# PROCEDIMENTO OPERACIONAL PADRÃO

## *PROCESSO DE COLETA E EXTRAÇÃO DE DADOS DE DISPOSITIVOS MÓVEIS*

*Jhonny de Castro Bacelar*
*Pedro Gleuciano Farias Moreira*
*Renato Hidaka Torres*

| CÓDIGO | TÍTULO: | Versão nº |
|---|---|---|
| **000xx** | **PROCESSO DE COLETA E EXTRAÇÃO** | **0x.0** |

Belém – Pará - Brasil
2024

| | **PROCEDIMENTO OPERACIONAL PADRÃO - POP** | | | Páginas 16 |
|---|---|---|---|---|
| Código POP – «Nome_Unidade_00x» | Data Emissão<br>xx/xx/xxxx | Data de Vigência<br>20xx | Próxima Revisão<br>12/20xx | Versão nº X.X |
| **ELABORAÇÃO:**«NOME_DO_NÚCLEO_FORENSE_DO_ÓRGÃO_DE_INVESTIGAÇÃO_OU_INTELIGÊNCIA» | | | | |
| **TÍTULO:** PROCESSO DE COLETA E EXTRAÇÃO DE DADOS DE DISPOSITIVOS MÓVEIS | | | | |

## 1 - OBJETIVO:

Desenvolver um roteiro para a execução do procedimento de coleta de dispositivos móveis, em estrita adesão às demandas de natureza forense digital, com Base nos Atuais Padrões e Metodologias Científicas, sob a Supervisão do «NOME_DO_NÚCLEO_FORENSE_DO_ÓRGÃO_DE_INVESTIGAÇÃO_OU_INTELIGÊNCIA». O propósito primordial deste processo consiste não apenas em esclarecer as distintas fases associadas à coleta de dispositivos destinados à análise forense, mas também em definir com precisão o roteiro para tal extração de dados. Destaca-se, especialmente, a importância de assegurar a integridade e preservação desses dispositivos desde o instante inaugural da coleta até o arquivamento final, culminando nas etapas subsequentes de encerramento das responsabilidades e descarte apropriado das evidências.

## 2 - CONTEÚDO:

A criação deste Procedimento Operacional Padrão (POP) se fundamentou nas atribuições especificadas para cada setor responsável, conforme estabelecidas pela «NOME_DA_COORDENAÇÃO_DO_ÓRGÃO_DE_INVESTIGAÇÃO_OU_INTELIGÊNCIA» do «NOME_DO_ÓRGÃO_DE_INVESTIGAÇÃO_OU_INTELIGÊNCIA».

## 3 - ABRANGÊNCIA:

Este Procedimento Operacional Padrão (POP) se aplica aos setores que possam participar das diversas etapas e procedimentos essenciais para a condução eficaz da coleta dos dispositivos específicos relacionados ao caso em análise.

## 4 - DEFINIÇÕES:

A coleta e aquisição de dispositivos e/ou evidências são, por natureza, voltadas para a preservação desses elementos, com o propósito de fornecer os elementos essenciais para a

utilização das evidências obtidas em procedimentos legais, garantindo a integridade das evidências geradas durante o processo de coleta/aquisição. Esse processo pode ser realizado no local da investigação ou em laboratório, dependendo do contexto da investigação.

## 5 - PROCESSOS DESENVOLVIDOS:

- Meio de Requisição
- Documentação Obrigatória
- Fotos
- Etiquetas
- Coleta de Smartphones – Android/IOS
    - Identificação (Observações para Coleta e Aquisição)
    - Coleta com *Cellebrite*
    - Coleta – Dispositivo Não Funcional
    - Extração Avançada
        - Extração via EDL
        - Extração via ISP
        - Extração via Chip-off
- Identificação da Evidência Digital / Procedimento Pós-Coleta
    - Ferramentas Utilizadas
    - Instruções
- Responsabilidades

## 6 - MEIO DE REQUISIÇÃO:

- A solicitação para a execução de procedimentos específicos por parte do Agente/Perito externo ou Requerente deve ser feita por meio do Sistema ou por meio de Ofício.
- No contexto atual do «NOME_DO_ÓRGÃO_DE_INVESTIGAÇÃO_OU_INTELIGÊNCIA», o sistema empregado para tal finalidade é o «NOME_DO_SISTEMA» versão xx.xx-xx.

