

**Governo do Estado de São Paulo
Hospital das Clínicas da Faculdade de Medicina de Marília
Seção de Processos de Qualidade**

HCFAMEMA PROCEDIMENTO OPERACIONAL

Nº do Processo: 144.00016298/2025-38

Assunto: DESCARTE CORRETO DE MATERIAIS SENSÍVEIS E EQUIPAMENTOS

CÓDIGO: HCF-DITI-PO-01

REVISÃO: 0

1. OBJETIVO

Assegurar o descarte adequado de dados sensíveis, como toners, fotocondutores, peças e componentes de informática e equipamentos obsoletos, garantindo a proteção das informações, o cumprimento das exigências legais e a sustentabilidade ambiental, de modo a impedir qualquer possibilidade de recuperação de dados.

2. APLICAÇÃO

Aplica-se a todos os colaboradores, estagiários, setores administrativos, unidades assistenciais, prestadores de serviço e demais terceiros envolvidos no tratamento, armazenamento ou descarte de materiais que contenham dados sensíveis.

3. RESPONSABILIDADE

3.1 USUÁRIOS/SETORES SOLICITANTES

- Abertura da solicitação;
- Entrega adequada do material.

3.2 CHEFE DE DIVISÃO / ANALISTA DE SISTEMAS / OPERADOR DE COMPUTADOR E PROGRAMADOR

- Destruição de mídias digitais;
- Execução técnica do descarte de equipamentos.
- Validação dos métodos de destruição;
- Supervisão do processo.
- Auditoria, conformidade e mitigação de riscos.
- Orientação quanto ao tratamento e eliminação de dados.

3.3 ALMOXARIFADO / PATRIMÔNIO

Execução conforme etapa 7.7.

3.4 TERCEIROS/PRESTADORES

- Execução técnica do descarte ambiental;
- Emissão de Certificado de Destruição.

4. ABREVIATURAS E SIGLAS

DITI – Divisão de Infraestrutura em Tecnologia da Informação;

GLPI - *Gestionnaire Libre de Parc Informatique*: software livre utilizado para gestão de ativos de TI, helpdesk e suporte técnico.

HCFAMEMA – Hospital das Clínicas da Faculdade de Medicina de Marília;

LGPD - Lei Geral de Proteção de Dados;

PO – Procedimento Operacional;

SEI – Sistema Eletrônico de Informação;

TI – Tecnologia da Informação.

5. MATERIAIS/EQUIPAMENTOS/FERRAMENTAS

Materiais:

Não se aplica.

Equipamentos:

Computadores.

Ferramentas:

Ferramentas (chaves e alicate);

Recipientes lacrados e invioláveis.

6. CONCEITOS E FUNÇÕES

6.1 DESCARTE

Ato de remover materiais ou equipamentos que não possuem mais utilidade operacional ou que atingiram o fim de seu ciclo de vida, garantindo que não representem risco à informação, à segurança ou ao meio ambiente.

6.2 DESTRUIÇÃO

Processo que torna um documento, mídia ou equipamento irreversível e inacessível, de modo que a informação nele contida não possa ser recuperada.

6.3 CONTAMINAÇÃO CRUZADA

Situação em que materiais ou equipamentos limpos ou seguros são inadvertidamente expostos a materiais que contêm informações sensíveis, causando risco de vazamento ou acesso não autorizado.

6.4 DESMAGNETIZAÇÃO (OU DESMAGNETIZAÇÃO DE MÍDIA)

Processo físico ou eletromagnético que apaga permanentemente os dados armazenados em mídias magnéticas, como HDs, fitas ou discos removíveis.

6.5 SEGREGAÇÃO DE MATERIAIS

Separar documentos, equipamentos e mídias de acordo com seu nível de sensibilidade.

6.6 ARMAZENAMENTO SEGURO

Guardar temporariamente materiais sensíveis em local restrito até o recolhimento.

6.7 RECOLHIMENTO FORMAL

Solicitar órgãos ou serviços responsáveis (DITI, Controle Patrimonial, Divisão de Suprimentos) para o transporte seguro.

6.8 DESCARTE CERTIFICADO

Garantir destruição através de processos auditáveis, como fragmentação certificada, desmagnetização ou encaminhamento a fornecedores autorizados.

6.9 REGISTRO E RASTREABILIDADE

Manter evidências do descarte, incluindo data, responsável e método de destruição, para conformidade legal e institucional.

7. BASE LEGAL

7.1 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Este procedimento está fundamentado na Lei nº 13.709/2018 – LGPD, considerando que equipamentos submetidos à manutenção poderão conter dados pessoais, dados sensíveis, informações institucionais ou registros operacionais.

