Universidade Federal do Triângulo Mineiro
Programa de Mestrado Profissional em Inovações e Tecnologias

Márcio Giordani Ribeiro da Silva Martins

DO *BACKUP* AO DESCARTE: BOAS PRÁTICAS NO MANUSEIO DE EQUIPAMENTOS INFORMÁTICOS EM CONFORMIDADE COM AS DIRETRIZES DA LEI GERAL DE PROTEÇÃO DE DADOS E DA POLÍTICA NACIONAL DE RESÍDUOS SÓLIDOS

Uberaba - MG
2025

Márcio Giordani Ribeiro da Silva Martins

DO *BACKUP* AO DESCARTE: BOAS PRÁTICAS NO MANUSEIO DE EQUIPAMENTOS INFORMÁTICOS EM CONFORMIDADE COM AS DIRETRIZES DA LEI GERAL DE PROTEÇÃO DE DADOS E DA POLÍTICA NACIONAL DE RESÍDUOS SÓLIDOS

Dissertação apresentada ao Programa de Mestrado Profissional em Inovações e Tecnologias da Universidade Federal do Triângulo Mineiro, como requisito parcial para a obtenção do título de Mestre.
Orientador: Prof. Dr. Geoffroy Roger Pointer Malpass
Coorientadora: Profa. Dra. Ana Claudia Granato Malpass

Uberaba - MG

2025

Catalogação na fonte: Biblioteca da Universidade Federal do Triângulo Mineiro

M344b

Martins, Márcio Giordani Ribeiro da Silva

Do *backup* ao descarte: boas práticas no manuseio de equipamentos informáticos em conformidade com as diretrizes da Lei Geral de Proteção de Dados e da Política Nacional de Resíduos Sólidos / Márcio Giordani Ribeiro da Silva Martins. -- 2025.

209 f. : il., graf., tab.

Dissertação (Mestrado Profissional em Inovação Tecnológica) -- Universidade Federal do Triângulo Mineiro, Uberaba, MG, 2025

Orientador: Prof. Dr. Geoffroy Roger Pointer Malpass

Coorientadora: Profa. Dra. Ana Claudia Granato Malpass

1. Tecnologia da informação. 2. Armazenamento de dados. 3. Proteção de dados - legislação. 4. Gestão integrada de resíduos sólidos. I. Malpass, Geoffroy Roger Pointer. II. Universidade Federal do Triângulo Mineiro. III. Título.

CDU 316.422.44

Mirtes Soares - Bibliotecária - CRB-6/2181

MÁRCIO GIORDANI RIBEIRO DA SILVA MARTINS

DO BACKUP AO DESCARTE: BOAS PRÁTICAS NO MANUSEIO DE EQUIPAMENTOS INFORMÁTICOS EM CONFORMIDADE COM AS DIRETRIZES DA LEI GERAL DE PROTEÇÃO DE DADOS E DA POLÍTICA NACIONAL DE RESÍDUOS SÓLIDOS

Dissertação apresentada ao Programa de Pós-graduação Profissional em Inovações e Tecnologias da Universidade Federal do Triângulo Mineiro como requisito parcial para obtenção do título de mestre.

Uberaba, 17 de novembro de 2025

Banca Examinadora:

Dr. Geoffroy Roger Pointer Malpass – Orientador
Universidade Federal do Triângulo Mineiro

Dra. Mariangela Torreglosa Ruiz Cintra
Universidade Federal do Triângulo Mineiro

Dr. Pedro Henrique Aparecido Damaso de Melo
Universidade Federal de Viçosa

Dedico este momento e todo meu esforço a Deus, primeiramente, pois ele foi minha fortaleza. A minha família, que são a razão da minha luta diária.

AGRADECIMENTOS

Agradeço, com apreço, ao Professor Doutor Geoffroy Roger Pointer Malpass, pela orientação atenta, pelo tempo dedicado às discussões e reflexões, e pela generosidade em compartilhar seus conhecimentos, que foram fundamentais para o desenvolvimento desta dissertação e para o meu crescimento acadêmico e profissional.

Ao Professor Dr. Fernando Mattioli, Analista de Sistemas, à Professora Doutora Magda Stella de Melo Martins, Gestão Ambiental, expresso meu reconhecimento pelas importantes contribuições técnicas, especialmente no aprimoramento dos fluxogramas, o que muito enriqueceu este trabalho.

Ao Advogado Matheus Pereira, inscrito na OAB sob n° 16886802, pelas valiosas sugestões e "consultas técnicas interpretativas", que contribuíram de forma significativa para o aprofundamento das análises jurídicas e para a correta interpretação das leis e normas.

À Professora Doutora Mariângela Torreglosa Ruiz Cintra, pelas profícuas contribuições na qualificação, em especial pela sugestão na elaboração de um artigo científico sobre o tema da pesquisa e pela indicação da aplicação do ciclo PDCA, que enriqueceram significativamente este trabalho.

Aos docentes e técnicos do Programa de Mestrado Profissional em Inovação e Tecnologias da UFTM, cujo apoio constante, dedicação e ensinamentos deixaram marcas valiosas ao longo dessa caminhada.

Aos membros da banca examinadora, pelas observações criteriosas e sugestões relevantes que colaboraram significativamente para o aperfeiçoamento desta pesquisa.

Aos colegas da Divisão de Microinformática da UFTM, meu muito obrigado pela parceria, incentivo e trocas que tornaram o percurso mais leve e enriquecedor.

À minha família, agradeço profundamente pelo amor, paciência e pela motivação contínua que me sustentaram em todos os momentos. Sem vocês, este percurso não teria sido possível.

À FAPEMIG e ao CNPq pelo apoio financeiro e institucional que possibilitaram a realização desta pesquisa.

Por fim, agradeço àqueles que contribuíram, direta ou indiretamente, para a realização deste trabalho, registro aqui minha sincera gratidão.

“Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, e que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, porque os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação”.

Singh, 2022, p.13

RESUMO

Este estudo interdisciplinar teve como objetivo analisar as melhores práticas para o manuseio seguro de ativos de Tecnologia da Informação (TI) que contenham dispositivos que armazenam dados, buscando responder à questão de quais práticas podem ser adotadas para garantir o descarte seguro de ativos contendo dados pessoais, em conformidade com a Lei Geral de Proteção de Dados (LGPD), a Política Nacional de Resíduos Sólidos (PNRS) e as normas da família *International Organization for Standardization* (ISO) 27000, promovendo tanto a segurança da informação, quanto a sustentabilidade ambiental. A pesquisa consistiu em revisão da literatura científica, abrangendo as publicações nas bases de dados do Portal de Periódicos da CAPES, Google Acadêmico e Minha Biblioteca, com foco em estudos recentes, que identificam boas práticas de descarte e sanitização de dados em equipamentos eletrônicos. A metodologia adotada foi descritiva, com revisão bibliográfica documental sobre legislações e normas aplicáveis, além de análise de procedimentos de sanitização e descarte de equipamentos que armazenam dados. Os estudos bibliográficos foram comparados com as diretrizes estabelecidas pela LGPD, pela PNRS e os dados coletados foram analisados qualitativamente por meio de análise documental, possibilitando uma interpretação aprofundada e a formulação de recomendações para aprimorar as práticas seguras de descarte desses ativos. Como resultado, foi elaborado um "Manual de Boas Práticas", em forma de *E-book*, de caráter orientativo, que visa aumentar a segurança no descarte de ativos de TI e promover a sustentabilidade. O trabalho destaca a interconexão entre segurança da informação e gestão de resíduos, oferecendo um olhar integrado sobre a conformidade legal e as melhores práticas para o manejo adequado desses ativos.

Palavras-chave: Tecnologia da informação; Armazenamento de dados; Proteção de dados – legislação; Gestão integrada de resíduos sólidos.

ABSTRACT

This interdisciplinary study aimed to analyze best practices for the secure handling of Information Technology (IT) assets containing data storage devices, seeking to answer the question of which practices can be adopted to ensure the safe disposal of assets containing personal data, in compliance with the General Data Protection Law (LGPD), the National Solid Waste Policy (PNRS), and the International Organization for Standardization (ISO) 27000 family of standards, promoting both information security and environmental sustainability. The research consisted of a review of the scientific literature, covering publications in the databases of the CAPES Journal Portal, Google Scholar, and my library, focusing on recent studies that identify best practices for data disposal and sanitization in electronic equipment. The adopted methodology was descriptive, with a bibliographic and documentary review of applicable legislation and standards, as well as an analysis of data sanitization and disposal procedures for data-storing equipment. The bibliographic studies were compared with the guidelines established by the LGPD, the PNRS, and the collected data were qualitatively analyzed through documentary analysis, enabling an in-depth interpretation and the formulation of recommendations to improve disposal practices for these assets. As a result, a Best Practices Manual was developed as a guiding document aimed at enhancing the security of IT asset disposal and promoting sustainability. The study highlights the interconnection between information security and waste management, offering an integrated perspective on legal compliance and best practices for the proper handling of these assets.

Keywords: Information technology; Data storage; Data protection – legislation; Integrated solid-waste management.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ADF	Atestado de Destinação Final
ANPD	Autoridade Nacional de Proteção de Dados
ANSI	*American National Standards Institute*
BDTD	Biblioteca Digital de Teses e Dissertações
BEA	*Bureau of Economic Analysis*
BMP	Banco Máximo de Pagamentos
BPMN	*Business Process Model and Notation*
CAFe	Comunidade Acadêmica Federada
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CCTs	Cláusulas Contratuais-Tipo
CD	*Compact Disc*
CF	Constituição Federal
CFD	Ciência Forense Digital
CDC	Código de Defesa do Consumidor
CIA	*Central Intelligence Agency*
COAF	Conselho de Controle de Atividades Financeiras
COPPA	*Children's Online Privacy Protection Act*
CP	Código Penal
CSI	Comitê de Segurança da Informação
CTF/APP	Cadastro Técnico Federal de Atividades Potencialmente Poluidoras e Utilizadoras de Recursos Ambientais
DAS	*Direct-Attached Storage*
DFRWS	*Digital Forensic Rearch Workshop*
DPO	*Data Protection Officer*
DVD	*Digital Versatile Disc*
DVR	*Digital Video Recorder*
EEE	Equipamentos Eletroeletrônicos
ESR	Escola Superior de Rede
EU	*European Union*
EUA	*Estados Unidos da América*

FDD	*Floppy Disk Drive*
FEIS/UNESP	*Faculdade de Engenharia de Ilha Solteira/ Universidade Estadual Paulista "Júlio de Mesquita Filho"*
GDPR	*General Data Protection Regulation*
GSI	Gestão de Segurança da Informação
HDD	*Hard Disk Drive*
IBM	*International Business Machines Corporation*
IDSC	*International Data Sanitization Consortium*
IEC	*International Electrotechnical Commission*
IoT	*Internet of Things*
ISA	*International Federation of the National Standardizing Associations*
ISCSI	*Internet Small Computer System Interface*
ISO	*International Organization for Standardization*
ISP	*Information Security Policies*
JNT	*Facit Business and Technology Journal*
LAI	Lei de Acesso à Informação
LAN	Local Area *Network*
LGPD	Lei Geral de Proteção de Dados
LUN	*Logical Unit Number*
MCTI	Ministério da Ciência, Tecnologia e Inovação
NAS	*Network Attached Storage*
NBR	Norma Brasileira
NSA	National Scurity Agency
OOCRP	*Organized Crime and Corruption Reporting Project*
PDCA	*Plan* (Planejar)*, Do* (Executar), *Check* (Verificar), *Act* (Agir*)*
PEVs	Pontos de Entrega Voluntária
PGRS	Plano de Gerenciamento de Resíduos Sólidos
PIMS	Privacy Information Management System
PIPEDA	*Personal Information Protection and Electronic Documents Act*
PMPIT	Programa de Mestrado Profissional em Inovação e Tecnologias
PNRS	Política Nacional de Resíduos Sólidos
PEVs	Pontos de Entrega Voluntária
RAM	*Random Access Memory*
RDBCI	Revista Digital de Biblioteconomia e Ciência da Informação

RCB	*Registered Certification Body*
REEE	Resíduos de Equipamentos Eletroeletrônicos
RILCO DS	*Revista de Desarrollo Sustentable, Negocios, Emprendimiento y Educación*
RNP	Rede Nacional de Pesquisa
ROM	Read-Only Memory
RPO	Recovery Point Objective
RSC	Revista de Sistemas e Computação
RTO	Recovery Time Objective
SAN	Storage Area Network
SD	Secure Digital Card
SGPI	Sistema de Gestão da Privacidade da Informação
SGSI	Sistema de Gestão de Segurança da Informação
SI	Segurança de Informação
SINIR	Sistema Nacional de Informações sobre a Gestão dos Resíduos Sólidos
SNIA	Storage Networking Industry Association
SSD	Solid State Drive
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia de Informação e Comunicação
UE	União Europeia
UFRGS	Universidade Federal do Rio Grande do Sul
UFTM	Universidade Federal do Triângulo Mineiro
UNIFAGOC	Centro Universitário Governador Ozanam Coelho
UNILA	Universidade Federal da Integração Latino-Americana
UNSCC	United Nations Standards Coordinating Committee
UNITAR	United Nations Institute for Training and Research
VLAN	Virtual Local Area Network

SUMÁRIO

1 INTRODUÇÃO

A presente dissertação, apresentada ao Programa de Mestrado Profissional em Inovação e Tecnologias (PMPIT) da Universidade Federal do Triângulo Mineiro (UFTM), constitui requisito parcial para a obtenção do título de Mestre em Inovação e Tecnologias e tem como objeto de estudo o descarte seguro e sustentável de ativos de Tecnologia da Informação (TI) que contenham dispositivos de armazenamento de dados.

