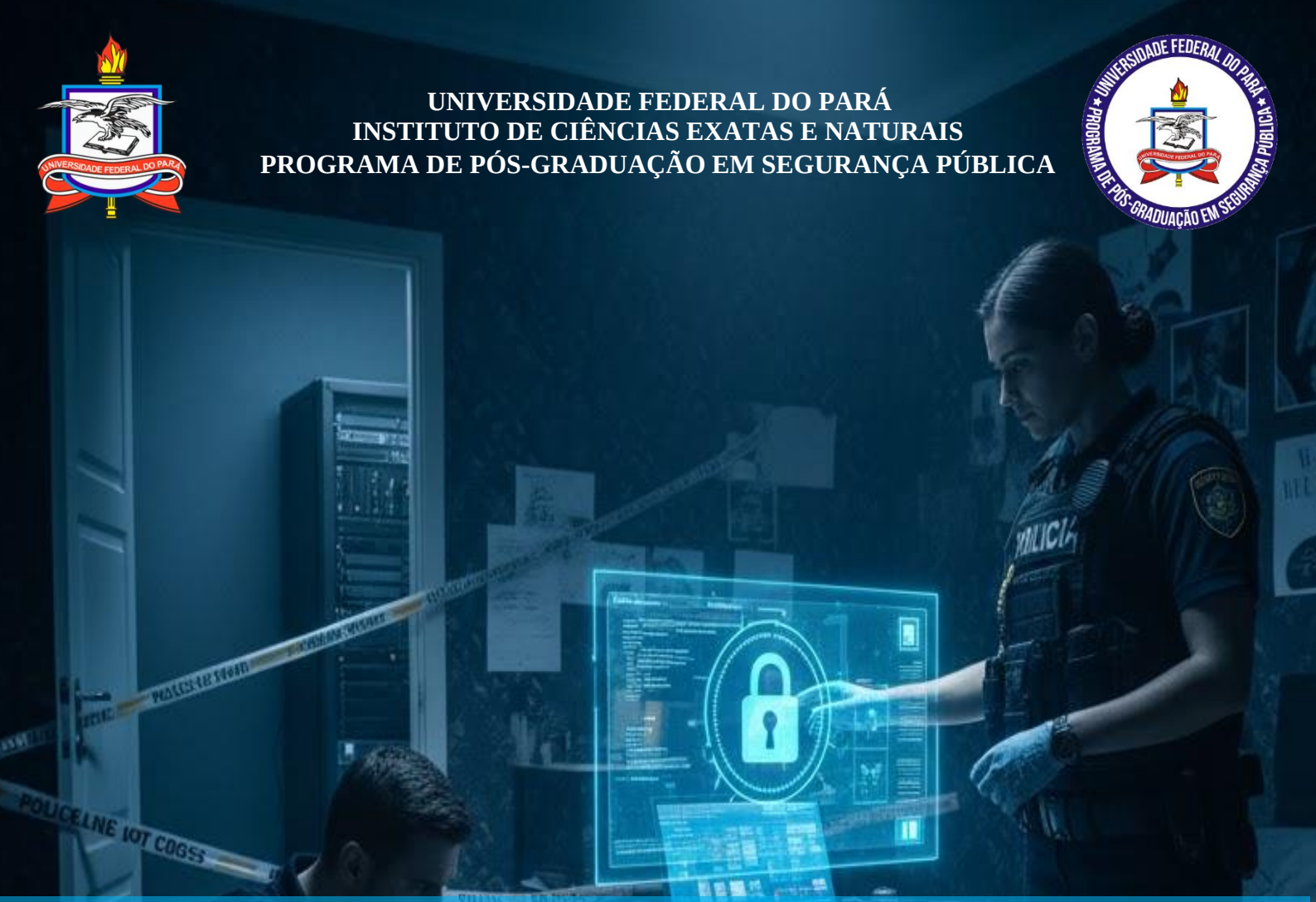
UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM SEGURANÇA PÚBLICA



PROCEDIMENTO OPERACIONAL PADRÃO

PRIMEIRA INTERVENÇÃO DIGITAL (POP/PID)