Assim, todas as etapas deste procedimento devem observar e atender os seguintes princípios:

- **Finalidade:** acessar dados apenas quando estritamente necessário para diagnóstico, correção ou validação da manutenção.
- **Adequação:** todo o tratamento realizado deve ser compatível com a finalidade prevista neste PO.
- **Necessidade:** o acesso será mínimo e limitado ao indispensável para resolução do incidente.
- **Prevenção:** adoção de medidas para evitar incidentes que possam comprometer dados, sistemas ou equipamentos.
- **Segurança:** aplicação de controles técnicos e administrativos para prevenir acesso não autorizado, perda, vazamento, destruição ou modificação indevida.
- **Responsabilização e Prestação de Contas:** todos os envolvidos devem comprovar conformidade com a LGPD e registrar adequadamente suas atividades.
- **Minimização:** qualquer arquivo, dado ou informação acessada será limitada ao essencial para o atendimento.

7.2 CLASSIFICAÇÃO DA INFORMAÇÃO

Todos os documentos e materiais são classificados nas seguintes categorias:

- **Públicos:** informações que podem ser divulgadas sem restrição.
- **Internos:** informações destinadas apenas ao uso dentro da organização, sem autorização para divulgação externa.
- **Confidenciais:** informações restritas a áreas ou pessoas específicas, cuja divulgação indevida pode gerar riscos operacionais ou institucionais.

- **Dados Pessoais:** informações relacionadas a pessoa física identificada ou identificável.
- **Dados Sensíveis:** dados pessoais que revelam origem racial ou étnica, convicções religiosas, opiniões políticas, dados de saúde, biométricos, entre outros protegidos por legislação específica.
- **Requisito de Segurança:** Materiais que contenham dados pessoais ou dados sensíveis devem ser submetidos a controles rigorosos de segurança, incluindo destruição certificada, a fim de evitar acesso, uso ou recuperação indevida das informações.

8. DESCRIÇÃO DO PROCEDIMENTO

8.1 MÉTODOS SEGUROS DE DESTRUIÇÃO

8.1.2 MÍDIAS DIGITAIS

- HDs: desmagnetização + trituração física;
- SSDs: Secure Erase + destruição física (NIST 800-88);
- Pendrives/cartões: perfuração + trituração.

8.1.3 EQUIPAMENTOS DE TI

- Remoção e destruição do meio de armazenamento.

8.2 REQUISITOS DE SEGURANÇA DURANTE O PROCESSO

- Armazenamento em local seguro com acesso controlado;
- Transporte em recipiente lacrado e identificado;
- Registro fotográfico quando aplicável.

8.3 TONERS E FOTOCONDUTORES PADRONIZADOS

Os toners e fotocondutores padronizados que necessitarem de descarte devem ser acondicionados de forma adequada e identificados. Após isso, o responsável deverá solicitar à Divisão de Suprimentos e Abastecimento o recolhimento e o encaminhamento para o descarte conforme os procedimentos institucionais vigentes.

8.4 TONERS NÃO PADRONIZADOS

Os toners não padronizados devem ser acondicionados adequadamente e devidamente identificados. Em seguida, o responsável deverá solicitar à empresa fornecedora o recolhimento e o encaminhamento para o descarte, conforme previsto nos procedimentos e responsabilidades estabelecidos contratualmente.

8.5 EQUIPAMENTOS E COMPONENTES DE INFORMÁTICA

Os equipamentos e componentes de informática que necessitarem de descarte devem ser acondicionados de forma adequada e mantidos em local seguro. Após este procedimento, o responsável deverá emitir solicitação via SEI ao Serviço de Controle Patrimonial, para que seja realizado o recolhimento e o devido encaminhamento para descarte, conforme as normas e procedimentos institucionais vigentes.

8.6 CADEIA DE CUSTÓDIA

Registro obrigatório contendo:

Setor solicitante;
Responsável pela entrega;
Responsável pelo recebimento;

Quantidade e descrição do material;
Número de patrimônio;
Método de destruição;
Fotos;
Data e hora.

8.7 FORNECEDOR HOMOLOGADO

Toda empresa de descarte:

Deve ser homologada;
Seguir normas ambientais e de privacidade;
Emitir Certificado de Destruição.

8.8 RISCOS E CONTROLES

8.8.1 RISCOS

Vazamento de dados;
Recuperação indevida;
Danos reputacionais;
Sanções administrativas;
Infrações ambientais.

8.8.2 CONTROLES

Destruição prévia;
Cadeia de custódia;
Registro completo;
Auditorias;
Fornecedores homologados.