A informação, como ativo de alto valor estratégico, consolidou-se como recurso essencial para indivíduos, instituições públicas e organizações privadas, especialmente no que tange à privacidade e à segurança de dados pessoais. Nesse contexto, a responsabilidade solidária entre empresas, órgãos públicos e consumidores no tratamento adequado dessas informações é cada vez mais necessária, sobretudo diante dos riscos associados ao descarte inadequado de equipamentos que armazenam dados sensíveis. Tal negligência pode acarretar exposições indevidas, comprometendo a integridade, a confidencialidade e a disponibilidade de informações pessoais ou corporativas, além de gerar implicações legais e danos à imagem institucional (Barreto *et al*., 2018).

Essa realidade tornou a Segurança da Informação (SI) uma preocupação de prioridade global, conforme demonstrado por casos de grande repercussão mundial, como o do ex-técnico da *Central Intelligence Agency* (CIA)[1], Edward Snowden[2], ocorrido em 2013 e, mais recentemente, o caso do militar Jack Teixeira[3], em 2023 (Gouveia, 2023). Ambos os episódios revelaram vulnerabilidades nos sistemas de segurança e as graves consequências que podem surgir para instituições e indivíduos.

No Brasil, o caso da atriz Carolina Dieckmann[4], que teve fotos íntimas expostas na internet após receber ameaças de extorsão, evidenciou a vulnerabilidade da segurança digital. Esse episódio resultou na criação da Lei n. 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos, alterando o Decreto-Lei n. 2.848, de 7 de

---

[1] *Central Intelligence Agency* (CIA) Agência de inteligência dos Estados Unidos, criada em 1947, responsável por coletar, analisar e disseminar informações sobre segurança nacional e realizar operações secretas no exterior.

[2] Edward Snowden revelou documentos confidenciais que expunham o funcionamento de programas de vigilância do governo dos Estados Unidos. As informações divulgadas mostraram que a espionagem atingia não apenas cidadãos norte-americanos, por meio do monitoramento de dados de grandes empresas de tecnologia como Google, Apple e Facebook, mas também diversos países, incluindo nações da Europa e da América Latina. Entre os alvos estava o Brasil, com registros de que até mesmo as comunicações da então presidenta Dilma Rousseff e de sua equipe mais próxima foram interceptadas.

[3] Jack Teixeira, 22 anos, membro da Guarda Nacional Aérea dos EUA, vazou documentos do Departamento de Justiça dos Estados Unidos, ultra secretos sobre a guerra na Ucrânia, em rede social.

[4] Carolina Dieckmann é uma atriz brasileira de televisão, cinema e teatro, nascida em 1978, conhecida por suas atuações em telenovelas da Rede Globo.

dezembro de 1940 — Código Penal[5] (CP) — , e dá outras providências, que ficou conhecida no país como "Lei Carolina Dieckmann", destinada a punir crimes cibernéticos (Ferreira; (Vilarinho, 2022).

Porém, mesmo após mais de uma década em vigor, sua eficácia ainda é questionada diante da frequência e gravidade dos ataques cibernéticos (Beserra; Santos; Amaral, 2020). Um exemplo recente ocorreu em 23 de julho de 2024, quando o grupo *hacker* denominado *Fog* realizou um ataque ao governo federal brasileiro[6] (Madureira; Goulart, 2024). O episódio não apenas evidenciou a sofisticação dos crimes virtuais, como também revelou a limitada capacidade da legislação penal brasileira aplicada aos crimes cibernéticos, diante da ousadia dos ofensores.

Diversos especialistas em segurança da informação classificaram, outro caso, como um dos mais graves já registrados no Brasil: o ataque cibernético ocorrido em junho de 2025, que comprometeu os sistemas de ao menos seis instituições financeiras. Segundo noticiado pelo portal G1, os invasores tiveram acesso ao ambiente da empresa C&M *Software* — responsável por interligar bancos e *fintechs*[7] ao sistema PIX[8] — por meio de credenciais privilegiadas de um colaborador, que teria fornecido suas senhas em troca de pagamento ilícito. A partir disso, os criminosos realizaram transferências em massa por meio de ordens falsas de PIX, desviando valores estimados em até R$ 800 milhões, sendo R$ 541 milhões apenas da instituição Banco Máximo de Pagamentos **(**BMP), em um intervalo de poucas horas (Helder; Bolzani, 2025). A vulnerabilidade demonstrada no caso, ilustra a necessidade de adoção de estratégias de segurança em profundidade, conforme preconizado pelas boas práticas da governança da informação e da cibersegurança.

---

[5] O Código Penal brasileiro, instituído pelo Decreto-Lei nº 2.848, de 7 de dezembro de 1940, estabelece as normas gerais sobre crimes, penas e medidas de segurança aplicáveis em todo o território nacional.

[6] O ataque afetou nove ministérios, além da Casa da Moeda e o Conselho de Controle de Atividades Financeiras (Coaf). Segundo investigações da Polícia Federal, envolveu o sequestro de 28 gigabytes de dados, posteriormente transferidos para servidores localizados nos Estados Unidos. Os responsáveis deixaram uma mensagem em um arquivo nomeado *ReadMe (leia-me)*, informando que os sistemas haviam sido invadidos e solicitando o início de uma negociação por meio da *dark web*, com promessa de devolução dos dados, exigiram um resgate de 1,2 milhões de dólares. Diante da complexidade do caso, considerado sensível e urgente, o Ministério da Justiça acionou autoridades norte-americanas e o Departamento de Justiça dos EUA, buscando cooperação internacional. Documentos trocados entre a Polícia Federal e órgãos dos Estados Unidos, acessados pela organização *Organized Crime and Corruption Reporting Project* (OCCRP), revelaram a dimensão do ocorrido e os esforços em curso para responsabilizar os autores e mitigar os danos causados ao Estado brasileiro (Madureira; Goulart, 2024).

[7] *Fintechs* é um termo em inglês originado da junção de *financial* (financeiro) e *technology* (tecnologia). Refere-se a empresas que aplicam recursos tecnológicos para inovar nos serviços e produtos financeiros, como pagamentos digitais, empréstimos *online*, investimentos, seguros e gestão financeira. Essas organizações se destacam pela agilidade, pelo uso de plataformas digitais e pela oferta de soluções mais acessíveis em comparação às instituições bancárias tradicionais.

[8] Sistema PIX - sistema de pagamentos instantâneos do Banco Central do Brasil, lançado em 2020, que permite transferências e pagamentos em tempo real, de forma rápida e segura.

Nesse cenário de fragilidades normativas e tecnológicas, pode-se avaliar que a exposição de dados não tem se limitado apenas a grandes sistemas governamentais ou corporativos, mas também afeta qualquer indivíduo, quando se trata da SI. Casos cotidianos de descuido com a segurança digital também representam riscos concretos. É nesse contexto que o estudo de Freitas (2019) ganha relevância ao analisar o descarte inadequado de 583 *Hard Disk Drive (HDDs)* adquiridos como sucata nos estados de Minas Gerais e São Paulo, tanto no comércio físico quanto eletrônico, ao longo de 2018. Os resultados revelaram que muitos continham informações intactas ou recuperáveis, independentemente do estado de funcionamento dos discos. Esse fato evidenciou um risco significativo de exposição de informações pessoais sensíveis[9], ressaltando a importância de práticas adequadas de sanitização[10] e descarte de dispositivos de armazenamento[11] de dados.

De maneira semelhante, Schneider *et al.* (2021), analisaram de forma forense[12], 614 *pen drives* adquiridos como novos e originais. Dentre os dispositivos analisados, 75 continham informações variadas, como fotos de pessoas nuas ou seminuas, imagens, gravações de voz, códigos-fontes e filmes completos. Os autores concluíram que a presença de dados nesses dispositivos, supostamente novos, indica que práticas de sanitização inadequadas de dispositivos de armazenamento de dados podem levar à exposição de informações sensíveis, comprometendo a privacidade e a segurança dos usuários.

Esses exemplos demonstram que tanto pessoas físicas quanto jurídicas, sejam públicas ou privadas, estão sujeitas a riscos associados ao descarte inadequado de dispositivos de armazenamento de dados. A ausência de procedimentos adequados de sanitização pode permitir a recuperação de informações, resultando na exposição indevida de dados sensíveis e aumentando a vulnerabilidade de indivíduos e organizações a fraudes, vazamentos e outras ameaças à SI (D'Angelo; Mota, 2024).

Neste contexto, este estudo analisou as melhores práticas para o descarte correto de equipamentos de TI que contenham dispositivos de armazenamento de dados, em conformidade com a Política Nacional de Resíduos Sólidos (PNRS), instituída pela Lei nº 12.305, de 2 de

---

[9] A Lei Geral de Proteção de Dados (LGPD) define dados pessoais sensíveis como quaisquer dados pessoais relativos à: origem racial ou étnica; crença religiosa; opinião política; sindicato; associação a organização religiosa, filosófica ou política; saúde ou vida sexual; dados genéricos ou biométricos.

[10] Sanitização: Refere-se ao processo de remoção de dados de mídias de armazenamento, de forma que haja garantia razoável de que os dados não possam ser facilmente recuperados e reconstruídos.

[11] Dispositivo de armazenamento é qualquer elemento de armazenamento ou agregação de elementos de armazenamento, projetado e construído principalmente para fins de armazenamento e entrega de dados.

[12] A investigação forense utiliza métodos científicos e tecnológicos para coletar, analisar e interpretar evidências, auxiliando na identificação de culpados e na resolução de crimes. Combinando conhecimentos jurídicos e técnicos, como análise de impressões digitais, recuperação de dados, análise de dispositivos eletrônicos, entre outros.

agosto de 2010; a Lei Geral de Proteção de Dados (LGPD), instituída pela Lei n. 13.709, de 14 de agosto de 2018; e as diretrizes da *International Organization for Standardization* (ISO) – Organização Internacional de Normalização. Como resultado, foi elaborado um "Manual de Boas Práticas", que reúne orientações, com a finalidade de aumentar a segurança no descarte de ativos de TI e, consequentemente, promover a sustentabilidade.

A PNRS tem o propósito de estabelecer a responsabilidade compartilhada pelo ciclo de vida dos produtos, promovendo a logística reversa[13] para a reintegração de resíduos ao ciclo produtivo ou sua destinação ambientalmente adequada. Além disso, incentiva práticas de redução, reutilização e reciclagem de materiais, contribuindo para a minimização dos impactos ambientais. Por fim, determina a disposição final adequada dos rejeitos, assegurando a proteção do meio ambiente e a sustentabilidade dos processos produtivos (Schaun *et al.*, 2023).

A LGPD, por sua vez, estabelece diretrizes para o tratamento de dados[14] pessoais, em meios digitais e físicos, abrangendo tanto indivíduos quanto organizações, sejam elas públicas ou privadas. O seu propósito é regulamentar o uso de dados pessoais, garantindo a proteção dos direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade da pessoa natural ou jurídica[15] (Teixeira; Guerreiro, 2022).

Neste sentido, Sá (2019) explica que a LGPD representa uma mudança significativa na forma como as empresas gerenciam dados pessoais, exigindo uma abordagem mais rigorosa e transparente na administração dessas informações, tanto em ambientes *online* quanto *offline*, resguardando os direitos fundamentais à liberdade e à privacidade, em qualquer cenário de interação que envolva seu tratamento.

A família de normas ISO/IEC 27000 foi desenvolvida conjuntamente pela ISO e pela *International Electrotechnical Commission* (IEC) – Comissão Eletrotécnica Internacional. Ela estabelece diretrizes e princípios fundamentais para a implementação, manutenção e aprimoramento contínuo de um Sistema de Gestão da Segurança da Informação (SGSI) e é aplicável a organizações de diferentes segmentos e portes (Magalhães, 2021). O seu propósito,

---

[13] Logística reversa: instrumento de desenvolvimento econômico e social caracterizado por um conjunto de ações, procedimentos e meios destinados a viabilizar a coleta e a restituição dos resíduos sólidos ao setor empresarial, para reaproveitamento, em seu ciclo ou em outros ciclos produtivos, ou outra destinação final ambientalmente adequada.