RODRIGO OCTÁVIO SALDANHA LEITE
RENATO HIDAKA TORRES

BELÉM – PARÁ -BRASIL
2025

REALIZAÇÃO
Universidade Federal do Pará
Instituto de Ciências Exatas e Naturais
Programa de Pós-Graduação em Segurança Pública
Resolução Nº 5.983/2025- CONSEPE/UFPA, de 15 de outubro de 2025

RODRIGO OCTÁVIO SALDANHA LEITE
RENATO HIDAKA TORRES

PROCEDIMENTO OPERACIONAL PADRÃO PRIMEIRA INTERVENÇÃO DIGITAL (POP/ID)

COMO REFERENCIAR ESTA OBRA

LEITE, Rodrigo; TORRES, Renato. Procedimento Operacional Padrão: Primeira intervenção digital (POP/PID). Programa de Pós- Graduação em Segurança Pública. Instituto de Ciências e Naturais. Universidade Federal do Pará. PPGSP/ICEN/UFPA, 2025

BELÉM – PARÁ – BRASIL
2025

SOBRE A PESQUISA CIENTÍFICA QUE RESULTOU NO PRODUTO

O Protocolo Operacional Padrão de Primeira Intervenção Digital (POP/PID) constitui produto técnico-normativo derivado diretamente da pesquisa científica desenvolvida no curso de pós-graduação stricto sensu, tendo como finalidade padronizar a atuação inicial dos policiais militares da Polícia Militar do Pará diante de locais de crime que contenham vestígios digitais.

A construção do POP/PID decorre da constatação, evidenciada na pesquisa, de que falhas nas primeiras ações policiais sobre dispositivos digitais podem comprometer a cadeia de custódia e a validade da prova penal.

Assim, o protocolo foi elaborado para orientar o primeiro agente público quanto à identificação, isolamento, preservação e encaminhamento de vestígios digitais, em conformidade com o Código de Processo Penal, a Portaria nº 82/2021 do MJSP e normas técnicas internacionais.

Do ponto de vista metodológico, o POP/PID resulta de pesquisa aplicada, de abordagem qualitativa, fundamentada em revisão bibliográfica, análise documental e exame do arcabouço jurídico-normativo relacionado à cadeia de custódia digital. Os achados teóricos foram convertidos em diretrizes operacionais claras, objetivas e compatíveis com a rotina do policiamento ostensivo.

O protocolo estrutura-se em etapas sequenciais que contemplam a identificação de evidências digitais, a proteção e o isolamento do local, a definição de ações proibidas e excepcionalmente permitidas, o registro minucioso das intervenções realizadas e o correto encaminhamento dos dispositivos apreendidos. Essas fases visam assegurar a integridade, autenticidade e rastreabilidade dos vestígios desde o primeiro contato policial.

O POP/PID articula-se diretamente com os artigos científicos desenvolvidos na pesquisa[1], os quais discutem a cadeia de custódia digital, a capacitação[2], a responsabilidade do primeiro interveniente e os impactos processuais das falhas na preservação da prova. Enquanto os artigos aprofundam a análise teórica e jurídica, o protocolo materializa esses conhecimentos em instrumento normativo de aplicação imediata.

---

[1] LEITE, Rodrigo; TORRES, Renato. **Análise forense em dispositivos moveis: Gestão da Polícia Militar do Pará na obtenção de provas técnicas digitais.** Programa de Pós- Graduação em Segurança Pública. Instituto de Ciências e Naturais. Universidade Federal do Pará. PPGSP/ICEN/UFPA, 2025.

[2] LEITE, Rodrigo; TORRES, Renato. **A capacitação em preservação de vestígios digitais na polícia militar do Pará.** Programa de Pós- Graduação em Segurança Pública. Instituto de Ciências e Naturais. Universidade Federal do Pará. PPGSP/ICEN/UFPA, 2025.

Dessa forma, o POP/PID consolida a integração entre produção científica e prática institucional, atendendo às exigências acadêmicas do curso e contribuindo para o aprimoramento da atuação da Polícia Militar do Pará na preservação de vestígios digitais e na confiabilidade da prova penal.