8.9 REGISTRO

8.9.1 FORMULÁRIO DE REGISTRO DE DESCARTE

Devem conter:

Descrição do material;
Classificação da informação;
Quantidade;
Setor solicitante;
Responsáveis;
Método de destruição;
Evidências;
Certificação (quando aplicável).

8.9.2 ARMAZENAMENTO DAS EVIDÊNCIAS

Evidências, registros e certificados devem ser armazenados por 5 anos.

8.10 PROIBIÇÕES

É proibido:

Descartar equipamentos sem destruir dados;
Doar equipamentos com armazenamento intacto;
Utilizar fornecedores não homologados;
Armazenar materiais em locais sem controle;
Transportar itens sensíveis sem lacre;
Permitir acesso de pessoas não autorizadas.

9. ORIENTAÇÕES GERAIS

9.1 IDENTIFICAÇÃO DO MATERIAL

Sempre verifique a classificação da informação (Público, Interno, Confidencial, Dados Pessoais, Dados Sensíveis). Caso haja dúvida sobre o nível de sensibilidade, considere o material como confidencial ou sensível até orientação formal pela chefia imediata e/ou protocolo institucional.

9.2 ARMAZENAMENTO TEMPORÁRIO

Mantenha documentos sensíveis em pastas, caixas ou envelopes fechados e **identificados como “material para descarte seguro”**.

Nunca deixe materiais com dados pessoais/sensíveis sobre mesas, lixeiras comuns ou ambientes de circulação.

9.3 TRANSPORTE INTERNO

Ao transportar documentos ou materiais até o ponto de coleta, utilize:

- Pastas ou caixas lacradas;
- Percursos diretos, sem deixar o material sem supervisão;
- Portas fechadas e acessos restritos, quando aplicável.

9.4 DESCARTE DE ITENS DE INFORMÁTICA

Equipamentos como HDs, CPUs, notebooks, mídias, toners e componentes eletrônicos devem ser enviados em caixa lacrada para a área responsável.

Não entregue equipamentos obsoletos a terceiros ou coloque em armazenamento não autorizado.

9.5 SIGILO DURANTE TODO O PROCESSO

Não fotografe, compartilhe ou comente sobre o conteúdo dos materiais descartados.

Se notar que alguém está manuseando ou armazenando de forma inadequada, oriente com cautela ou comunique o setor responsável.

9.6 REGISTRO E RASTREABILIDADE

Sempre siga os formulários, planilhas ou sistemas que registram o descarte.

Não descarte por conta própria se o procedimento prevê controle, recolhimento agendado ou destruição certificada.

9.7 CUMPRIMENTO DO PROTOCOLO INSTITUCIONAL

Para evitar desvios do protocolo:

Leia e siga rigorosamente as instruções internas.

Não realize etapas adicionais ou diferentes das orientadas.

Em caso de dúvida, procure o responsável pelo procedimento (ex.: DITI).

Lembre-se: a violação de procedimentos pode gerar riscos legais, operacionais e de segurança .

10. REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, 15 ago. 2018.

11. CONTROLE DE QUALIDADE

11.1 REVISÃO

Nº DA REVISÃO	DATA	ITEM	MOTIVO	VIGÊNCIA
-	26/01/2026	-	Elaboração	2 anos a partir da elaboração/revisão.

12. ELABORAÇÃO

UNIDADE	NOME
Divisão de Infraestrutura em Tecnologia da Informação	Adriano Gonçalves de Lima

13. CONFERÊNCIA

UNIDADE	NOME
Seção de Processos de Qualidade	Amanda Sabatine dos Santos
Coordenadoria de Tecnologia da Informação	Mariana Micena da Silva Tamborim

14. APROVAÇÃO

UNIDADE	NOME
Coordenadoria de Tecnologia da Informação	José Luís de Almeida



Documento assinado eletronicamente por **Amanda Sabatine Dos Santos, Chefe de Seção**, em 26/01/2026, às 08:42, conforme horário oficial de Brasília, com fundamento no [Decreto Estadual nº 67.641, de 10 de abril de 2023](#).



Documento assinado eletronicamente por **Mariana Micena Da Silva Tamborim, Assessor II**, em 26/01/2026, às 08:54, conforme horário oficial de Brasília, com fundamento no [Decreto Estadual nº 67.641, de 10 de abril de 2023](#).



Documento assinado eletronicamente por **José Luis De Almeida, Assessor IV**, em 26/01/2026, às 09:17, conforme horário oficial de Brasília, com fundamento no [Decreto Estadual nº 67.641, de 10 de abril de 2023](#).



A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0092221801** e o código CRC **DB812BBA**.