[14] Tratamento de Dados é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[15] Pessoa Natural é o termo técnico usado na CF de 1988, no Código Civil e na LGPD, para designar o indivíduo considerado como sujeito de direitos e deveres. Enquanto a pessoa jurídica refere-se às entidades, instituições ou organizações formadas por um grupo de pessoas com finalidade comum, reconhecidas legalmente como sujeito de direitos.

conforme Diniz e Diniz (2021) é garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações, promovendo a proteção de dados e a mitigação de riscos relacionados à SI.

De acordo com a Escola Superior de Rede (2025)[16], a confidencialidade garante que apenas indivíduos autorizados tenham acesso às informações, prevenindo acessos indevidos. A integridade preserva a exatidão das informações, evitando alterações não autorizadas ou acidentais. Por sua vez, a disponibilidade garante que os dados estejam acessíveis sempre que necessários, mantendo a continuidade dos serviços. Por fim, a autenticidade permite assegurar a veracidade das informações, possibilitando a confirmação da identidade da pessoa ou entidade responsável por fornecê-las.

À medida que a PNRS orienta a gestão adequada dos resíduos sólidos e a promoção da reciclagem (Brasil, 2010), a LGPD foca na proteção e privacidade dos dados pessoais (Brasil, 2018). Diante dessa premissa, Diniz e Diniz (2021) elucidam que as normas regulatórias da família ISO/IEC 27000 oferecem uma estrutura para a gestão da segurança da informação complementando essas legislações ao proporcionarem diretrizes para a proteção, coleta, utilização, disseminação e descarte de informações. Giovanini (2021) esclarece que a família ISO/IEC foca na gestão da segurança da informação, enquanto a LGPD foca na gestão e tratamento de dados pessoais. Essas regulamentações e normas, apesar de focadas em áreas específicas, estão interligadas, especialmente no contexto do descarte correto de ativos que armazenam dados pessoais. Portanto, a compreensão e a aplicação dessas diretrizes são essenciais para garantir que as práticas de descarte sejam seguras e alinhadas com os padrões legais e normativos, promovendo a SI e a sustentabilidade ambiental.

Com a implementação da LGPD, conforme mencionado por Silva e Novais (2023), as organizações e indivíduos devem seguir regras rigorosas para proteger dados pessoais e evitar vazamentos que podem ter graves consequências jurídicas e sociais. Ferrari (2021) aponta a complexidade e a importância do descarte correto do lixo, especialmente em relação a dados pessoais e informações sigilosas. O autor enfatiza que mesmo que o lixo seja considerado abandonado e sua posse se torne lícita para quem o encontre, os dados pessoais contidos nele não podem ser tratados legalmente sem o devido respaldo legal.

Portanto, conforme enfatizado pela ESR (2025), a SI atua criando barreiras para impedir acessos não autorizados aos dados, enquanto que a proteção dos dados visa garantir que essas

[16] A Escola Superior de Rede (ESR) é coordenada pela Rede Nacional de Pesquisa (RNP), uma organização vinculada ao Ministério da Ciência, Tecnologia e Inovação. A RNP é responsável pela infraestrutura de internet acadêmica, além de atuar na capacitação e inovação tecnológica.

informações sejam utilizadas de forma adequada. Além disso, a privacidade proporciona que indivíduos e organizações mantenham o controle sobre as informações pessoais e de terceiros, garantindo um tratamento ético e seguro.

1.1 JUSTIFICATIVA

Com o avanço tecnológico e a crescente digitalização das atividades sociais e econômicas, têm-se gerado um volume expressivo de dados pessoais armazenados em dispositivos eletrônicos. Paralelamente, também há uma preocupação cada vez maior com a forma como esses dados são protegidos, bem como ocorre o descarte dos equipamentos e ativos de TI, como HDs, SSDs, celulares e *pen drives*. Quando não há uma política de manuseio e descarte desses dispositivos, há um potencial risco de vazamento de informações sensíveis (Barreto *et al.*, 2018) — situação que compromete direitos fundamentais, como a privacidade e a segurança do cidadão (Alencar, 2023).

Essa preocupação é respaldada por legislações como a LGPD, que estabelece diretrizes para o tratamento adequado de dados pessoais no Brasil (Brasil, 2018). A Autoridade Nacional de Proteção de Dados (ANPD, 2024), criada pela LGPD (Brasil, 2018), reforça a importância de que as instituições adotem medidas administrativas e técnicas para garantir a integridade, confidencialidade e disponibilidade das informações, inclusive nos processos de descarte.

Além do aspecto jurídico, o problema também se estende à dimensão ambiental. A PNRS, prevê diretrizes para a gestão adequada de resíduos eletrônicos e impõe responsabilidades aos geradores de lixo tecnológico quanto à destinação final desses materiais (Brasil, 2010). Portanto, o desafio contemporâneo está na integração entre a SI, a conformidade legal e a sustentabilidade ambiental.

Estudos como o de Freitas (2019) revelam que muitos dispositivos de armazenamento, mesmo após serem descartados, continuam contendo dados recuperáveis. Essa realidade demonstra uma falha crítica nas práticas de descarte e evidencia a necessidade urgente de políticas claras de sanitização. Conforme apontado por Diniz e Diniz (2021), a gestão da segurança da informação deve estar alinhada com normas internacionais, como a Família ISO/IEC 27000, que oferece diretrizes para o ciclo de vida completo das informações, incluindo o descarte.

Além disso, os procedimentos de *backup* — essencial para garantir a continuidade do negócio e a preservação de dados — ainda apresenta falhas em sua execução, como evidenciado por Amancio *et al.* (2024), que apontam a necessidade de conferência na realização de cópias

de segurança em ambientes institucionais. Tal negligência compromete não apenas a recuperação da informação, mas também a confiabilidade dos processos de descarte, uma vez que dados mal gerenciados podem permanecer em equipamentos inutilizados.

No contexto brasileiro, o Decreto n. 10.240, de 12 de fevereiro de 2020, criado para regulamentar o inciso VI do *caput* do art. 33 e do art. 56 da lei da PNRS e complementar o Decreto n. 9.177, de 23 de outubro de 2017, quanto à implementação de sistema de logística reversa de produtos eletroeletrônicos e seus componentes de uso doméstico, reforça a necessidade de um controle rigoroso sobre o ciclo de vida dos dados e impõe obrigações às instituições públicas no tocante à governança da informação (Brasil, 2020). Mesmo assim, muitas empresas ainda não dispõem de diretrizes para lidar com as informações de seus clientes e fornecedores, o que pode gerar situações de vazamentos de dados e acesso não autorizado (Miragem, 2019).

Sob o ponto de vista legal, o incidente pode ser interpretado à luz da LGPD, que impõe às organizações o dever de adotar medidas de segurança aptas a proteger os dados pessoais contra acessos não autorizados e incidentes de segurança. Nesse sentido, falhas como a ocorrida na C&M *Software*, por exemplo, evidenciam não apenas riscos operacionais, mas também potenciais responsabilidades jurídicas e regulatórias, sujeitando a empresa a sanções administrativas pela ANPD e a possíveis demandas judiciais.

Esses cenários levantam a necessidade de investigar quais práticas podem ser consideradas eficazes para garantir a gerência segura de equipamentos eletroeletrônicos (EEE) que armazenam dados, em conformidade com as normas legais e técnicas vigentes. Respondendo à pergunta norteadora: quais são as boas práticas no manuseio, sanitização e descarte de EEE que garantem a proteção de dados pessoais em conformidade com a LGPD e a PNRS?

Diante disso, a pesquisa foi projetada com o intuito de contribuir com a estruturação de um modelo prático de descarte de TI. Parte-se da premissa de que a adoção de boas práticas, baseadas na legislação brasileira e nas normas internacionais de segurança da informação, pode minimizar significativamente os riscos de vazamento de dados e os impactos ambientais decorrentes do descarte inadequado, considerando as exigências legais da LGPD, os princípios da PNRS e as boas práticas internacionais de segurança da informação. O objetivo é desenvolver um manual que possa servir como referência para organizações públicas e privadas, unindo conformidade legal, mitigação de riscos e responsabilidade socioambiental — elementos que, cada vez mais, se mostram interdependentes no cenário da governança de dados.

A relevância deste estudo fundamentou-se na necessidade de assegurar que o descarte de ativos que armazenam dados pessoais seja realizado de forma ambientalmente responsável, ao mesmo tempo em que diminui os riscos de vazamento de informações e assegura a proteção desses dados. Perante da crescente preocupação com a proteção de dados e a destinação adequada de resíduos tecnológicos, esta pesquisa supriu uma lacuna prática ao investigar os procedimentos para o manuseio correto de ativos que armazenam dados, abrangendo todas as etapas, desde a coleta das informações até o descarte final dos ativos.

Nesse sentido, a relevância social do estudo se manifesta na contribuição para a preservação do direito à privacidade e à proteção dos dados pessoais — princípios garantidos pela Constituição Federal (CF) e reforçados pela LGPD. Ao propor práticas seguras e sustentáveis para o descarte de dispositivos de armazenamento, o trabalho colabora com a construção de uma cultura de responsabilidade informacional e ambiental, impactando diretamente a segurança dos cidadãos e a integridade das organizações.

Do ponto de vista acadêmico, a pesquisa avança no debate interdisciplinar entre as áreas de Direito, Segurança da Informação e Gestão Ambiental, articulando, portanto, com marcos legais brasileiros — a LGPD e a PNRS —, além de dialogar com normas internacionais — Família ISO/IEC 27000. Com isso, oferece base teórica e aplicada para novos estudos e iniciativas institucionais, contribuindo com a formação de profissionais capacitados a lidar com os desafios contemporâneos da proteção de dados em contextos tecnicamente complexos e socialmente sensíveis.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Identificar e analisar as melhores práticas legais, ambientais e técnicas para o descarte seguro e sustentável de ativos de armazenamento de dados, visando subsidiar a elaboração de um manual de boas práticas orientado à prevenção de vazamentos de dados e à conformidade com a LGPD, a PNRS e as normas da família ISO/IEC 27000.

1.2.2 Objetivos específicos

a) analisar criticamente as legislações e normas nacionais e internacionais aplicáveis à gestão da segurança da informação, correlacionando-as às práticas de governança,

proteção de dados e descarte seguro de ativos contendo informações pessoais e corporativas;

b) mapear, identificar e classificar os riscos de vazamento de dados ao longo de todo o ciclo de vida dos ativos de armazenamento;
c) modelar fluxogramas estruturados e padronizados dos processos de armazenamento, backup, sanitização, descarte e do ciclo de melhoria contínua, alinhando-os às diretrizes da LGPD, PNRS e normas ISO da família 27000.
d) desenvolver um manual de boas práticas, composto por fluxogramas orientativos, com foco na prevenção de vazamentos de dados e na sustentabilidade ambiental.

Esta dissertação de Mestrado Profissional buscou explorar os métodos e práticas recomendadas para o correto descarte de equipamentos que contenham dispositivos de armazenamento de dados em conformidade com as diretrizes da LGPD e PNRS, visando contribuir para a SI a sustentabilidade ambiental.

1.3 ESTRUTURA DA DISSERTAÇÃO

A presente dissertação está organizada em cinco seções, contando com esta Introdução, na qual são apresentados o tema da pesquisa, sua relevância e contextualização, seguidos pela definição dos objetivos gerais e específicos que orientam o desenvolvimento do estudo. A seção proporciona ao leitor uma visão geral das demais seções da dissertação e estabelece o escopo da investigação. Nessa etapa, são explicitados os objetivos que a pesquisa pretende atender, especialmente os relacionados à análise das leis LGPD e PNRS e das normas da família ISO/IEC 27000, bem como o desenvolvimento de um manual de boas práticas voltado à gestão de dados sensíveis.

A seção Referencial Teórico aborda os fundamentos que sustentam a pesquisa e está diretamente relacionada à análise dos dispositivos de armazenamento de dados, gestão de armazenamento e backups, legislação aplicável, políticas internacionais de segurança de dados e à Política Nacional de Resíduos Sólidos. Também contempla a família de normas ISO/IEC 27000, destacando suas principais normas, além de temas como computação forense, técnicas de sanitização em dispositivos de armazenamento de dados e a aplicação do ciclo PDCA no sistema de gestão de segurança da informação. Dessa forma, atende aos objetivos de analisar as leis de proteção de dados pessoais, políticas de descarte de resíduos sólidos, normas ISO/IEC 27000 e investigar técnicas de backup, sanitização e descarte em dispositivos de armazenamento de dados.

A seção Metodologia da Pesquisa detalha a abordagem adotada, enfatizando seu caráter interdisciplinar, a natureza aplicada, o tipo de pesquisa e as estratégias de coleta de dados. Esta seção descreve o levantamento bibliográfico, a pesquisa documental e a elaboração do produto técnico, no caso, o manual de boas práticas desenvolvido ao longo do estudo. Dessa forma, contribui diretamente para o objetivo de desenvolver um manual composto por fluxogramas orientativos, voltado a organizações que lidam com dados sensíveis, com foco na prevenção de vazamentos de dados e na sustentabilidade dos processos de descarte de ativos de armazenamento de dados.