PROCEDIMENTO OPERACIONAL PADRÃO 010.00x	
NOME DO PROCESSO	
PRIMEIRA INTERVENÇÃO DIGITAL (POP/PID)	
ETAPA	**PROCEDIMENTO**
VESTIGIOS DIGITAIS	POP 010.00x
ESTABELECIDO EM	**REVISADO EM**
xx/12/2025	xx/xx/202x
PROCEDIMENTO	
ATUAÇÃO POLICIAL MILITAR NA PRESERVAÇÃO DO LOCAL DE CRIME COM VESTIGIOS DIGITAIS	

1. OBJETIVO

Estabelecer diretrizes e procedimentos operacionais padronizados para que os policiais militares da PMPA realizem a primeira intervenção em locais de crime contendo vestígios digitais, assegurando a correta preservação da integridade, autenticidade e rastreabilidade dos dados, conforme os princípios da cadeia de custódia.

2. ÂMBITO DE APLICAÇÃO

2.1. Aplicação: Este protocolo aplica-se a todos os policiais militares da PMPA, especialmente aos que atuam no atendimento de ocorrências, preservação de local de crime, patrulhamento tático e policiamento ostensivo.

2.2. Responsável direto: Comandante da guarnição que primeiro acessar o local.

2.3. Material necessário:

a) uniforme de serviço;

b) colete balístico;

c) armamento regulamentar e carregadores;

d) algemas com chave;

e) viatura policial;

f) cinto de guarnição;

g) BAPM digital;

h) bloco de anotações;

i) rádio portátil;

j) luvas descartáveis;

k) fita de isolamento zebrada;

l) saco antiestático (quando disponível);

m) envelopes próprios para lacre;

n) etiquetas de identificação;

o) lacres numerados;

p) (opcional) bolsas de contenção eletromagnética (Faraday), quando disponíveis.

2.4. Fundamentação Legal

a) Constituição Federal/1988 – Art. 144, §5º

b) Código de Processo Penal (Decreto-Lei nº 3.689/1941) – Art. 6º, I, II e Art. 158-B a 158-F (cadeia de custódia)

c) Código Penal (Decreto-Lei nº 2.848/1940) – Arts. 150, 154-A, 266 e 313-A

d) Portaria nº 82/2021 – Ministério da Justiça e Segurança Pública

e) Lei nº 12.965/2014 (Marco Civil da Internet)

f) Lei nº 13.709/2018 (LGPD)

g) ABNT NBR ISO/IEC 27037:2013 – Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais

3. CONCEITOS BÁSICOS

3.1. Vestígio digital: dado ou informação armazenada, processada ou transmitida em formato digital, relevante para investigação.

3.2. Primeira intervenção: ações iniciais da guarnição ao identificar dispositivos digitais no local do fato.

3.3. Preservação: medidas destinadas a impedir modificação, perda, destruição ou acesso indevido aos vestígios.

3.4. Cadeia de custódia: procedimentos documentados que garantem a rastreabilidade do vestígio desde sua localização até seu uso no processo judicial.

4. FASES DO POP/PID

4.1. Identificação de Evidências Digitais: Ao chegar ao local, a guarnição deve:
4.1.1. reconhecer dispositivos com potencial probatório, tais como:

a) computadores, notebooks, servidores e HDs externos;
b) smartphones, celulares, tablets;
c) pendrives, cartões de memória, SSDs;
d) roteadores, modems, DVRs, NVRs, câmeras IP;
e) consoles de videogame;
f) dispositivos IoT (assistentes virtuais, câmeras inteligentes, fechaduras digitais, automação residencial etc.).

*4.1.2. identificar o estado de cada dispositivo**:** ligado, desligado, bloqueado, conectado à rede, em gravação contínua, etc.*

4.1.3. avaliar risco imediato de perda de dados, como:

a) gravação cíclica (DVR);
b) alertas de autodestruição;
c) mensagens sendo apagadas;
d) bateria crítica;
e) acesso remoto não autorizado.

4.2. Proteção e Isolamento do Local. É primordial:
4.2.1. Estabelecer perímetro de segurança físico (uso da fita zebrada) e perímetro lógico, proibindo manipulação de dispositivos.

4.2.2. Evitar desconectar a energia do ambiente. Caso haja risco iminente (curto, incêndio), realizar a ação sem desligar manualmente os dispositivos, mantendo-se atento a aparelhos ligados que dependam de energia para manter dados voláteis.

4.2.3. Proibir qualquer tentativa de uso, navegação, desbloqueio ou acesso aos equipamentos.

4.2.4. Proteger dispositivos contra:

a) calor, umidade e poeira;

b) manipulação indevida;

c) interferência eletromagnética. (Preferir bolsa de Faraday quando houver risco de apagamento remoto.)