## 7 - DOCUMENTAÇÃO OBRIGATÓRIA:

### 7.1- Formulário de Diligência Padrão

- Este formulário de solicitação de diligência permite que o Agente/Perito ou Requerente expresse claramente o que deseja requisitar, incluindo solicitações de desbloqueio, extração e/ou análise do dispositivo apreendido. O Documento Padronizado deve abranger:
    - Informações do Requerente: Nome, e-mail, endereço e telefone.
    - Matéria do Procedimento: Criminal, Improbidade Administrativa, e/ou outros.
    - Termos da Demanda: Especificam as tarefas a serem realizadas.
    - Referência: Este item identifica a ação ou procedimento que motivou a solicitação de diligência, que pode ser originada a partir do pedido de assistência, o cumprimento de um mandado, entre outros.
    - Anexos: Enumerar os itens, fornecendo o número do lacre e uma breve descrição dos objetos apreendidos, incluindo detalhes como fabricante, modelo e cor.
    - Data e Assinatura do Requerente.

### 7.2- Auto de Apreensão e Apresentação

- Documento que fornece detalhes sobre um dispositivo eletrônico apreendido em uma investigação ou processo legal. Este documento é essencial para o registro adequado e a documentação das evidências eletrônicas. O Auto de Apreensão e Apresentação deve abranger diversos elementos, como:
    - Procedência: informa a origem do dispositivo, como foi encontrado no local da investigação, apreendido de um suspeito ou de outra fonte.
    - Local da Apreensão: fornece informações sobre onde o dispositivo foi apreendido, como endereço, sala, veículo, entre outros.
    - Lacres: registra detalhes dos lacres usados para selar o dispositivo.
    - Data e Hora: registra o momento exato da apreensão, incluindo a data e a hora.
    - Quadro de Identificação: deve conter informações de identificação do dispositivo, como o fabricante, IMEI (Identificação Internacional de Equipamento Móvel), modelo, número de série, tipo (por exemplo, smartphone, tablet, laptop), cor, e outras características físicas relevantes.

- Condição: registra o estado geral do dispositivo no momento da apreensão, incluindo se estava bloqueado, protegido por senha, danificado, ou qualquer outra condição que seja relevante para a investigação.
- Responsáveis: relaciona os nomes e respectivos cargos das pessoas envolvidas na apreensão e na manipulação do dispositivo. Para todos os propósitos legais, este documento deve ser assinado pelo responsável da equipe, que é a autoridade competente, bem como pelo secretário e por duas testemunhas.

### 7.3- Mandado Judicial/Decisão Judicial

- Um mandado judicial é um instrumento emitido por um magistrado que autoriza ações específicas em investigações legais. Ele é fundamental para permitir que as autoridades realizem buscas e apreensões de dispositivos eletrônicos, bem como acessem os dados armazenados nesses dispositivos e em serviços de armazenamento em nuvem. Essa autorização é concedida com base em uma decisão judicial, que determina os parâmetros e as condições para a emissão do mandado. O mandado judicial pode incluir:
  - Autorização para Busca e Apreensão: permissão concedida por uma decisão judicial para que as autoridades busquem e apreendam dispositivos eletrônicos em locais específicos durante uma investigação.
  - Acesso aos dados: permite que as autoridades, de acordo com uma decisão judicial, acessem informações nos dispositivos eletrônicos durante uma investigação. Isso envolve desbloquear dispositivos protegidos e examinar seu conteúdo em busca de evidências relevantes.
  - Acesso a Serviços de Nuvem: autorização legal para recuperar informações de serviços de armazenamento em nuvem, um elemento fundamental em investigações. Conforme determinado na decisão, isso pode envolver a interceptação e a quebra do sigilo de dados em contas de e-mail.
- Assim, a decisão judicial serve como base para a emissão do mandado, estabelecendo os parâmetros legais e os requisitos para a condução da investigação.

### 7.4- Cadeia de Custódia

- Procedimento essencial no campo jurídico e investigativo, visando registrar e documentar evidências ao longo de processos legais e investigações. Sua finalidade principal é

preservar a integridade e autenticidade das evidências, o que, por sua vez, assegura sua admissibilidade jurídica.