Na seção Resultados e Discussão, são apresentados os resultados obtidos, incluindo a interlocução com especialistas e a validação técnica dos fluxogramas elaborados. Essa seção detalha os procedimentos específicos relacionados ao armazenamento de dados, backups, sanitização, descarte de ativos contendo dados e a aplicação do PDCA na gestão de ativos de informação, permitindo uma análise crítica e integrada dos processos investigados. Assim, contribui para atender aos objetivos de investigar técnicas de backup, sanitização e descarte, além de consolidar a aplicação prática das normas legais, ambientais e técnicas estudadas.

Por fim, a seção Considerações Finais sintetiza os principais achados da pesquisa, destacando suas contribuições, limitações e sugestões para investigações futuras, reafirmando a relevância do manual de boas práticas desenvolvido e o atendimento aos objetivos propostos em relação à segurança da informação, conformidade legal e sustentabilidade ambiental.

Em apêndice está o Manual de Boas Práticas, resultado final da dissertação, no qual são apresentados fluxogramas orientativos voltados a organizações que lidam com dados sensíveis. O manual detalha procedimentos para armazenamento, backup, sanitização e descarte de ativos contendo dados, integrando aspectos legais, como a LGPD, ambientais, conforme a PNRS, e técnicos, baseados nas normas da família ISO/IEC 27000. Esse material foi desenvolvido com base nos resultados da pesquisa, incluindo levantamento bibliográfico, análise documental e interlocução com especialistas, com o objetivo de oferecer diretrizes práticas que promovam a segurança da informação e a sustentabilidade nos processos de gestão de ativos de dados.

2 REFERENCIAL TEÓRICO

O manejo adequado dos Resíduos Eletroeletrônicos (REEE) é de extrema importância, uma vez que o descarte incorreto desses equipamentos pode causar sérios prejuízos à saúde pública e ao meio ambiente, principalmente pelo consumismo pós revolução industrial, ao avanço tecnológico e à produção em massa de EEE, que intensificou o descarte de REEE (Mota *et al*., 2016). Os autores ainda ressaltam a insuficiência de campanhas realizadas pelo poder público sobre o descarte adequado de eletrônicos, o que faz com que muitos sejam eliminados junto ao lixo comum. De forma complementar, Xavier *et al*. (2025) destacam os riscos ambientais decorrentes dos metais pesados, como cromo, cádmio, mercúrio, ouro, prata e platina, presentes nos REEE, os quais exigem atenção especial da sociedade quanto ao descarte adequado.

Paralelamente, Leme e Black (2020) asseveram que a crescente preocupação com a privacidade e a segurança de dados reforça a necessidade de práticas seguras para assegurar a proteção de informações pessoais sensíveis e a conformidade com a LGPD, o que envolve processos que vão desde a coleta, classificação, arquivamento e avaliação até a eliminação dos dados, de modo a resguardar os usuários contra o uso indevido, abusivo ou discriminatório de suas informações.

De acordo com Carvalho (2021) a LGPD constitui um instrumento legal essencial para garantir que os dados pessoais sejam tratados de maneira segura e responsável durante todo o seu ciclo de vida, incluindo a etapa do descarte dos equipamentos. A legislação exige que as organizações adotem medidas eficazes para proteger os dados pessoais contra acesso não autorizado, vazamentos e violações de privacidade, abrangendo, inclusive, o processo de eliminação de equipamentos que armazenam essas informações. O descumprimento dessas diretrizes, conforme abordado por Rodrigues (2024), pode resultar em sanções e danos à reputação da organização.

Além disso, as empresas têm a responsabilidade de seguir as normas legais relativas à gestão de resíduos eletrônicos, implementando práticas que garantam a rastreabilidade e o descarte apropriado desses materiais. Segundo a norma ISO/IEC 27040, a rastreabilidade dos equipamentos contendo dados é essencial para prevenir acessos não autorizados, devendo conter toda a movimentação destes equipamentos ao longo do seu ciclo de vida. Também é papel das organizações colaborarem com órgãos públicos na conscientização da população sobre a importância do descarte correto dos resíduos eletrônicos. Esse esforço educativo é

fundamental para assegurar que a gestão desses resíduos, seja conduzida de forma eficiente e ambientalmente correta (Jucon, s.d.).

As boas práticas no descarte de REEE[17] são fundamentais tanto para a proteção ambiental quanto para a SI. Xavier *et al*. (2025) ressaltam a importância de uma abordagem integrada, que envolva sustentabilidade e proteção dos dados contidos nos dispositivos, como a eliminação das informações antes do descarte. Entre essas práticas, destaca-se a reciclagem, essencial para reduzir impactos ambientais e recuperar materiais valiosos. Marques (2017) aponta que resíduos eletrônicos coletados em pontos específicos podem ser transformados em novos produtos, reintegrando-se ao ciclo produtivo como matéria-prima.

O gerenciamento correto de REEE constitui medida essencial não apenas para garantir a sustentabilidade ambiental, mas também para assegurar a proteção dos dados. Sobre isso, Mota *et al*. (2016) enfatizam que muitas empresas negligenciam essa etapa, deixando esses equipamentos expostos a riscos de segurança mesmo após o término de sua vida útil.

Portanto, é imprescindível reforçar a importância do descarte seguro de dispositivos que armazenam dados, uma vez que a simples exclusão dos arquivos não é suficiente para impedir o acesso indevido a informações pessoais ou empresariais (Malik, 2023). Nesse sentido, o gerenciamento correto de REEE, conforme a PNRS e a LGPD, é prioritário não apenas para assegurar a proteção dos dados, mas também para promover a sustentabilidade. Desta forma, práticas como a realização de *backups*, a sanitização de mídias e a destinação adequada de ativos contendo dados são fundamentais para garantir a segurança digital e ambiental no descarte desses dispositivos.

2.1 DISPOSITIVOS DE ARMAZENAMENTO DE DADOS

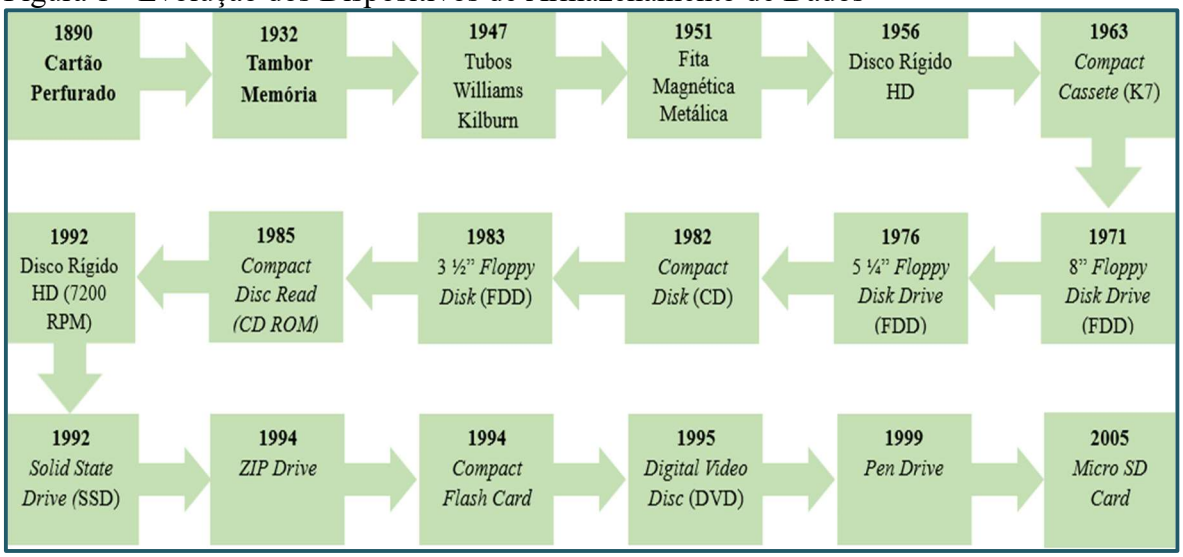
O universo da pesquisa é amplo, no caso da pesquisa científica, por exemplo, ela representa um processo sistemático voltado à produção de conhecimento novo e útil para a compreensão da realidade (Gil, 2022). Neste contexto, a busca contínua por conhecimento impulsionou o desenvolvimento de estratégias e instrumentos capazes de registrar, organizar e transmitir informações. Assim, surgiram e foram aperfeiçoados diversos dispositivos de armazenamento de dados, como resposta às crescentes demandas por segurança, eficiência e capacidade na preservação e circulação da informação (Costa; Pinto, 2017).

[17] Boas práticas no descarte de REEE são procedimentos que garantem o descarte seguro e ambientalmente responsável de equipamentos eletrônicos, incluindo reciclagem de materiais, destruição segura de dados e conformidade com normas ambientais e de proteção de informações.

Diante desse cenário, os autores classificam os dispositivos de armazenamento de dados em três categoria: o armazenamento magnético, presentes nos *Hard Disk Drive (HDD), Floppy Disk Drive (FDD)* e fitas magnéticas; o armazenamento óptico, utilizados em CDs e DVDs e o armazenamento realizados por semicondutores, encontrados em dispositivos como nos *Solid State Drives* (SSDs), pendrives e *Secure Digital Card (SD).*

A Figura 1 ilustra a evolução das tecnologias dos dispositivos de armazenamento de dados, destacando o surgimento e o aperfeiçoamento dos dispositivos magnéticos, ópticos e semicondutores.

Figura 1 - Evolução dos Dispositivos de Armazenamento de Dados



Fonte: elaboração própria, 2025 adaptada de Costa e Pinto, 2017.

Essas tecnologias representaram avanços importantes na evolução dos meios de armazenamento de dados, contribuindo para o desenvolvimento das soluções atuais. Os disquetes, por exemplo, possibilitaram a transferência física de dados em uma era anterior à popularização dos CDs e DVDs. As fitas magnéticas, por sua vez, consolidaram-se como uma opção utilizada para *backup,* em razão de seu baixo custo e elevada capacidade de armazenamento (Costa; Pinto 2017).

Posteriormente, surgiram os *HDDs* de alta velocidade, que devido à sua estrutura mecânica, apresentam maior vulnerabilidade a danos físicos e podem possuir velocidades de acesso inferiores em comparação com tecnologias mais recentes, como os SSDs que são dispositivos eletrônicos sem partes móveis, formados por semicondutores (*chips*) que apresentam diversas vantagens, como menor consumo de energia, maior resistência a impactos físicos, maior velocidade de acesso e um tamanho reduzido quando comparados aos HDDs tradicionais (Costa; Pinto 2017).

Enquanto os HDDs são ideais para armazenamento de grandes volumes de dados a baixo custo, os SSDs oferecem vantagens em termos de desempenho. A escolha entre essas opções deve considerar fatores como velocidade necessária, capacidade de armazenamento e orçamento disponível (Pedrozo, 2019).

Além dos aspectos estruturais e funcionais mencionados, é importante considerar que os dispositivos de armazenamento, como os HDDs, SSDs, pertencem ao grupo das memórias não voláteis. Esses dispositivos mantêm os dados armazenados mesmo na ausência de energia elétrica, o que os torna ideais para a preservação permanente de informações, diferenciando-se da *Read-Only Memory* (ROM), que é outro tipo de memória não volátil utilizada principalmente para *firmware* e instruções de inicialização (Lenovo, 2025).

Por outro lado, existem as memórias voláteis, como a *Random Access Memory* (RAM), que segundo a Lenovo (2025), são utilizadas para armazenar dados e instruções de forma temporária com o objetivo de permitir que o processador acesse rapidamente as informações necessárias durante a execução das tarefas. No entanto, seu conteúdo é apagado sempre que o equipamento é desligado.

2.2 GESTÃO DE ARMAZENAMENTO E *BACKUPS*

A realização de *backups* é uma prática essencial na proteção de dados, pois permite a recuperação de informações em casos de falhas operacionais ou incidentes diversos. Segundo Amancio *et al.,* (2024), *backup* é o processo que consiste na duplicação e armazenamento de dados com a finalidade de prevenir a perda da informação em diversas situações como falhas de sistema, corrupção de arquivos, exclusão acidental, alterações indevidas e ataques de *softwares* maliciosos, permitindo a criação de uma cópia fiel dos arquivos.

A norma ISO/IEC 27040 orienta que essas cópias devem ser armazenadas em locais seguros, com acesso restrito e protegidas contra danos físicos e lógicos, além de discos e locais redundantes, possibilitando a sua recuperação em caso de necessidade.

Neste contexto, Gillis e Castagna (2024) destacam a existência de um procedimento conhecido como a regra de *backup* 3-2-1, que visa garantir a integridade e a disponibilidade das informações. Esse procedimento visa a criação de três cópias de dados, armazenadas em pelo menos dois tipos distintos de mídias, sendo que uma dessas cópias deve ser mantida em um local externo ao ambiente principal, mitigando riscos associados a pontos únicos de falha.