4.2.5. Em dispositivos móveis, quando possível sem manuseio, evitar que recebam sinal:

a) colocando em local isolado;

b) utilizando barreira física (Faraday).

4.3. Ações Proibidas pela Guarnição

*4.3.1. A guarnição NÃO deve, sob nenhuma circunstância**:***

a) ligar dispositivos que estejam desligados;

b) manusear menus, pastas, arquivos, aplicativos ou configurações;

c) inserir senhas, padrões, biometria ou tentar desbloqueio;

d) conectar qualquer dispositivo externo ou cabo;

e) realizar prints internos, gravações de tela ou fotografias de conteúdo interno;

f) alterar posição de mouse, teclado ou tela de computadores ligados;

g) remover dispositivos de armazenamento sem orientação técnica.

4.4. Ações Permitidas em Situações Excepcionais

4.4.1. Quando o dispositivo estiver ligado e houver risco real e imediato de perda de dados, a guarnição pode:

a) fotografar a tela visível, sem toque no equipamento, registrando: hora, ângulo e ambiente;

b) registrar mensagens ou ações que estejam se apagando em tempo real;

c) registrar bateria crítica, alertas de wipe, indícios de acesso remoto;

d) comunicar imediatamente ao CIOp e solicitar equipe especializada (CIISP/PC/Força Tarefa Cibernética);

e) se houver roteador/modem conectado, desconectar fisicamente o cabo de rede, sem acessar menus, evitando comunicação remota.

*4.4.2. Quando houver risco de desligamento automático (ex.: bateria fraca), o militar pode, **sem interagir com o aparelho**, conectá-lo à energia **mantendo o estado atual**, desde que:*

a) não desbloqueie a tela;

b) não navegue em menus;

c) registre no BO a ação realizada e o motivo.

4.5. Registro e Comunicação

4.5.1. O BAPM/BO deve conter obrigatoriamente:

a) descrição detalhada dos dispositivos localizados;

b) estado de cada equipamento (ligado, desligado, bloqueado, conectado à rede);

c) ações tomadas pela guarnição e justificativas;

d) identificação de todas as pessoas que tiveram contato;

e) fotos gerais do local, posição dos dispositivos, numeração de lacres;

f) número de série, marca, modelo e características externas;

g) acionamento formal da equipe técnica (horário, responsável, meio usado);

h) risco identificado (apagamento remoto, overwrite, autodestruição etc.).

4.5.2. Os dispositivos devem permanecer sob vigilância contínua até a chegada da equipe especializada.

5. ENCAMINHAMENTO

5.1. Destino: Os dispositivos apreendidos devem ser lacrados e encaminhados com termo de apreensão específico, seguindo as normas da cadeia de custódia (Portaria nº 82/2021 – MJSP e CPP Art. 158-B).

5.2. Sempre utilizar, quando possível:

a) embalagens antiestáticas;

b) envelopes próprios para evidências digitais;

c) lacres numerados e etiquetas padronizadas.

5.3. Cada etapa de transferência entre responsáveis deve ser registrada com:

a) nome, matrícula/RG e assinatura;

b) data e horário;

c) condição do lacre;

d) destino e finalidade.

6. CAPACITAÇÃO E ATUALIZAÇÃO

6.1. Capacitação: Todos os policiais militares devem receber formação contínua sobre identificação, isolamento e preservação de evidências digitais, incluindo novas tecnologias.

6.2. Atualização: O POP/PID deverá ser revisado anualmente ou sempre que houver atualização legal, normativa ou tecnológica relevante.

7. DISPOSIÇÕES FINAIS

7.1. O descumprimento das diretrizes deste POP: poderá acarretar responsabilização administrativa, civil e penal, além de comprometer a validade probatória.

7.2. Resultado esperado: Este protocolo fortalece a atuação da PMPA no enfrentamento a crimes cibernéticos e crimes tradicionais com elementos digitais, assegurando maior confiabilidade nas investigações.

Paragominas-PA, 03 de novembro de 2025.

RODRIGO OCTÁVIO SALDANHA LEITE
DISCENTE – PESQUISADOR

RENATO HIDAKA TORRES
DOCENTE - PESQUISADOR