- A cadeia de custódia começa no instante da apreensão do dispositivo eletrônico, simultaneamente ao Auto de Apreensão e Apresentação. Para garantir uma cadeia de custódia apropriada das evidências eletrônicas, é essencial que ela incorpore os elementos a seguir:

### 7.4.1- Informações Procedimentais

- Número do Procedimento Investigatório
- Número do Processo
- Lacre
- Forma de apreensão do aparelho (busca e apreensão, flagrante, entrega voluntária)
- Há autorização judicial ou expresso consentimento dos proprietários para extração dos dados?

### 7.4.2- Mídia Eletrônica

- Número de itens
- Descrição (Inclusive cor, estado de conservação e eventual senha)
- Fabricante
- Modelo
- Número de Série

### 7.4.3- Arquivo Digital (Para evidência digital coletada no local)

- Data
- Criada por
- Nome da ISO criada
- *Hash* da ISO

**Obs.:** O preenchimento da descrição do arquivo digital deve ocorrer de forma simultânea ao preenchimento da Certidão de Cópia da Evidência Digital, que poderá ser assinada pelo investigado, seu advogado legal ou por alguém designado no momento.

### 7.4.4- Sequência da Cadeia de Custódia:

- Esses são os elementos essenciais da cadeia de custódia para documentar a jornada das evidências eletrônicas desde a sua coleta até seu armazenamento e movimentações subsequentes. Eles ajudam a garantir a integridade e a admissibilidade das evidências em um contexto legal:
    - Origem
    - Nome do responsável pela movimentação
    - Motivo da movimentação
    - Data e hora da movimentação
    - Assinatura/Matrícula do responsável
    - Destino

## 8 - ETIQUETAS

- Tanto os dispositivos apreendidos quanto os dispositivos de destino, como os HDs externos, devem ser marcados com etiquetas de identificação.
    - Dispositivo Apreendido (Origem):
        - A Identificação do dispositivo apreendido deve constar:
        - A Unidade responsável pela extração
        - O nome da Operação
        - Número da demanda do «SISTEMA»
        - Lacre
        - Fabricante, modelo e cor do aparelho.
        - Exemplo de Etiqueta do dispositivo apreendido:

«NOME_DO_ÓRGÃO»/«NOME_DO_NÚCLEO_FORENSE»

«**NOME_DA_OPERAÇÃO**»
«SISTEMA»: «Nº_DO_PROCESSO»
LACRE: «Nº_DO_LACRE»
Dispositivo: «TIPO_DE_DISPOSITIVO»

«FABRICANTE DO DISPOSITIVO»
«MODELO DO DISPOSITIVO» «COR»
T. Resp: «ID_DO_TÉCNICO_RESPONSÁVEL»

- Unidade de Armazenamento (Destino):
  - Deve seguir formato laboratorial padrão que engloba os seguintes elementos:
  - O nome da Operação
  - Números das demandas do «SISTEMA»
  - Lacres
  - Tipo de Dispositivos (Smartphones, SSDs, HDs, Pen drives, etc...)
  - Técnico Responsável
  - Exemplo de Etiqueta de identificação da Unidade de Armazenamento (Destino):

«NOME_DO_ÓRGÃO»/«NOME_DO_NÚCLEO_FORENSE»

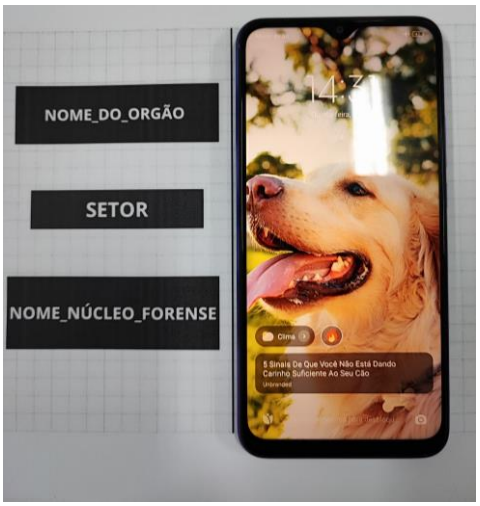
«**NOME_DA_OPERAÇÃO**» «**HD xx**»
«SISTEMA»: «Nº_DOS_PROCESSOS»
LACRES: «Nº_DOS_LACRES »
Dispositivos: «TIPO_DE_DISPOSITIVOS»
T. Resp: «ID_DO_TÉCNICO_RESPONSÁVEL»

**Obs.:** Caso o Órgão possua envelopes com lacre de segurança personalizados, os códigos de barras nas etiquetas de identificação dos smartphones podem ser utilizados.