Neste mesmo sentido, o Art. 46 da LGPD determina que os agentes de tratamento adotem medidas técnicas[18] e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, bem como situações acidentais ou ilícitas de destruição, perda e alteração (Marinho; Paranaguá; Piva, 2024). Desta forma, a norma ISO/IEC 27002 destaca que a realização e testes periódicos de *backups* são práticas fundamentais que asseguram a continuidade das operações e a preservação dos dados em caso de falhas ou incidentes. Além disso, a norma ISO/IEC 27040:2015 recomenda que as organizações estabeleçam normas procedimentais específicas para a gestão dos processos de armazenamento e *backup*.

Para garantir a segurança das informações, conforme abordado na ISO/IEC 27002 é essencial implementar controles de autenticação, autorização e criptografia. A autenticação deve ser aplicada para identificar o usuário ou dispositivo antes de permitir o acesso. A autorização deve ser configurada para definir quais dados e operações cada usuário poderá acessar, aplicando sempre o princípio do menor privilégio[19]. Além disso, a criptografia[20] deve ser utilizada para proteger os dados sensíveis e sigilosos, garantindo que apenas quem possui a chave correta consiga ler as informações.

De acordo com Tanaka e Gomes (2019), podem ser classificados em três categorias principais: completo, incremental e diferencial. O *backup* completo consiste na cópia integral de todos os dados do sistema, garantindo uma réplica exata das informações armazenadas. O *backup* incremental, por sua vez, registra exclusivamente os dados alterados desde a última cópia completa, reduzindo o volume de armazenamento necessário e otimizando o tempo de execução do procedimento. Já o *backup* diferencial preserva as modificações realizadas desde o último *backup* completo ou incremental, possibilitando uma recuperação mais ágil em comparação ao modelo incremental, embora demande maior espaço de armazenamento.

Um fator determinante para a proteção das informações, tanto em ambientes corporativos quanto residenciais, é a arquitetura de armazenamento de dados. De acordo com

---

[18] Medidas técnicas referem-se a recursos e procedimentos tecnológicos utilizados para proteger os dados pessoais contra acessos não autorizados, alterações indevidas, vazamentos e perdas. Exemplos incluem o uso de criptografia, controle de acesso por senhas, sistemas de autenticação, *firewalls*, antivírus, *backup* seguro e monitoramento de rede. Essas medidas devem ser compatíveis com o grau de sensibilidade das informações e com os riscos envolvidos no tratamento dos dados, conforme previsto no art. 46 da LGPD, Lei n.º 13.709/2018 (Brasil, 2018).

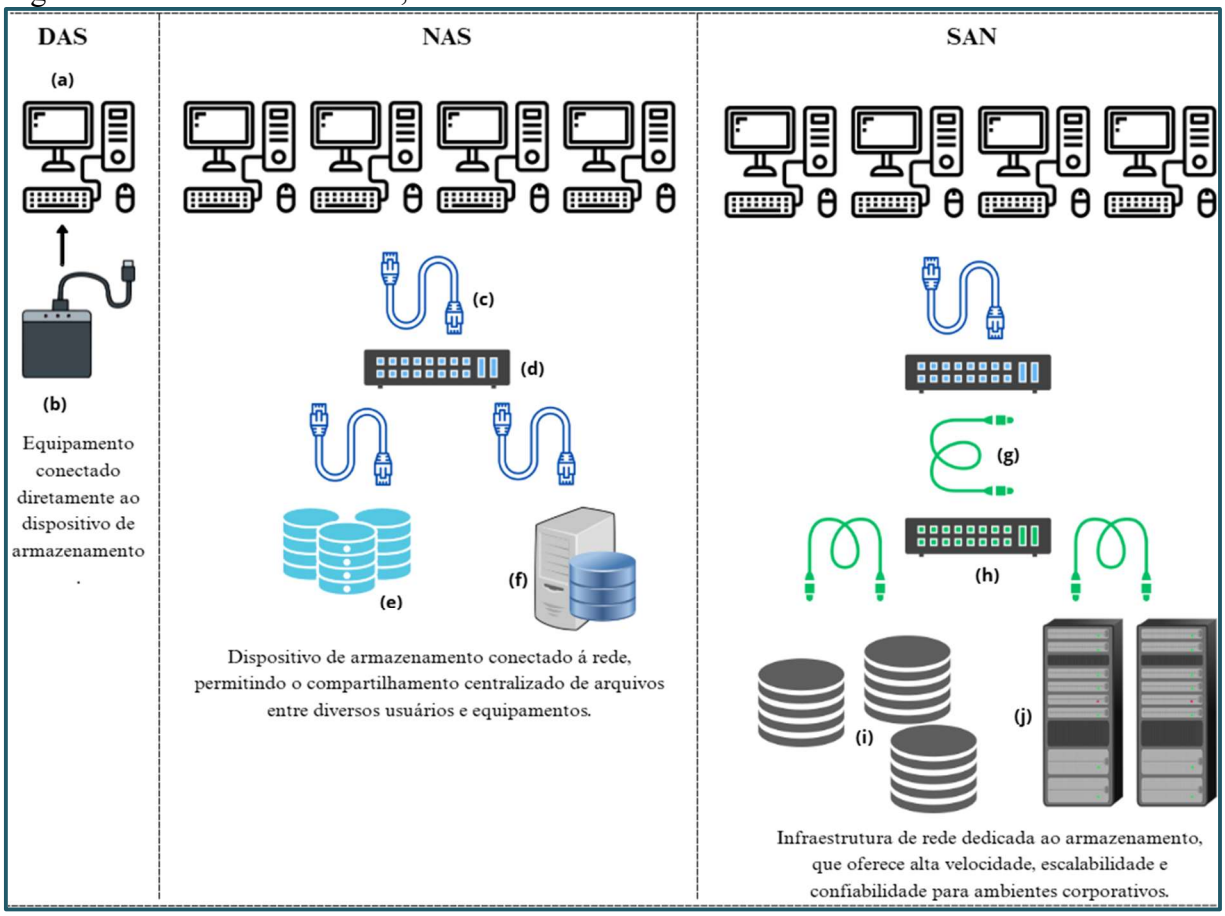
[19] Privilégio ou permissões determinam direitos de acessos específicos, como se um usuário pode ler, gravar ou executar um objeto (ISO/IEC 27002)

[20] Criptografia é uma técnica de segurança da informação que utiliza algoritmos para codificar dados, tornando seu conteúdo inacessível a pessoas não autorizadas. Apenas aqueles que possuem a chave de decodificação apropriada conseguem acessar a informação original. É amplamente utilizada para proteger dados em repouso (armazenados) ou em trânsito (transmitidos), sendo um dos principais mecanismos recomendados por normas como a ISO/IEC 27002 para assegurar a confidencialidade, integridade e autenticidade das informações.

Susnjara e Smalley (2024) os dados podem ser estruturados por duas formas principais: por meio de conexão direta (*Direct-Attached Storage* – DAS) ou através da conexão em rede, que inclui soluções como o *Network Attached Storage* (NAS) e *o Storage Area Network* (SAN).

Essas modalidades de armazenamento estão representadas na Figura 2, que ilustra os elementos principais e a interação entre usuários, dispositivos de armazenamento e infraestrutura de rede em cada modelo. Essa forma esquemática evidencia como o armazenamento direto é conectado localmente aos usuários, enquanto os modelos em rede (NAS e SAN) dependem de dispositivos de comunicação específicos para o acesso seguro e eficiente aos dados, apresentadas de forma esquemática.

Figura 2 - Demonstrativo DAS, NAS e SAN



Fonte: elaboração própria, 2025 com base na ISO/IEC 27040:2015.

Para facilitar a compreensão da imagem esquemática, o Quadro 1, apresenta uma Legenda Técnica dos Componentes DAS, NAS e SAN, no qual se descreve tecnicamente cada componente identificado, relacionando-o com boas práticas e recomendações normativas, especialmente a ISO/IEC 27040:2015, voltada para segurança da informação em ambientes de armazenamento.

Quadro 1 - Legenda Técnica dos Componentes DAS, NAS e SAN

Elemento	Legenda Técnica
(a)	Estações ou servidores clientes – acessam diretamente os dados em dispositivos conectados fisicamente ao computador, sem intermediação de rede (Susnjara; Smalley, 2024). No modelo DAS, a ISO/IEC 27040:2015 destaca a necessidade de controles de acesso físico e sanitização de mídias, pois a perda ou roubo do equipamento pode comprometer a confidencialidade das informações.
(b)	Dispositivo de armazenamento - unidade de armazenamento interno ou externo (Susnjara; Smalley, 2024). A segurança envolve proteção contra manipulação não autorizada, uso de criptografia e descarte adequado, conforme recomenda a ISO/IEC 27040:2015.
(c)	Cabos de Rede - conexões físicas (Ethernet ou similares) que permitem a comunicação entre os usuários e equipamentos (Amaral, 2012). A norma ISO/IEC 27040:2015 sugere o uso de canais criptografados e segmentação da rede para reduzir riscos de interceptação de tráfego e acesso não autorizado.
(d)	Switch[21] NAS - dispositivo de rede que gerencia a comunicação entre múltiplos clientes e equipamentos como computadores, impressoras, IoT, dispositivos de armazenamento, sistemas de segurança (Amaral, 2012). Esse componente deve ser configurado com monitoramento de tráfego, prevenindo ataques internos e externos (ISO/IEC 27040:2015).
(e)	Armazenamento em rede (NAS) - unidades de disco configuradas para compartilhamento de arquivos entre usuários e dispositivos (Susnjara; Smalley, 2024). A norma ISO/IEC 27040:2015 orienta aplicar controles de acesso e monitoramento para evitar uso indevido das informações.
(f)	Servidor dedicado (NAS) - responsável por gerenciar o serviço de armazenamento em rede, garantindo que apenas usuários autorizados tenham acesso aos arquivos (ISO/IEC 27040:2015).
(g)	Cabos de rede SAN – conexões especializadas (ex: Fibre Channel, Internet Small Computer System Interface (iSCSI) que compõem a infraestrutura física de uma SAN, interligando servidores e dispositivos de armazenamento de forma dedicada e alta performance (Amaral, 2012).
(h)	Switch SAN - equipamento de comutação especializado, que gerencia o tráfego em alta velocidade entre servidores e dispositivos de armazenamento em SAN (ISO/IEC 27040:2015, Susnjara; Smalley (2024).
(i)	Arrays de discos – sistemas de armazenamento conectados à SAN, que podem ser integrados aos servidores através de virtualização ou mapeamento de volumes (ISO/IEC 27040:2015).
(j)	Servidores corporativos - acessam volumes de armazenamento através da SAN, com alta performance, confiabilidade e escalabilidade, conforme orientado para ambientes corporativos na ISO/IEC 27040:2015.

Fonte: elaboração própria, 2025.

O DAS refere-se a um sistema de armazenamento de dados conectado diretamente a um único servidor ou estação de trabalho, sem intermediação de rede, sendo o acesso restrito ao equipamento ao qual está conectado. Sua principal característica é a simplicidade estrutural,

[21] *Switch* é um dispositivo de rede que conecta múltiplos equipamentos dentro de uma rede local (LAN), permitindo o envio eficiente de dados apenas para o dispositivo de destino. Os switches podem ser não gerenciáveis, com configuração simples, ou gerenciáveis, com controle avançado de tráfego.

na qual o dispositivo de armazenamento está fisicamente ligado ao computador por meio de interfaces. Essa modalidade caracteriza-se por baixo custo de aquisição e simplicidade de implementação, mas possui alto desempenho, configurando-se como alternativa adequada para ambientes residenciais e empresas de pequeno porte (Susnjara; Smalley, 2024). Contudo, conforme mencionado pela ISO/IEC 27040:2015, apresenta limitações relevantes, pois falhas físicas podem comprometer a integridade e a disponibilidade das informações. Além disso, a ausência de mecanismos centralizados de gerenciamento e segurança pode comprometer a proteção das informações, sobretudo em organizações que lidam com dados sensíveis.

O NAS, por sua vez, refere-se a uma solução de armazenamento de dados conectados à rede e acessíveis simultaneamente por múltiplos usuários. Essa solução é amplamente empregada em compartilhamento de arquivos e realização de backup, permitindo que dados sejam compartilhados de forma padronizada e organizada, ampliando a colaboração entre usuários em diferentes dispositivos (Susnjara; Smalley, 2024). A característica multiusuária demanda e permite a implementação de mecanismos robustos de segurança, tais como autenticação eficaz, segregação de rede, criptografia, controles de *logging* e auditorias, de modo a assegurar o rastreamento adequado dos acessos (ISO/IEC 27040:2015). Trata-se, assim, de uma solução eficiente e viável economicamente para pequenas e médias empresas (Susnjara; Smalley, 2024).

