 2º No laudo pericial sem análise de dados deverão constar os seguintes itens:

1. Número do caso de extração, juntamente com documentos relacionados (por exemplo: requisição de perícia, mandado judicial, memorandos, ofícios, auto de apreensão de objetos, etc.);
2. Número do lacre rompido, para realização do exame, bem como o número do novo lacre, após sua realização;

3. Objeto do Exame, contendo a descrição completa do dispositivo computacional portátil;

4. Técnicas de extração realizadas no dispositivo computacional portátil;

5. Informações referentes a cadeia de custódia, incluindo a identificação dos agentes que coletaram, transportaram e entregaram o dispositivo computacional portátil, além dos responsáveis pelas extrações de dados e documentação dos resultados destas extrações;

6. Relação dos dados extraídos do dispositivo computacional forense;

7. Indicação dos anexos do laudo pericial sem análise de dados.

§ 3º O laudo do exame pericial em equipamentos computacionais portáteis sem fase de análise deverá explicitar que se trata de extração e processamento de vestígios computacionais portáteis de forma automatizada, não passando pela fase de análise pericial dos vestígios.

§ 4° Os arquivos resultantes da extração de dados dos dispositivos computacionais portáteis devem ser disponibilizados em serviço de armazenamento de nuvem para as delegacias requisitantes e para o Instituto de Criminalística, respeitada a cadeia de custódia. Caso o armazenamento de nuvem não esteja disponível, os requisitantes devem providenciar mídia para armazenamento dos dados.

§ 5° A integridade dos dados contidos no anexo eletrônico deve ser garantida por meio de utilização de uma função de hash.

Artigo 13º As informações sobre cada Armazenamento de um vestígio (onde, quando e por quem foi armazenado ou retirado) deverão ser registrados no Documento de Acompanhamento de Extração.

I. Caso a instituição disponibilize sistema de armazenamento de grande volume de dados (storage), a Central manterá a cópia das extrações realizadas. Caso contrário, será necessário excluir a extração para possibilitar a execução das demais extrações da fila de espera.

Artigo 14º Após a extração do dispositivo computacional portátil, a mesma estará disponível para acesso da Unidade policial demandante para análise dos dados extraídos. Na necessidade de dar prosseguimento às investigações, a Autoridade Policial poderá requerer ao NIPJ/PCAM, setor integrante da CIEX, a confecção de relatório técnico acerca do caso ou solicitar ao Instituto de Criminalística a confecção do Laudo Pericial com Análise de Dados, conforme descrito no Artigo 6° da presente portaria.

Artigo 15º O Descarte de vestígios digitais que incluam suporte (aparelhos celulares, tabletes e drones) poderá ser realizada por devolução ao interessado ou encaminhamento para o Setor de Informática Forense para análise das extrações de dados e emissão do Laudo Pericial com análise.

§ 1º Em caso de entrega de HD externo para armazenamento de extrações, sugere-se o prazo de 30 (trinta) dias para a Região Metropolitana e 90 (noventa) dias para os demais municípios para a retirada do dispositivo, restando ciente que o acúmulo indiscriminado de tais equipamentos na CIEX causará prejuízo às atividades desenvolvidas.

Artigo 16º O uso das ferramentas forenses, como o “UFED 4PC” e/ou “INSEYETS UFED” - CELLEBRITE deve estar diretamente relacionado às atividades laborais dos usuários autorizados, ficando proibido o acesso e o uso indevido das imagens captadas para outros fins.

Artigo 17º Qualquer uso indevido, negligência ou violação das diretrizes estabelecidas nesta portaria poderá acarretar em medidas disciplinares.

Artigo 18º Os usuários autorizados devem utilizar o sistema de forma ética, responsável e dentro dos padrões legais vigentes. É vedado o acesso e utilização do sistema para fins ilícitos, prejudiciais à imagem da Polícia Civil do Amazonas, ou que violem direitos de terceiros.

Artigo 19º Fica proibida a extração de dados de dispositivos móveis que não possuam autorização judicial ou que não estejam incluídos nas hipóteses previstas no Artigo 4º, § 2º, desta portaria.

Artigo 20º Esta portaria entra em vigor na data de sua publicação, revogando-se as disposições em contrário

DELEGADO-GERAL ADJUNTO, AOS DEPARTAMENTOS, ÀS ASSESSORIAS E AOS SERVIDORES, PARA QUE TOMEM CONHECIMENTO E ADOTEM AS MEDIDAS LEGAIS DECORRENTES DESTE ATO.

DELEGACIA GERAL DE POLICIA CIVIL DO ESTADO DO AMAZONAS, EM MANAUS, 22 DE MAIO DE 2024.

[ASSINADO DIGITALMENTE]

BRUNO DE PAULA FRAGA
DELEGADO–GERAL DA POLICIA CIVIL
MAT. Nº 210.936.0 A

G.A/GDG/PC – GB

HINO DA POLÍCIA CIVIL DO ESTADO DO AMAZONAS
AUTOR: FRANCISCO JOSÉ ITAMAR DANTAS DA COSTA

A Polícia Civil do Amazonas
Devoção ao Estado darás
No requinte do culto da glória
Triunfante vitória viverás

Soberana em prol da Justiça
És conquista, és facho de luz
Nos caminhos de paz desta vida
Nossa história tão linda traduz

Ser real nesta luta inglória
Pela força de um amor varonil
Ser leal é fazer nossa história
Toda glória à Polícia Civil

Soberanos da lei com ousadia
E no peito este orgulho que traz
Respeitamos a nossa hierarquia
Como homens de bem e de paz

Saberemos transpor com clareza
Com firmeza a injustiça viril
Deleitando na honra de ser
Toda a glória à Polícia Civil