## 9 - FOTOS

- São registradas em todas as etapas, desde a apreensão e lacração inicial até o deslacramento para extração e subsequente relacração. Desempenham um papel fundamental na documentação e no registro do dispositivo.
  - **Na apreensão**
    - Fotografias da parte frontal e traseira do dispositivo com a finalidade de identificar seu fabricante e modelo, qualquer identificação pessoal (se presente) e seu estado físico. Além disso, é necessária uma fotografia do aparelho devidamente lacrado, a ser usada na elaboração do Relatório de Operação.
  - **Deslacre pelo Núcleo de Extração**

- O «NOME_DO_NÚCLEO_FORENSE_DO_ÓRGÃO_DE_INVESTIGAÇÃO» do «NOME_DO_ÓRGÃO_DE_INVESTIGAÇÃO_OU_INTELIGÊNCIA»/«NOME_DO_ÓRGÃO», é o departamento responsável pela extração do conteúdo dos dispositivos apreendidos. Portanto, somente o técnico encarregado da extração deve abrir o dispositivo, registrando uma imagem do mesmo ainda dentro do envelope com lacre de segurança personalizado antes de romper o lacre.
- Exemplos de Fotografias:

| **Fotos de Smartphones apreendidos para extração (Origem)** | |
|---|---|
| Frente do aparelho | Traseira do aparelho |
|  |  |

| **Fotos de HDs de Armazenamento (Destino)** | |
|---|---|
| HD de Destino | Mais de um HD de destino |



## 10 - COLETA DE SMARTPHONES

### 10.1- Identificação:

- Fabricante/modelo
- Verificar se aparelho se encontra bloqueado ou desbloqueado
    - Caso bloqueado
        - Verificar a presença da senha no auto de apreensão. Se ausente, iniciar procedimento de desbloqueio conforme protocolo interno e ferramentas disponíveis.
    - Caso Desbloqueado e em funcionamento:
        - *Cellebrite*;
        - Outras ferramentas forenses para equipamentos *MOBILE*;
        - Avilla *Forensics*;
    - Caso exista algum problema que resulte no não funcionamento do dispositivo:
        - Utilizar os métodos de extração avançada.
        - Reparo eletrônico.

**Obs.:** A prioridade na coleta é usar o *Cellebrite* como método principal, mas se não for viável, outros métodos podem ser usados.

### 10.2- Coleta com *Cellebrite*:

- De acordo com a criptografia do dispositivo, o técnico ou perito deve ser capaz de identificar a melhor técnica para realizar a coleta. Tendo como guia de ordem:
  - Coleta de Sistema de Arquivos;
  - Coleta Lógica;
  - Coleta Física ou Completa;
  - Coleta Lógica com downgrade de aplicativos;
- Ainda que a coleta física seja viável, o técnico/perito deve seguir uma ordem para prevenir perda de dados em caso de falha na coleta física.
- É fundamental obter a aprovação expressa do requerente antes de considerar a coleta com *downgrade* de aplicativos. Isso é necessário devido à possibilidade de perda da capacidade de visualizar conversas em aplicativos como o WhatsApp, por exemplo. Mesmo que as tabelas do aplicativo estejam acessíveis, apenas uma extração completa ou física, que inclua a reinstalação do aplicativo no dispositivo, pode restaurar as conversas.
- Caso não seja possível utilizar o *Cellebrite*, pode se utilizar as outras ferramentas disponíveis no laboratório:
  - Avilla *Forensics*;
  - *Magnet Axiom*;
  - Coleta avançada com ISP, CHIPOFF, ou outro meio;

## 11 - DISPOSITIVO NÃO FUNCIONAL

- Caso o dispositivo se encontre com avaria e não seja possível realizar a aquisição, o técnico deve avaliar o cenário.
  - **O dispositivo pode ser consertado?**
    - Se sim, o dispositivo deve receber a manutenção para que possa ser feita a extração pela ferramenta adequada.
    - Caso não seja possível uma manutenção, deve se avaliar a necessidade e possibilidade de métodos de extração avançada.