Já o SAN, conforme destacado pela ISO/IEC 27040:2015, destina-se a ambientes corporativos (data centers, instituições financeiras, organizações de saúde e empresas que necessitam de infraestrutura crítica de TI) que exigem elevado desempenho, disponibilidade e escalabilidade no tratamento dos dados, tornando-se um pilar essencial para estratégias de continuidade de negócios, recuperação de desastres e ataques cibernéticos. Apesar de suas vantagens, apresenta custos de implantação e manutenção elevados, necessitando de profissionais altamente especializados e políticas de segurança robustas, o que limita sua adoção a organizações que dispõem de maior capacidade de investimento (Susnjara; Smalley, 2024).

Ademais, conforme recomenda a ISO/IEC 27040:2015, soluções de armazenamento como o DAS, NAS e SAN devem ser acompanhadas por controles de segurança que assegurem a confidencialidade, integridade e disponibilidade das informações, prevenindo vulnerabilidades decorrentes de acessos não autorizados e falhas na infraestrutura. Nesse mesmo sentido, a LGPD estabelece a necessidade de adoção de medidas técnicas e administrativas capazes de proteger os dados pessoais contra acessos indevidos, perdas ou

vazamentos, reforçando responsabilidades quanto ao tratamento seguro das informações (Brasil, 2018).

Para melhor compreensão das características, vantagens e limitações de cada modalidade o Quadro 2 sintetiza os principais critérios comparativos entre DAS, NAS e SAN, com destaque para aspectos de custo, desempenho, escalabilidade, complexidade, compartilhamento e segurança.

Quadro 2 - Comparativo entre DAS, NAS e SAN

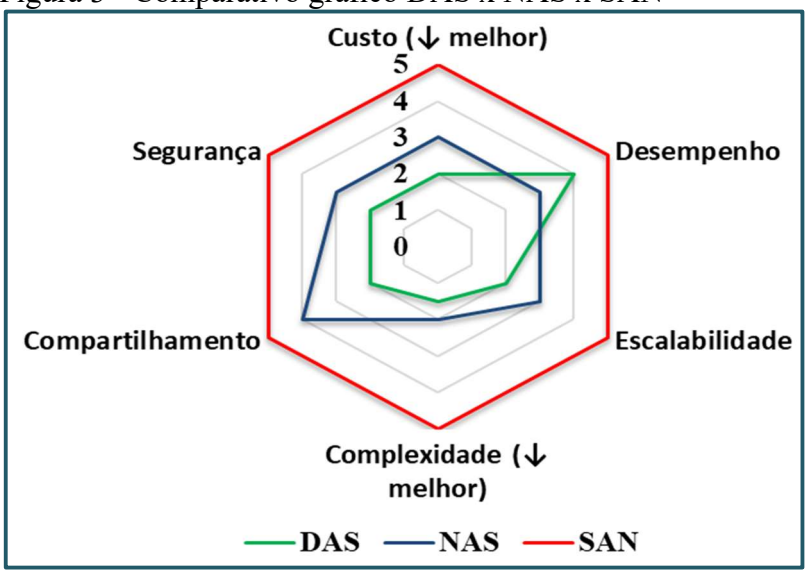
Critério	DAS	NAS	SAN
Custo	Baixo custo de aquisição e manutenção, adequado para residências e pequenas empresas.	Custo intermediário, acessível para pequenas e médias empresas.	Custo elevado de implantação e manutenção.
Desempenho	Limitado, dependente do equipamento ao qual está conectado.	Bom desempenho para acesso multiusuário e *backups.*	Alto desempenho, indicado para aplicações críticas e processamento intensivo.
Escalabilidade	Baixa escalabilidade, limitado ao dispositivo conectado.	Escalável, podendo ser expandido conforme a demanda.	Altamente escalável, suportando grandes volumes de dados e múltiplos servidores.
Complexidade	Baixa complexidade de instalação e uso.	Complexidade intermediária, exige configuração de rede e segurança.	Alta complexidade de gestão e manutenção, requer equipe especializada.
Compartilhamento	Não permite compartilhamento nativo, acesso restrito ao equipamento local.	Suporte multiusuário, compartilhamento eficiente via rede.	Compartilhamento avançado entre servidores e *storages*, com alta disponibilidade.
Segurança (ISO/IEC 27040:2015).	Vulnerável a falhas físicas e acessos não autorizados.	Requer autenticação, segregação de rede, criptografia e auditoria para garantir segurança.	Necessita de controles robustos de proteção, com foco em confidencialidade, integridade e disponibilidade.

Fonte: elaboração própria, 2025 adaptado de Gillis; Castagna, 2024; Susnjara; Smalley, 2024.

Sob uma perspectiva crítica, observa-se que, conforme o gráfico da Figura 3, a escolha entre DAS, NAS e SAN não deve ser pautada apenas em custos ou desempenho, mas também nos riscos associados à segurança da informação e à conformidade. No quesito custo, o DAS representa a alternativa mais acessível e de fácil adoção, ainda que apresente limitações evidentes. O NAS configura uma opção intermediária, equilibrando gastos com maior flexibilidade de uso, ao passo que o SAN, devido à sua robustez e desempenho superior, implica

em investimentos significativamente mais elevados, viabilizando-se sobretudo em ambientes corporativos de grande porte.

Figura 3 - Comparativo gráfico DAS x NAS x SAN



Fonte: elaboração própria, 2025.

No que se refere ao desempenho, o DAS tende a atender pequenas demandas locais, mas demonstra restrições em cenários de múltiplos acessos simultâneos. O NAS proporciona maior eficiência em ambientes colaborativos, enquanto o SAN é adequado a aplicações críticas que exigem alta disponibilidade. Quanto à escalabilidade, o DAS revela-se limitado, exigindo substituições físicas quando ocorre crescimento expressivo do volume de dados. O NAS oferece flexibilidade moderada, mas é o SAN que apresenta maior capacidade de expansão, mantendo a consistência operacional em grandes volumes de informação.

Sob a ótica da complexidade, o DAS é de fácil implementação e administração, o que pode ser visto como vantagem em cenários menos exigentes. O NAS, por depender de integração em rede, demanda maior conhecimento técnico e monitoramento contínuo. Já o SAN é a solução mais complexa, exigindo governança sólida, equipes capacitadas e processos estruturados de gestão, em conformidade com práticas recomendadas pela ISO/IEC 27001:2024.

No critério compartilhamento, o DAS mostra-se restritivo, limitado ao dispositivo ou servidor conectado, enquanto o NAS favorece a colaboração por permitir acesso simultâneo a múltiplos usuários, ampliando a eficiência em redes corporativas. O SAN, ainda que menos intuitivo que o NAS, também possibilita compartilhamento seguro e organizado, especialmente em ambientes de missão crítica.

Por fim, a dimensão da segurança se revela crucial. O DAS, apesar da simplicidade, é vulnerável a falhas físicas e carece de mecanismos de rastreabilidade[22], contrariando as recomendações da ISO/IEC 27040:2015, que estabelece diretrizes de proteção para ambientes de armazenamento. O NAS, por estar conectado em rede, expande a superfície de ataque e exige controles rigorosos de autenticação, criptografia e auditoria, de modo a cumprir os requisitos da LGPD no que se refere à confidencialidade e ao tratamento responsável de dados (Brasil, 2018). Já o SAN, embora disponha de recursos avançados, demanda administração especializada para assegurar que tais mecanismos sejam eficazes e que a infraestrutura atenda tanto às exigências técnicas quanto às obrigações legais.

Assim, a definição da solução mais adequada deve considerar, de forma integrada, os seis critérios analisados – custo, desempenho, escalabilidade, complexidade, compartilhamento e segurança – ponderando não apenas os aspectos tecnológicos, mas também o alinhamento às normas internacionais de segurança da informação, às legislações vigentes e à realidade orçamentária de cada organização.

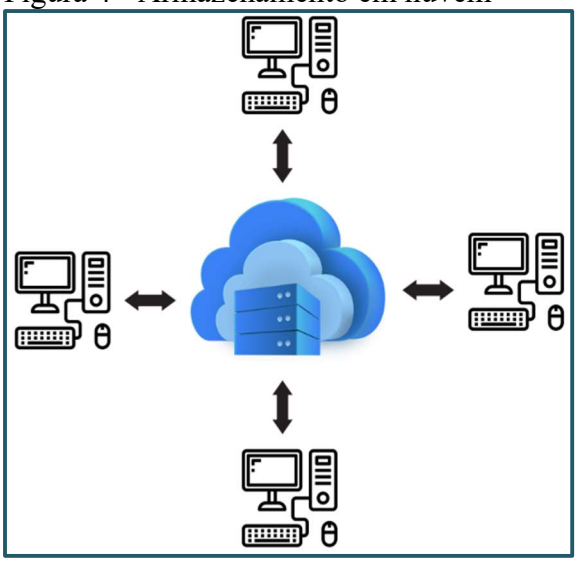
As soluções de armazenamento DAS, NAS e SAN apresentam vantagens e limitações específicas que devem ser ponderadas conforme o contexto de uso. Como evolução do processo de armazenamento, a computação em nuvem surge como uma alternativa diferenciada, destacando-se pela escalabilidade, flexibilidade e redução de custos operacionais, onde o cliente paga pela utilização efetiva, conforme a demanda, “substituindo a dependência de infraestruturas físicas locais por recursos virtualizados” (Paula; Roland, 2024).

Com o aumento constante na geração de dados e a necessidade de acesso ágil e seguro às informações, o armazenamento de dados passou a ser fundamental tanto para indivíduos quanto para organizações. Nesse contexto, a computação em nuvem surge como uma alternativa eficaz, oferecendo não apenas escalabilidade e flexibilidade, mas também a possibilidade de redução de custos operacionais. Considera-se que o armazenamento em nuvem proporciona a solução mais acessível e adaptável, desde que observadas as normas de segurança estabelecidas pela plataforma utilizada. Esse modelo tem se difundido amplamente devido à sua praticidade, permitindo o acesso a grandes volumes de dados a partir de múltiplos dispositivos e oferecendo maior versatilidade ao usuário, além de incorporar recursos de segurança robustos, como criptografia de dados, que asseguram a proteção das informações sensíveis (Freitas, 2025).

[22] Entre os mecanismos de rastreabilidade recomendados pela ISO/IEC 27040 para ambientes de armazenamento de dados, destacam-se: registro detalhado de logs de acesso e operações, identificação única de dispositivos e volumes, utilização de sistema de auditoria e monitoramento contínuo e controle de alterações em dados e configurações. Esses mecanismos permitem acompanhar a movimentação de informações, detectar falhas ou acessos não autorizados e garantir a integridade e a segurança dos dados armazenados.

Na Figura 4, ilustra-se o modelo conceitual do armazenamento em nuvem, no qual diversos dispositivos estão conectados a um servidor central baseado em nuvem. Freitas, 2025 destaca que essa arquitetura permite que os usuários armazenem, compartilhem e acessem dados de forma remota, independentemente da localização física, desde que haja conexão com a internet.

Figura 4 - Armazenamento em nuvem



Fonte: elaboração própria, 2025.

A representação evidencia o princípio de centralização do armazenamento em nuvem, onde a nuvem funciona como repositório principal, garantindo escalabilidade e segurança, enquanto os dispositivos atuam apenas como pontos de acesso. Essa estrutura facilita a colaboração e a mobilidade, características essenciais para ambientes corporativos e pessoais.

Entre as principais plataformas que oferecem esse serviço, destacam-se *Dropbox, Google Drive e OneDrive,* que se consolidaram como referências no mercado por atender diferentes perfis de usuários e oferecerem planos diversificados, desde versões gratuitas com espaço limitado até pacotes corporativos robustos (Freitas, 2025).

O Quadro 3 apresenta uma síntese das características centrais dessas plataformas, incluindo informações sobre os tipos de planos disponíveis e as principais características oferecidas e observações relevantes quanto ao seu uso e alcance. Esse comparativo permite visualizar as especificidades de cada serviço e auxilia na compreensão das vantagens e limitações de cada solução, servindo como subsídio para a escolha mais adequada ao contexto de cada usuário ou organização.

Quadro 3 - Principais plataformas de armazenamento nas nuvens

Plataforma/ referência	Plano gratuito ou pago	Principais Características
Dropbox	Gratuito: armazenamento limitado (2 GB). Planos pagos/ mais recursos e espaço (*Dropbox Plus, Family*, *professional* e *Business*).	1. Armazena e compartilha nas nuvens; 2. Sincronização automática entre dispositivos; 3. Acesso via *app* ou navegador; 4. Compatível com Windows, *macOS, Linux, iOS e Android*; 5. Suporte à colaboração em tempo real
Google Drive	Gratuito com 15 GB compartilhados (Drive, Gmail e Fotos); planos pagos via Google One.	1. Armazenamento e compartilhamento em nuvem; 2. Criação, edição e colaboração em Docs, Sheets, Slides e Forms; 3. Integração com Google Workspace; 4. Acesso via app ou navegador; 5. Histórico de versões; 6. Organização por pastas com controle de acesso; 7. Compatível com Windows, macOS, Android e iOS; sincronização automática.
One Drive	Plano gratuito: 5 GB. Plano pago: 1 TB (via assinatura do Microsoft 365)	1. Armazenamento em nuvem integrado ao Office; 2. Criação e edição de arquivos Word, Excel e PowerPoint; 3. Sincronização entre dispositivos.

