Boas Práticas no Tratamento de Evidências Digitais

1. Finalidade

Estabelecer diretrizes operacionais e controles mínimos para a identificação, preservação, coleta, aquisição, transporte, processamento, armazenamento e destinação de evidências digitais, assegurando integridade, autenticidade, confiabilidade, rastreabilidade e admissibilidade da prova.

As atividades descritas neste documento possuem caráter orientativo e de boas práticas, não se caracterizando como atividade pericial nem substituindo a atuação do órgão de perícia oficial de natureza criminal, nos termos do art. 158-C do Código de Processo Penal e da Nota Técnica CNMP nº 01/2026.

2. Campo de Aplicação

Aplica-se às Organizações Militares situadas na área de atuação da Procuradoria de Justiça Militar em Bagé/RS, quando envolvidas em atividades relacionadas ao tratamento de vestígios e evidências digitais, limitando-se às atividades de preservação, controle, documentação e apoio técnico à investigação.

3. Papéis e Responsabilidades

3.1 Primeiro Interventor da Evidência Digital (DEFR - Digital Evidence First Responder)

Agente público responsável pelo primeiro contato com o vestígio digital no local da diligência, incumbido de reconhecer a potencial evidência, preservar o estado original e iniciar a documentação da cadeia de custódia, limitando-se às ações compatíveis com sua competência técnica.

3.2 Especialista em Evidência Digital (DES)

Profissional com conhecimento técnico aprofundado, responsável por decisões técnicas complexas, aquisição forense (cópias), validações de integridade e orientação técnica, devendo justificar e documentar métodos, ferramentas e parâmetros empregados.

As atividades desempenhadas pelo DES no âmbito do Ministério Público Militar caracterizam apoio técnico à investigação, não se confundindo com atividade pericial.

3.3 Princípio da Competência Técnica

Nenhum agente deverá executar ação técnica que exceda sua capacitação. Em caso de dúvida, deve-se priorizar a preservação do vestígio, reduzir intervenções e acionar suporte especializado.

4. Princípios Fundamentais

Relevância: coletar e preservar aquilo que seja pertinente à investigação ou que, justificadamente, possa conter dados de interesse.

Confiabilidade: empregar métodos robustos, verificáveis e suficientemente documentados.

Auditabilidade: registrar todas as ações de forma a permitir revisão posterior por terceiros autorizados.

Repetibilidade: os mesmos métodos e condições devem conduzir aos mesmos resultados.

Reprodutibilidade: resultados equivalentes devem ser alcançáveis por outros profissionais e, quando possível, por ferramentas diferentes.

Justificabilidade: toda decisão técnica deve ter fundamento e registro formal, especialmente quando houver intervenção inevitável.

5. Cadeia de Custódia (conceito operacional)

A cadeia de custódia é o conjunto de procedimentos utilizados para manter e documentar, de forma contínua e cronológica, a história do vestígio, permitindo rastrear

sua posse, manuseio, transferências, processamento, armazenamento e destinação final, desde o reconhecimento até o descarte. Inicia-se no primeiro contato do agente público com o vestígio e deve permanecer ininterrupta.

6. Processo Estruturado (etapas operacionais)

6.1 Reconhecimento

Distinguir e registrar um elemento como potencial vestígio digital (dispositivo, mídia, sistema, dado, conta, credencial, registro de log ou serviço). **Nenhuma intervenção técnica deve ocorrer antes do reconhecimento formal e da fixação mínima do cenário**.

6.2 Isolamento

Evitar alteração do estado das coisas: controlar o ambiente imediato e mediato; afastar pessoas dos dispositivos; restringir acesso à energia e às redes quando tecnicamente indicado; impedir manipulação por terceiros.

6.3 Fixação

A cadeia de custódia de evidências digitais é a etapa documental e técnica preliminar, na qual se registra minuciosamente o estado original do vestígio digital (como um celular, computador ou arquivo em nuvem) antes que qualquer manipulação ou coleta forense seja realizada.

Descrever detalhadamente o vestígio conforme encontrado (posição, estado, conexões, telas ativas, acessórios, etiquetas, número de patrimônio, número de série, sinais de dano). Deve ser ilustrada por fotografias, vídeos ou croqui, sempre que possível.

6.4 Coleta

Recolher o vestígio para análise, respeitando suas características técnicas. A coleta deve priorizar a preservação, podendo ocorrer sem aquisição imediata quando o risco de alteração superar o benefício de intervenção no local.

A coleta observará o disposto nos arts. 158-A a 158-D do Código de Processo Penal.

6.5 Acondicionamento

Embalar cada vestígio de forma individualizada em recipientes adequados (antiestáticos, resistentes, com proteção contra impacto), com lacres numerados e identificação completa. O lacre não deve obstruir ventilação, portas ou partes mecânicas sensíveis.

