

## POLÍTICA DE DESCARTE DE MÍDIA PARA CERTIFICADO A3

### IDENTIFICAÇÃO

<b>Nome da Empresa: IDFEDERAL CERTIFICADOS DIGITAIS LTDA</b>
<b>CNPJ: 33.216.689/0001-45</b>
<b>Endereço: Av. Virgílio Soeira, Nº 127</b>
<b>Versão: 01</b>
<b>Grau de Sigilo: Ostensivo</b>
<b>Vigência: Início: 01/03/2024   Fim: Indeterminado</b>

### 1. FINALIDADE

Esta política estabelece diretrizes para o descarte seguro de mídias utilizadas na emissão de certificados digitais A3, garantindo a proteção das informações e prevenindo a recuperação indevida de dados sensíveis.

### 2. ÂMBITO DE APLICAÇÃO

Aplica-se a todos os colaboradores, prestadores de serviço e setores da IDFEDERAL CERTIFICADOS DIGITAIS LTDA envolvidos na manipulação, armazenamento e descarte de mídias físicas e digitais relacionadas aos certificados digitais A3.

### 3. DEFINIÇÕES

**Ativo de Informação:** Qualquer meio de armazenamento que contenha dados sigilosos ou sensíveis, incluindo tokens USB, smart cards e dispositivos de armazenamento.

**Sanitização de Dados:** Processo de eliminação segura de informações para impossibilitar a recuperação.

**Descarte Seguro:** Procedimento formal de retirada de ativos de informação do uso, garantindo a irreversibilidade da remoção de dados.

## **4. DIRETRIZES**

### **4.1. Procedimentos para Sanitização**

**4.1.1.** Todo ativo de informação que deixar de ser utilizado, por qualquer motivo, deverá obrigatoriamente passar por um processo de sanitização antes do descarte, reaproveitamento ou reciclagem.

**4.1.2.** No caso de falha ou defeito no ativo de informação, a unidade responsável deverá seguir o procedimento de sanitização antes de encaminhar para substituição, reciclagem ou devolução ao fabricante.

**4.1.3.** Os métodos recomendados para sanitização incluem:

- Desmagnetização (quando aplicável)
- Sobrescrita com dados aleatórios
- Reset para configurações de fábrica
- Destruição física (caso não haja outra opção viável)

### **4.2. Certificação da Sanitização**

**4.2.1.** Após a sanitização, o responsável deverá preencher e assinar um Certificado de Sanitização, contendo:

- Identificação do ativo (fabricante, modelo, número de série);
- Método utilizado na sanitização;
- Ferramenta e versão utilizada;
- Destino do ativo (reuso, doação, reciclagem ou destruição);
- Assinatura do responsável pela sanitização.

**4.2.2.** O Certificado de Sanitização deverá ser arquivado pelo período mínimo de 5 anos para fins de auditoria e conformidade.

### **4.3. Responsabilidades**

**4.3.1.** A responsabilidade pelo cumprimento desta política recai sobre:

- Setor de TI: Implementação e execução dos processos de sanitização.
- Gestão de Segurança da Informação: Monitoramento e auditoria do cumprimento da política.
- Setor de Logística: Recolhimento e destinação dos ativos sanitizados.

## **5. DISPOSIÇÕES FINAIS**

**5.1.** O descarte de ativos de informação somente será realizado mediante autorização formal.

**5.2.** Qualquer situação não prevista nesta política deverá ser encaminhada à Coordenação de Segurança da Informação para orientação.

**5.3.** Esta política entra em vigor na data de sua aprovação e deverá ser revisada periodicamente para garantir sua atualização e eficácia.

Documento assinado digitalmente em conformidade com a Medida Provisória nº 2200-2/2001.



# FEDERAL