Fonte: elaboração própria, 2025 adaptada de Paschoal; Paschoal e Abreu, 2021.

De acordo com Sousa e Gonçalves (2020), esse modelo de armazenamento em nuvem permite a preservação de dados pessoais e corporativos de forma prática e econômica. Entre suas principais funcionalidades estão a sincronização automática de dados[23], que permite o acesso a informações em tempo real a partir de diversos equipamentos, proporcionando acessibilidade e a possibilidade de trabalhos colaborativos, nos quais múltiplos usuários podem editar e compartilhar documentos simultaneamente, independentemente de sua localização geográfica. Os autores destacam, ainda, que o armazenamento na nuvem está em expansão, consolidando-se como uma tecnologia moderna baseada em servidores remotos[24] acessíveis via internet.

Enfim, pode-se destacar que os dispositivos de *backup*, conforme ressaltado por Lemos (2023), frequentemente apresentam vulnerabilidades críticas, como configurações de rede inseguras e permissões de acesso inadequadas, tornando-os alvos privilegiados para ataques

[23] A sincronização automática de dados é um processo pelo qual informações armazenadas em diferentes dispositivos, sistemas ou locais são atualizadas de forma contínua, garantindo que todos os pontos possuam a mesma versão dos dados. Quando ocorre uma alteração em um arquivo, o sistema propaga automaticamente essa mudança para os demais dispositivos conectados, sem necessidade de intervenção manual. Esse mecanismo é amplamente utilizado em serviços de nuvem, backup online, aplicativos de colaboração e sistemas corporativos, permitindo consistência, disponibilidade e acesso em tempo real às informações.

[24] Servidores remotos acessíveis via internet são computadores ou sistemas de armazenamento localizados em um data center ou outro local remoto, que podem ser acessados por usuários ou aplicativos por meio de redes públicas, como a internet. Esses servidores permitem armazenar, processar e gerenciar dados sem a necessidade de recursos locais, possibilitando o acesso a informações de qualquer lugar e a qualquer momento, desde que haja conexão à rede. Essa configuração é amplamente utilizada em serviços de nuvem, hospedagem de sites, aplicativos corporativos e plataformas de colaboração online.

cibernéticos, especialmente *ransomware*[25], que é, segundo Pinheiro *et al*., (2020), um tipo de *malware* que bloqueia o acesso aos dados ou ao sistema exigindo um resgate para sua liberação.

2.3 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Diante dos inúmeros desafios que a sociedade contemporânea tem enfrentado em decorrência da era digital, a proteção de dados pessoais emergiu como um dos temas centrais, tanto no campo tecnológico, quanto jurídico (Sá, 2019). O crescente uso da internet, aliado ao volume expressivo de informações trafegadas diariamente, tornou urgente a criação de normas voltadas à segurança da informação e à preservação da privacidade (Schwaitzer, 2020). Esse debate, intensificado nas últimas décadas, resultou em diversas legislações brasileiras que antecederam a promulgação da LGPD, contribuindo para consolidar a preocupação com o uso ético e seguro dos dados no ambiente virtual (Beserra; Santos; Amaral, 2020).

A LGPD foi inspirada no *General Data Protection Regulation* (GDPR) — o Regulamento Geral sobre a Proteção de Dados da União Europeia (Sá, 2019) — e estruturada com base em sessenta e cinco (65) artigos, que juntos asseguram a proteção dos dados pessoais e da privacidade dos cidadãos, alinhando-se às melhores práticas globais (Teixeira; Guerreiro, 2022). Tendo forte inspiração na GDPR, a lei "traz, como grande diferencial para a sociedade brasileira, a garantia de que o indivíduo possui direito sobre seus dados e que aquele que efetua o tratamento de dados possui uma série de obrigações para com o seu titular" (Schwaitzer, 2020, p. 40).

No contexto brasileiro, a construção normativa que culminou na LGPD teve início com a promulgação da Lei de Acesso à Informação (LAI), Lei nº 12.527, de 18 de novembro de 2011, que faz a distinção entre os dados pessoais e os dados comuns, estabelecendo orientações quanto ao seu tratamento (Bartolomeo, 2021). Essa legislação, conforme Sá (2019), regulamenta o direito constitucional de acesso a informações públicas, previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da CF. A LAI promove a transparência da administração pública, permitindo que cidadãos acessem dados sobre o uso de recursos governamentais, salvo quando classificados como sigilosos, sendo, portanto, uma base inicial relevante para as discussões posteriores sobre proteção de dados no país (Weber; Schmidt, 2023).

---

[25] *Ransomware* é um tipo de *software* malicioso que infecta sistemas de computador, criptografa dados e torna-os inacessíveis até que a vítima pague um resgate ao atacante. Esse tipo de ataque representa um risco significativo à segurança da informação, podendo comprometer a confidencialidade, integridade e disponibilidade dos dados pessoais e corporativos.

Em um segundo momento, à medida que cresciam os riscos de violação de dados no ambiente digital[26], tornou-se necessário um instrumento legal voltado à segurança dos dispositivos informáticos e à privacidade individual (Bartolomeo, 2021). Nesse cenário, foi sancionada a lei n. 12.737, de 30 de novembro de 2012, que ficou popularmente conhecida como "Lei Carolina Dieckmann", representando um avanço ao criminalizar a invasão de EEE – como computadores e smartphones — e a obtenção indevida de dados pessoais sem o consentimento do titular (Ferreira; Vilarinho, 2022).

Com o avanço das tecnologias digitais e o uso crescente da internet em diferentes esferas da vida social, surgiu a necessidade de uma legislação mais ampla e estruturada, que normatizasse o uso da rede no país (Bartolomeo, 2021). Para este fim foi sancionada a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. A referida lei passou a ser chamada de "Marco Civil da Internet", pois foi à primeira lei "a regulamentar o uso da internet no Brasil, o qual objetiva estabelecer princípios, garantias, direitos e deveres para quem utiliza a rede, além de orientar a atuação do Estado nesse contexto" (Cardoso; Régis, 2024, p. 4). Portanto, o Marco Civil da Internet definiu direitos e deveres relacionados à privacidade e proteção de dados no ambiente digital, além de garantir a neutralidade da rede[27].

No entanto, para melhor regulamentar a proteção de dados pessoais e a privacidade no Brasil, foi sancionada a LGPD que somente entrou em vigor em agosto de 2020 (Teixeira; Guerreiro, 2022). A LGPD, portanto, trata-se de uma lei federal de caráter obrigatório para todas as instituições, independentemente de seu porte ou setor (Giovanini, 2021).

Considerando a expansão das tecnologias digitais e o aumento das ameaças cibernéticas[28], o ordenamento jurídico brasileiro tem se adaptado para enfrentar esses desafios. A Lei nº 14.155/2021, sancionada em 27 de maio de 2021[29], alterou o código Penal brasileiro para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato

---

[26] Violação de dados no ambiente digital ocorre quando informações confidenciais ou sensíveis são acessadas, copiadas, alteradas ou divulgadas sem autorização, comprometendo a privacidade, a segurança e a integridade dos dados. Exemplos incluem o roubo de dados de clientes em uma base de e-commerce, o acesso não autorizado a registros médicos eletrônicos, o vazamento de senhas e credenciais em serviços online, e ataques cibernéticos como *ransomware,* que criptografa dados de uma organização e exige resgate para a liberação. Tais incidentes podem gerar prejuízos financeiros, danos à reputação e implicações legais para indivíduos e empresas.

[27] A neutralidade da rede é o princípio que garante que todos os dados na internet sejam tratados de forma igual, sem discriminação ou prioridade, independentemente do conteúdo, origem ou destino.

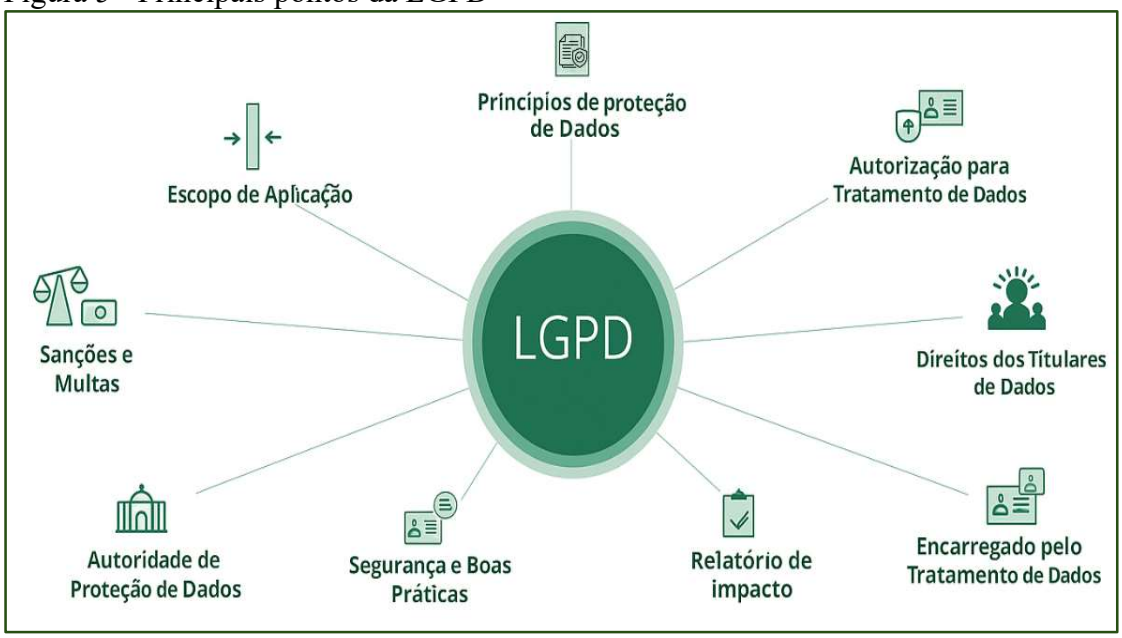
[28] Ameaças cibernéticas como: *phishing, malware, ransomware*, ataques de negação de serviço (DDoS) e acesso não autorizado a sistemas, entre outras.

[29] A Lei n. 14.155/2021 promoveu alterações pontuais no Código Penal, visando, entre outros aspectos, atualizar dispositivos relacionados à segurança pública, às medidas penais e à tipificação de condutas criminosas, adequando a legislação às demandas sociais contemporâneas e decisões do Poder Judiciário.

cometidos de forma eletrônica ou pela *internet,* reforçando o combate aos crimes cibernéticos no país (Marques, 2024).

A LGPD, na sua composição legal, estabelece que todo tratamento de dados pessoais "[...] deve ser efetuado com observância da boa-fé e de dez princípios nela elencados: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas [...]" (Schwaitzer, 2020, p. 42). Esses princípios constituem a base normativa da lei e orientam sua aplicação prática. Neste sentido, Sá (2019) destaca que a LGPD é um marco regulatório fundamental para a governança de dados no Brasil e explica em nove pontos que classifica como principais, que são destacados na Figura 5.

Figura 5 - Principais pontos da LGPD



Fonte: elaboração própria, 2025 adaptada de Sá, 2019.

Sá (2019) explica detalhadamente esses nove pontos previstos na LGPD, e reforça que cada um deles está diretamente relacionado aos dispositivos específicos da legislação. A partir dessa descrição, elaborou-se a seguinte síntese dos 9 pontos, com o objetivo de sistematizar os fundamentos centrais da norma.

1. Princípios de Proteção de Dados, previstos no Art. 6º, orientam todo o tratamento de dados pessoais, estabelecendo diretrizes como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, segurança, transparência, prevenção e responsabilização.

2. Autorização de tratamento de dados, conforme o Art. 7º, refere-se às bases legais que legitimam tal prática, incluindo o consentimento do titular, o cumprimento de obrigações legais, a execução de políticas públicas, entre outras hipóteses legítimas.

3.Direitos dos Titulares de Dados, elencados no Art. 18, asseguram aos cidadãos o controle sobre suas informações pessoais, garantindo, por exemplo, os direitos de acesso, retificação, portabilidade e exclusão dos dados.

4. Encarregado pelo Tratamento de Dados (*Data Protection Officer* – DPO), definido no Art. 5º, inciso VIII, e detalhada no Art. 41. Esse profissional é responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional.

5. Relatório de Impacto à Proteção de Dados Pessoais, exigido pelo Art. 38, é um instrumento fundamental nas operações de tratamento que possam representar riscos à privacidade, devendo conter informações sobre o tipo de dados tratados, a finalidade do tratamento e as medidas de segurança adotadas.