### 11.1- Extração Avançada

- Quando as circunstâncias permitirem uma extração avançada, o técnico precisa possuir o conhecimento técnico para determinar o cenário mais adequado para o caso, considerando o risco e a importância da obtenção das informações. Deve-se avaliar a viabilidade de:
    - Extração via EDL (Modo de Download de Emergência)
        - Possível em alguns modelos que possuem processador Qualcom
- Extração via ISP
    - Possível através do conhecimento das pinagens
        - Processo Manual
        - Processo com VR-*Table*
- Extração através de *Chip-off*

## 12 - PROGRAMAS DE ANÁLISE

- Extração Inicial dos Dados
    - Os procedimentos de análise de dispositivos eletrônicos apreendidos são essenciais para coletar informações relevantes em investigações criminais, processos legais e questões de segurança. Ao apreender um dispositivo, a etapa inicial envolve a extração dos dados para criar um arquivo de "imagem". No entanto, essa imagem não é legível diretamente, sendo uma representação digital do conteúdo do dispositivo.
- Análise com Software Especializado:
    - Após a extração, os dados são tratados e analisados por meio de software especializado, como o *Physical Analyzer* no contexto do *Cellebrite*. Esses programas são desenvolvidos para descriptografar, organizar e apresentar os dados de maneira compreensível, permitindo aos investigadores examinar mensagens, registros de chamadas, fotos, vídeos e outros dados relevantes do dispositivo.
- Variedade de Softwares de Análise:
    - Além do *Physical Analyzer*, diversas opções de *software*, como *iPed, Autopsy*, FTK (*Forensic Toolkit*) e outros, estão disponíveis para conduzir a análise de dispositivos eletrônicos. Cada programa tem características e capacidades diferentes, sendo adequados para situações e requisitos específicos de investigação, oferecendo uma gama diversificada de ferramentas para os peritos utilizarem.

## 13 - IDENTIFICAÇÃO DA EVIDÊNCIA DIGITAL/PROCEDIMENTO PÓS-COLETA.

- Os resultados da extração e do processamento de dados são categorizados com base no software utilizado durante a coleta. Normalmente, a extração bruta obtida através das ferramentas forenses é organizada de acordo com o tipo de extração realizada no dispositivo.
- Qualquer extração bruta que precise ser tratada como parte do processo de evidência deve ser armazenada na pasta "Evidência Forense Digital", junto com o ***hash*** SHA 256 das extrações que serão processadas. Um ***hash*** é uma função matemática que converte um arquivo em um código alfanumérico, funcionando como uma "impressão digital" exclusiva do documento.
- A estrutura da pasta "Evidência Forense Digital" segue o seguinte formato: A pasta é organizada sob a pasta que identifica o fabricante e o número de lacre do dispositivo, separados por um sublinhado (_). Por exemplo, "«FABRICANTE DO DISPOSITIVO»_«nº do lacre»". A pasta com o fabricante e o número do lacre é posicionada abaixo da pasta que identifica o sistema e o número do procedimento que deu origem à demanda, como por exemplo: "«SISTEMA»_«nº do Processo»".
- Todas essas pastas são armazenadas em um disco rígido externo ou na nuvem. Portanto, a estrutura de pastas segue o padrão:
    - OPERAÇÃO «NOME DA OPERAÇÃO»
        - «SISTEMA»_«nº do Processo»
            - «FABRICANTE DO DISPOSITIVO»_«nº do lacre»
                - Evidência Forense Digital
                    - Extração Bruta
- Após a aquisição, o disco de destino da evidência deve ser etiquetado.
- O dispositivo deve ser relacrado em envelope com lacre de segurança personalizado e ser devolvido a Central de Custódia via cadeia de Custódia.
    - A cadeia de custódia deve estar preenchida com o ocorrido durante o processo referente a extração e deve reunir as assinaturas:
        - Referentes a cada movimentação na cadeia de custódia.
- A cadeia de custódia deve ser digitalizada em cada movimentação e anexada ao sistema ou constar no sistema próprio de custódia.

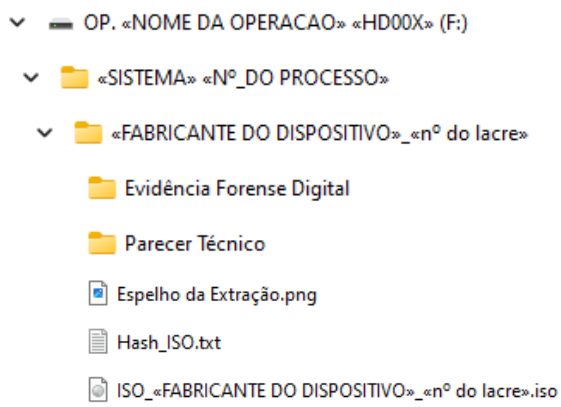
**Obs.:** A adoção de uma cadeia de custódia digital tem sido objeto de discussões, sendo importante que o órgão desenvolva um sistema próprio ou em parceria com outros órgãos ou universidades.