6.6 Transporte

Transferir o vestígio sob condições adequadas (proteção física, eletrostática e, para móveis ligados, bloqueio de radiofrequência), garantindo controle formal de posse e registro de horários e responsáveis.

6.7 Recebimento

Ato formal de transferência de custódia, documentado com identificação do procedimento, origem, destino, responsáveis, natureza do vestígio e finalidade do exame. Nenhum recebimento deve ocorrer sem conferência do lacre e do rótulo.

6.8 Processamento

Processamento técnico conforme metodologia adequada. Deve-se preferir o trabalho sobre cópias forenses verificadas. Toda manipulação deve ser registrada, incluindo ferramentas, versões, parâmetros e resultados.

O processamento destina-se à organização técnica dos dados, sem emissão de juízo técnico ou pericial conclusivo.

6.9 Armazenamento

Guarda em local controlado, com registro de entradas/saídas, controle de acesso e condições ambientais compatíveis. Prever possibilidade de contraperícia e verificações periódicas de integridade.

6.10 Destinação Final

Encerramento formal com registro de restituição, arquivamento, transferência definitiva, destruição ou descarte, conforme determinação competente. Deve constar a documentação que ampare a destinação.

A destinação final marca o encerramento formal da cadeia de custódia e deverá ser formalizada por meio de certidão específica.

7. Procedimentos no Local (regras de ouro)

Não interagir prematuramente com dispositivos: mudanças de estado podem alterar dados e acionar mecanismos de destruição.

Dispositivo DESLIGADO: manter desligado; é vedado ligá-lo no local para **"ver o conteúdo"**.

Dispositivo LIGADO: não desligar automaticamente; avaliar risco de criptografia, dados voláteis e impacto operacional.

Registrar imediatamente: fotos/vídeo da cena, telas, conexões, cabos e acessórios; anotar data/hora observada no sistema.

Controlar o ambiente: afastar pessoas; identificar quem teve acesso; evitar uso de dispositivos pessoais na operação.

8. Tratamento por Tipo de Dispositivo

8.1 Computadores/Notebooks/Servidores — LIGADOS

Fotografar tela(s) e registrar aplicações abertas, sessões, conexões e hora do sistema.

Avaliar aquisição imediata de dados voláteis quando houver risco de perda **(RAM, processos, conexões, chaves)**.

Não desligar se houver suspeita de criptografia, sessão autenticada crítica ou servidor de missão crítica.

Se a decisão for desligar e for tecnicamente seguro, documentar o método e justificar; considerar risco de cache de escrita.

8.2 Computadores/Notebooks/Servidores — DESLIGADOS

Manter desligado e acondicionar para análise em ambiente controlado.

Desconectar cabos preferencialmente pela extremidade do dispositivo; etiquetar portas e conexões para reconstituição.

Recolher mídias removíveis associadas (pendrives, cartões, HDs externos) e anotar correlações (porta, etiqueta, posição).

8.3 Dispositivos Móveis (Celulares/Tablets)

Isolar imediatamente da rede para mitigar risco de limpeza remota (wipe): preferir embalagem com bloqueio de sinal; alternativas devem ser avaliadas quanto ao risco de alteração.

Manter carga elétrica para evitar desligamento e perda de dados voláteis de sessão.

Registrar estado: ligado/desligado, tela, notificações visíveis, nível de bateria, presença de SIM/SD.

Evitar desbloqueio e navegação no conteúdo; qualquer interação inevitável deve ser registrada e justificada.

8.4 Equipamentos de Rede, CFTV e Armazenamento em Rede

Identificar topologia básica: roteadores, switches, pontos de acesso, DVR/NVR, NAS/SAN, cabos e portas.

Registrar indicadores visíveis (LEDs, conexões, etiquetas) e a posição de cada cabo.

Avaliar risco de interrupção do serviço e, quando aplicável, priorizar aquisição parcial/lógica no local por especialista.

Registrar indícios de armazenamento remoto/nuvem e providenciar preservação adequada conforme autorização e escopo.

9. Aquisição Forense (cópias) e Verificação de Integridade

A extração técnica de dados deve produzir cópia verificável, preferencialmente integral (bit a bit) quando aplicável, preservando a mídia original e permitindo validação matemática da integridade.

Registrar ferramenta, versão, parâmetros, identificadores do dispositivo/mídia e ambiente de aquisição.

A extração técnica de dados não se caracteriza como atividade pericial, destinando-se a subsidiar a análise investigativa.

Gerar e registrar funções *hash* (algoritmo e valores) da mídia/imagem e, quando possível, comparar antes/depois.

Admitir aquisição parcial/lógica quando houver restrição técnica (missão crítica, volume, escopo do mandado), com justificativa formal.

Garantir que análises sejam realizadas sobre cópias, com o original preservado e acesso restrito.

10. Lacres, Rompimentos e Re-Lacração

Todo recipiente deve ser selado com lacre numerado e inviolável.

