PROCEDIMENTO OPERACIONAL PADRÃO

PROCESSO DE RECUPERAÇÃO E SANITIZAÇÃO DE DADOS POR MÉTODOS FORENSES

Jhonny de Castro Bacelar
Pedro Gleuciano Farias Moreira
Renato Hidaka Torres

CÓDIGO **000xx**	TÍTULO: **PROCESSO DE RECUPERAÇÃO E ELIMINAÇÃO**	Versão nº **0x.0**

Belém – Pará - Brasil
2024

	PROCEDIMENTO OPERACIONAL PADRÃO - POP			Páginas 05
Código POP – «Nome_Unidade_00x»	Data Emissão xx/xx/xxxx	Data de Vigência 20xx	Próxima Revisão 12/20xx	Versão nº X.X
ELABORAÇÃO: «NOME_DO_NÚCLEO_FORENSE_DO_ÓRGÃO_DE_INVESTIGAÇÃO_OU_INTELIGÊNCIA»				
TÍTULO: PROCESSO DE RECUPERAÇÃO E SANITIZAÇÃO DE DADOS POR MÉTODOS FORENSES				

1 - OBJETIVO:

Desenvolver um Roteiro para a Execução de procedimentos de realização de recuperação e sanitização permanente de arquivos sensíveis armazenados em HDs, juntamente com os arquivos relacionados aos casos, pela área de Forense Digital do Órgão. Isso inclui a apresentação dos princípios e condutas para conduzir essas operações de maneira segura, atendendo às necessidades de backup e armazenamento seguro. Os procedimentos para manter os arquivos ou realizar seu descarte após o processo de análise dos dispositivos submetidos à análise forense serão esclarecidos, visando a preservação desses dados, o encerramento de responsabilidades e o descarte adequado das informações sensíveis.

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 a todos os setores envolvidos nas etapas e procedimentos relacionados a aquisição e tratamento de dados do Órgão.

4 - DEFINIÇÕES:

O processo de recuperação e sanitização de dados constitui uma etapa essencial no fluxo de trabalho, ocorrendo como parte integrante do processo laboral pós-investigativo. Este processo estabelece as normas e condições necessárias para sua execução de maneira adequada e eficaz.

5 - PROCESSOS DESENVOLVIDOS:

- Processos de Recuperação de dados via ferramentas Forenses
    - Ferramentas e técnicas
- Processos de sanitização permanente de dados de HDs
    - Sanitização Lógica
    - Sanitização Física
- Documentos de Sanitização
- Responsabilidades

6 - PROCESSOS DE RECUPERAÇÃO DE DADOS VIA FERRAMENTAS FORENSES

- Conectar a mídia na Case para HD
    - Avaliar estado da Mídia:
        - Verificar se os arquivos têm backup disponível.
        - Confirmar se a mídia está operacional
            - Sistema de arquivos funcional
            - Sistema de arquivos corrompido

- Utilização de Softwares de Recuperação
    - Executar um *Software* que utiliza a técnica *Data Carving* (*Scalpel, foremost, PhotoRec, TestDisk, etc.*)

- Executar um software confiável para recuperar os arquivos deletados (*Stellar Data Recovery, EaseUS Data Recovery Wizard, Puran File Recovery, Recuva, Disk Dril, Glarysoft File Recovery Free, Restoration, etc.)*

- Copiar o conteúdo recuperado para uma unidade de backup

7 - PROCESSOS DE SANITIZAÇÃO PERMANENTE DE DADOS DE HDS

O processo de sanitização é uma importante medida para preservar a integridade e a segurança das informações sensíveis, protegendo o órgão e seus usuários contra potenciais violações de segurança e garantindo a conformidade com regulamentações de proteção de dados.

- Destruição Lógica
  - Utilizado em unidades de armazenamento em funcionamento
    - Utilizar uma ferramenta de formatação de baixo nível de disco rígido *(Sistemas de distribuição forense como Linux, Hiren's Boot, Active Kill Disk, EaseUS Partition Master, File Shredder, etc.)*
  - Gerar certificado de sanitização
    - Encaminhar à unidade de armazenamento para reaproveitamento ou descarte
  - O disco deve ser verificado após o processo, mesmo após a expedição do certificado de sanitização.
  - Após a sanitização, esse disco deve ser formatado e criado o seu sistema de arquivo (Sistema de arquivo EXFAT).
  - Nomear o disco seguindo a nomenclatura «NOME_DO_DEPARTAMENTO»_XX.
  - Discos já esterilizados deverão receber a etiqueta de identificação como "SANITIZADO" e disponível para reutilização.

- Destruição Física
  - Utilizado em HDs com problema mecânico ou falhas
    - Martelar Mídia

- Perfurar o disco do drive
- Fragmentadora de Disco Rígido

- Gerar Certidão de Descarte de Unidade
  - Encaminhar unidade de armazenamento para reaproveitamento ou descarte

8 - DOCUMENTOS DE SANITIZAÇÃO

Ao final do procedimento de sanitização, é necessário gerar um relatório ou certificado que ateste a execução bem-sucedida do procedimento *Zero Fill*. Esse documento é essencial para garantir conformidade com regulamentações, responsabilizar os envolvidos, assegurar transparência e confiança, e fornecer evidências em caso de disputas legais ou auditorias.

9 - RESPONSABILIDADES:

- Os profissionais responsáveis pelos processos descritos devem realizar os procedimentos conforme orientado neste POP. A exceção ocorrerá apenas em situações em que o procedimento se tornar inviável devido à falta de equipamentos ou ao mau funcionamento destes.