## 14 - ARMAZENAMENTO E TRATAMENTO

- As evidências devem ser copiadas para outro HD Externo, em nuvem ou *Storage*.
- O Processamento então é realizado com o programa:
    - *Physical Analyzer* da *Cellebrite* ou outra ferramenta
- Se for necessário, o tratamento pode ser realizado pelo IPED (Indexador e Processador de Evidências Digitais). Isso ocorre porque, uma vez que são ferramentas diferentes, elas podem oferecer perspectivas de análise distintas. Independentemente do método de análise escolhido para o caso, os dados já devem estar processados quando o departamento de análise for examiná-los.
- A pasta resultante do processo deve ser denominada "Parecer Técnico". No caso do *Cellebrite*, os arquivos gerados seguem um padrão de nomenclatura com base na data e hora da aquisição. No entanto, a base de dados tratada é nomeada como "Base_Tratada". Além disso, um arquivo executável é criado, conhecido entre técnicos e peritos como "Reader".
- Os arquivos gerados durante o processo de tratamento devem ser armazenados em um disco rígido externo, em nuvem ou *Storage*. O caminho para a pasta parecer técnico, segue a seguinte estrutura:
    - OPERAÇÃO «NOME DA OPERAÇÃO»
        - «SISTEMA»_«nº do Processo»
            - «FABRICANTE DO DISPOSITIVO»_«nº do lacre»
                - Parecer Técnico
                    - Base_Tratada
                    - «Arquivo_executável».exe
- Criada a pasta, é essencial confirmar o funcionamento correto do executável para garantir o acesso a todo o conteúdo da base tratada. Caso o executável apresente falhas, é essencial repetir o procedimento de tratamento ou, em último caso, a etapa de extração.
- Para assegurar a adequada realização da extração e a correta indexação dos arquivos é fundamental capturar uma imagem da tela do «Arquivo_executável.exe» em uso, evidenciando a disposição dos arquivos acessíveis. Salve essa captura com o nome

"Espelho da Extração" e guarde-a na pasta identificada como "«FABRICANTE DO DISPOSITIVO»_«nº do lacre»".

- É essencial criar uma imagem ISO compactada da pasta "Parecer Técnico", possibilitando a substituição do arquivo em caso de problemas com o *Cellebrite*Reader.exe.
- Criar um ***Hash*** de integridade para essa imagem ISO.
- Após concluir a organização das pastas, tanto para a evidência digital quanto para o parecer técnico produzido, é fundamental manter a estrutura exemplificada abaixo até uma próxima atualização deste Procedimento Operacional Padrão (POP):




- A pasta referente ao Parecer Técnico conterá:
  - O arquivo com nome: “Base_Tratada”, que é o arquivo contendo a base de dados a ser executado.
  - O arquivo executável "«Arquivo_executável».exe", que permite que o usuário acesse o conteúdo extraído.
- Após os procedimentos, as evidências coletadas nos discos de armazenamento devem ser etiquetadas e disponibilizada em nuvem ou em outro HD Externo uma cópia ao demandante.
- Os HDs Externos sob posse do Núcleo Forense não devem sair do laboratório, nem ser movimentados entre os departamentos, para prevenir danos ou corrupção nos arquivos. APENAS as cópias e espelhamentos gerados a partir destes discos rígidos podem ser transportados. Esses HDs devem ser guardados protegidos contra poeira e umidade, evitando impactos físicos.
- O Backup em nuvem também deve ser observado para garantir segurança extra às extrações.

- Os dispositivos periciados devem ser inseridos em um novo envelope com lacre de segurança, acompanhados dos lacres rompidos, das documentações e devolvidos à Central de Custódia.

## 15 - RESPONSABILIDADES:

- Os profissionais que participam dos processos descritos devem aderir aos procedimentos recomendados neste POP. Exceções podem ser consideradas somente em circunstâncias além dos cenários delineados, como indisponibilidade, ausência de equipamento ou falhas técnicas.