A abertura do recipiente deve ocorrer apenas por quem procederá ao exame ou por pessoa autorizada, de forma motivada.

Após qualquer rompimento, registrar responsável, matrícula/identificação, data, local, finalidade e novo lacre aplicado.

O lacre rompido deve ser acondicionado conforme o procedimento adotado pela unidade, mantendo rastreabilidade.

11. Documentação Obrigatória

Registro de cena (fotos/vídeo/croqui) e descrição circunstanciada.

Termo/auto de apreensão com identificação completa dos itens.

Ficha de Acompanhamento de Vestígio Digital (FAV Digital MPM) preenchida desde a coleta.

Registro de movimentações, recebimentos, acessos e verificações de integridade.

Relatório técnico de extração (quando houver), com *hashes* e metodologia.

12. Proibições Expressas (controle de risco)

Ligar dispositivo encontrado desligado ou navegar no conteúdo para “verificar” dados no local.

Desligar dispositivo ligado sem avaliação técnica prévia, quando houver risco de criptografia/dados voláteis.

Utilizar mídias ou equipamentos pessoais para copiar dados.

Romper lacres ou transferir custódia sem registro formal.

Permitir acesso ao vestígio por pessoas não autorizadas.

13. Qualidade, Treinamento e Revisão

Treinamento periódico de DEFR e DES, com simulações e lições aprendidas.

Padronização de formulários e numeração de lacres; auditorias internas amostrais.

Revisão anual deste Manual, ou sempre que houver alteração normativa/procedimental relevante.

ANEXO I — *Checklist* Operacional (campo)

A. Antes da diligência

- ✓ Mandado analisado (escopo, limites, endereços, itens).
- ✓ Equipe definida (DEFR/DES) e responsabilidades distribuídas.
- ✓ Avaliação de risco: volatilidade, criptografia, destruição remota, missão crítica.
- ✓ Materiais: embalagens antiestáticas, bloqueio RF, lacres, etiquetas, formulários, câmera.
- ✓ Plano de documentação e de transporte (rota, guarda, recebimento).

B. No local

- ✓ Isolamento do ambiente e afastamento de pessoas dos dispositivos.
- ✓ Registro inicial de cena (fotos/vídeo/croqui) e quem teve acesso.
- ✓ Identificação de dispositivos/mídias e priorização por volatilidade.
- ✓ Dispositivos desligados: manter desligados.
- ✓ Dispositivos ligados: documentar telas e avaliar ação técnica.

C. Coleta, acondicionamento e transporte

- ✓ Etiquetar, embalar individualmente, lacrar e registrar FAV Digital.
- ✓ Para móveis ligados: isolar sinal e manter carga, quando aplicável.
- ✓ Registrar transferências e recebimentos (hora/local/responsáveis).

D. Pós-diligência

- ✓ Armazenar em local controlado; registrar entrada.
- ✓ Providenciar aquisição forense conforme prioridade e riscos.
- ✓ Consolidar relatório circunstanciado e anexar documentação.

ANEXO II — Documentos em anexo

- ✓ Ficha de Acompanhamento de Vestígio Digital– Fav
- ✓ Certidão de Destruição de Material e Evidências Digitais
- ✓ Cartilha Rápida - Evidências Digitais

ANEXO III — Fluxo Resumido: Dados Voláteis e Dispositivos de Missão Crítica

1. Dados voláteis (ex.: RAM, conexões, chaves de sessão)

- ✓ Avaliar relevância imediata e risco de perda com desligamento.
- ✓ Documentar estado do sistema antes de qualquer intervenção.
- ✓ Se necessária aquisição imediata, registrar ferramenta/método/parâmetros e preservar logs da ação.
- ✓ Justificar por escrito a intervenção e manter rastreabilidade na FAV Digital.

2. Suspeita de criptografia

- ✓ Evitar desligamento automático de equipamento ligado, pois pode tornar dados inacessíveis.
- ✓ Acionar especialista para decisão técnica e priorizar preservação de sessão autenticada, quando aplicável.
- ✓ Registrar justificativa e riscos considerados.

3. Dispositivos de missão crítica

- ✓ Evitar interrupção do serviço quando houver impacto relevante.
- ✓ Priorizar aquisição parcial/lógica e coleta de registros essenciais.
- ✓ Justificar limitações e medidas alternativas adotadas.

ANEXO IV — Procedimento Padronizado:Uso da FAV Digital MPM

- ✓ Preencher a FAV Digital no momento da coleta/reconhecimento, sem rasuras.
- ✓ Atribuir identificador único ao vestígio e correlacionar com lacre e embalagem.
- ✓ Registrar cada movimentação (envio/recebimento) com data/hora, origem/destino e assinaturas.
- ✓ Registrar todo rompimento de lacre, com finalidade, responsável e novo lacre aplicado.
- ✓ Vincular na FAV: relatórios de aquisição, mídias derivadas e *hashes.*