6. Segurança e Boas Práticas, os artigos 46 a 49 estabelecem a necessidade de adoção de medidas técnicas e administrativas que assegurem a proteção contra acessos não autorizados, vazamentos, destruição ou qualquer outro tipo de tratamento inadequado ou ilícito.

7. A Autoridade Nacional de Proteção de Dados (ANPD), criada pelos artigos 55-A a 55-K, é o órgão responsável por implementar e fiscalizar o cumprimento da LGPD, além de regulamentar e orientar sua aplicação, bem como aplicar sanções quando necessário.

8. Sanções e Multas, previstas no Art. 52, incluem desde advertências e multas simples ou diárias, até a suspensão ou proibição total do tratamento de dados pessoais.

9. Escopo de Aplicação da LGPD, conforme estabelecido no Art. 3º, é bastante amplo: aplica-se a qualquer operação de tratamento realizada por pessoa natural ou jurídica, de direito público ou privado, independentemente do meio, da sede ou do local onde os dados estejam armazenados, desde que a operação envolva dados de indivíduos localizados no Brasil ou tenha por objetivo a oferta de bens e serviços ao mercado nacional.

No entanto, mesmo com todos estes pontos positivos, a própria LGPD, como muitas legislações brasileiras, enfrenta desafios em sua aplicação. Segundo Galvão *et al.* (2024), mesmo após a promulgação da Lei n. 13.709/2018, os vazamentos de dados pessoais seguem sendo recorrentes, trazendo não apenas prejuízos financeiros, mas também impactos emocionais e financeiros aos indivíduos afetados. A principal causa apontada pelos autores para

essa permanência dos incidentes está na dificuldade de adesão por parte das organizações, muitas vezes inviabilizada pelos altos custos de implementação das medidas exigidas pela legislação. Essa resistência estrutural, como destaca o estudo, compromete o tratamento adequado das informações pessoais, que muitas vezes são coletadas em contextos cotidianos — como cadastros em *sites* de compras e navegação em plataformas digitais — e armazenadas sem os devidos mecanismos de segurança.

Galvão *et al.* (2024) reforçam que, embora a LGPD determine a responsabilidade solidária entre controladores e operadores no tratamento dos dados, conforme previsto no artigo 5º, inciso IX da lei, a ausência de investimentos em inovação tecnológica ainda compromete a efetividade da proteção de dados. Esta realidade evidencia que, além da base normativa construída ao longo da última década, é necessário promover uma cultura de segurança da informação que vá além do mero cumprimento formal das obrigações legais, tornando-se parte da ética organizacional e das práticas cotidianas no trato com os dados pessoais.

A aplicação da LGPD, segundo Vasconcelos (2020), não se restringe aos profissionais das áreas jurídica ou tecnológica, pois o tratamento de dados pessoais está presente em diversos setores da sociedade como: a saúde, a educação, o comércio, os serviços financeiros, o marketing, o setor público e até mesmo organizações do terceiro setor. Portanto, tais informações são amplamente utilizadas por entidades públicas e privadas com finalidades que vão desde o desenvolvimento de políticas públicas até a definição de estratégias de mercado e a análise comportamental dos consumidores.

Muncinelli *et al.* (2020) explicam que a LGPD estabelece normas para o tratamento de dados pessoais, abrangendo inclusive ambientes digitais, com o propósito de garantir os direitos fundamentais de liberdade, privacidade e o desenvolvimento pleno dos indivíduos. Todavia, Schwaitzer (2020) deixa evidente que a privacidade e a proteção de dados no Brasil, tiveram sua origem na CF de 1988, especialmente nos incisos X e XII do Art. 5°, que estabelecem:

> X *"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação", ou seja, em caso de violação do direito da pessoa é aplicável uma indenização cabível"*;
> XII *"é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal"* (Brasil, 1988).

Analisando a LGPD, pode-se ressaltar que ela representa um marco significativo na regulamentação do tratamento de dados pessoais no Brasil, assegurando que os direitos fundamentais à privacidade e à liberdade sejam respeitados (Brasil, 2018).

Teixeira e Guerreiro (2022) comentam que a LGPD foi elaborada para proteger os indivíduos contra o uso indevido de seus dados pessoais, estabelecendo princípios rigorosos, como a necessidade da obtenção do consentimento[30] explícito dos titulares dos dados[31] antes da coleta e utilização de suas informações. Giovanini (2021) afirma que a LGPD impõe a obrigação de adotar medidas de segurança adequadas para a proteção dos dados tratados, bem como a transparência em todas as etapas desse processo.

Chou, Albano e Almeida (2024), esclarecem que, apesar dessas disposições legais, muitos dos parâmetros e controles[32] necessários para a implementação efetiva da LGPD ainda carecem de regulamentação específica. Isso significa que as diretrizes práticas para garantir a segurança e proteção dos dados pessoais não estão completamente definidas, criando um desafio para as organizações em cumprir integralmente a lei.

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece diretrizes fundamentais para o tratamento adequado das informações pessoais no Brasil. Moreira (2023) enfatiza que a norma busca garantir os direitos dos titulares e definir responsabilidades para controladores[33] e operadores[34], embora ainda exista desconhecimento técnico sobre medidas eficazes de proteção. Nesse sentido, os artigos 42 a 45 da LGPD preveem a responsabilidade civil dos agentes de tratamento em casos de falhas de segurança ou uso indevido de dados pessoais, assegurando ao titular o direito à reparação de danos. Tanto o controlador quanto o operador podem ser responsabilizados, sendo este último solidariamente responsável quando descumprir as instruções recebidas ou agir em desacordo com a legislação (Galvão *et al*., 2024).

---

[30] Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

[31] A LGPD define titulares de dados pessoais como qualquer pessoa física cujos dados pessoais estão sendo tratados por uma organização ou indivíduo.

[32] Os parâmetros e controles referidos no contexto da norma ISO/IEC 27000 envolvem diretrizes e práticas para a gestão da segurança da informação. A série de normas ISO/IEC 27000, especialmente a ISO/IEC 27001 e ISO/IEC 27002, estabelece um conjunto de controles e processos para proteger a confidencialidade, integridade e disponibilidade das informações dentro de uma organização. Esses controles incluem a definição de políticas de segurança, avaliação de riscos, implementação de medidas de proteção, e monitoramento contínuo das práticas de segurança. O objetivo é garantir que os dados pessoais e outras informações sensíveis sejam adequadamente protegidos contra acesso não autorizado, vazamentos e outras ameaças. A adoção de um framework baseado nesta norma ajuda a assegurar a conformidade com regulamentos como a LGPD, promovendo práticas eficazes de segurança da informação.

[33] Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

[34] Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

A seguir, o Quadro 4 sintetiza os principais aspectos relacionados à responsabilização e às obrigações previstas na LGPD.

Quadro 4 - Responsabilidade Civil e Princípios da LGPD

Aspecto	Descrição	Estudo
Finalidade da LGPD	Visa garantir os direitos dos titulares e estabelecer obrigações para controladores e operadores no tratamento de dados pessoais.	Moreira (2023)
Desconhecimento técnico	Apesar da legislação, ainda há lacunas no conhecimento técnico sobre medidas eficazes de proteção e conformidade.	
Responsabilização civil	A LGPD prevê, nos artigos 42 a 45, a responsabilização civil dos agentes de tratamento (controlador e operador) em caso de falhas de segurança ou uso indevido dos dados pessoais.	Galvão *et al*. (2024)
Responsabilidade solidária	O operador pode ser responsabilizado solidariamente quando agir em desacordo com a legislação ou com as instruções do controlador.	
Irregularidade no tratamento	Configura-se quando há descumprimento da lei ou falha na segurança esperada pelo titular, considerando riscos e tecnologias disponíveis.	
Excludentes de responsabilidade	O agente pode se eximir se comprovar que não realizou o tratamento, que não houve violação legal ou que o dano decorreu de culpa exclusiva do titular ou de terceiros.	

Fonte: Adaptado pelo Autor, com base em Moreira (2023) e Galvão *et al*. (2024).

Para enfrentar essas lacunas, Chou, Albano e Almeida (2024) sugerem a adoção de um *framework*[35] de governança de dados, que serviria como um conjunto estruturado de práticas e normas internas. Este *framework* permitiria que as organizações implementem mecanismos de controle e supervisão eficazes, assegurando que o tratamento de dados pessoais seja feito de acordo com os princípios de privacidade e segurança estabelecidos pela LGPD. Além disso, ajudaria a promover a conformidade contínua com a lei, adaptando-se às atualizações e exigências regulatórias à medida que elas são formalizadas.

Chou, Albano e Almeida (2024) citam ainda a Autoridade Nacional de Proteção de Dados (ANPD), criada pela LGPD, que se destaca na supervisão e regulamentação da proteção de dados no Brasil. Além de garantir a conformidade com a LGPD, a ANPD tem a responsabilidade de elaborar guias e normas que orientem as empresas e instituições na correta aplicação da lei. A ausência de regulamentações detalhadas até o momento, reforça a importância da ANPD em preencher essas lacunas, proporcionando diretrizes claras que possam ser seguidas por todos os agentes de tratamento[36] de dados (Burkart, 2021). Dessa forma, a ANPD não apenas assegura a proteção dos direitos dos titulares de dados, mas também promove um ambiente de maior segurança jurídica para as organizações, facilitando a

[35] Um *framework* é um conjunto de diretrizes e práticas organizadas que ajuda a estruturar e gerenciar processos de forma eficaz. Ele fornece uma base para garantir que as atividades sejam realizadas de maneira consistente e segura, como um guia para implementar boas práticas e atender a requisitos específicos.

[36] Agente de tratamento: o controlador e o operador.

implementação de práticas que atendam aos requisitos da LGPD e, consequentemente, minimizando os riscos de sanções.

A ANPD foi instituída pela Medida Provisória nº 869, de 27 de dezembro de 2018, posteriormente convertida na Lei nº 13.853/2019, com sua estrutura organizacional definida pelo Decreto nº 10.474, de 26 de agosto de 2020. Sua missão é assegurar a aplicação da LGPD, garantindo os direitos fundamentais à privacidade, liberdade e desenvolvimento da personalidade. A ANPD foi criada para proporcionar segurança jurídica e adequar a LGPD à realidade brasileira, por meio de regulamentações complementares. A cooperação entre os poderes da República e órgãos reguladores é essencial para a criação de políticas públicas e códigos de conduta conforme o artigo 50 da LGPD. O artigo 55-A trata da criação da ANPD, com previsão inicial de natureza jurídica transitória, posteriormente convertida em autarquia — o que garante mais autonomia à entidade. A estrutura da ANPD inclui o Conselho Diretor, o Conselho Nacional de Proteção de Dados e outros órgãos internos. É importante destacar que a ANPD é o único órgão com competência para aplicar sanções previstas na LGPD, conforme o artigo 55-K da referida lei (Galvão *et al.*, 2024).

Conforme informações disponíveis no site oficial da ANPD, até o momento, não há organizações públicas ou privadas credenciadas pela Autoridade para oferecer cursos, certificações ou serviços de assessoria e consultoria em LGPD. Além disso, a ANPD não estabeleceu parcerias nem reconheceu oficialmente instituições para essas finalidades (Autoridade Nacional De Proteção De Dados, 2024).

Apesar do crescente reconhecimento da importância da LGPD, muitas organizações brasileiras ainda enfrentam barreiras para implementar suas exigências. Com o avanço tecnológico, as empresas perceberam a necessidade de adequação à lei, o que exige investimentos em governança, revisão de processos e mudanças na cultura organizacional. No entanto, grande parte ainda encontra dificuldades nesse processo (Galvão *et al*., 2024). Segundo os mesmos autores, dados de pesquisa realizada pela *RD Station* mostram que, embora 93% das mil empresas entrevistadas conheçam a LGPD, apenas 15% iniciaram ações efetivas de adequação. Os principais entraves envolvem a falta de investimento em tecnologia, a escassez de profissionais qualificados — como o DPO — e a ausência de políticas internas eficazes de proteção de dados, fatores que retardam a conformidade com a legislação.

Embora a LGPD estabeleça diretrizes claras para a proteção de dados pessoais, ela não detalha como esses dados devem ser eliminados com segurança. Essa lacuna pode gerar riscos de vazamentos, especialmente durante o descarte de informações. Duarte (2020) alerta que a falta de procedimentos rigorosos compromete a integridade e a confidencialidade dos dados,

tornando-os vulneráveis a acessos indevidos. Nesse contexto, é essencial que empresas e órgãos públicos desenvolvam políticas claras e eficazes de segurança da informação, reduzindo o risco de incidentes e assegurando o cumprimento dos princípios da lei.

Conforme destacam Teffé e Viola (2020), a LGPD cria mecanismos de controle sobre o tratamento de dados e impõe deveres e responsabilidades aos agentes envolvidos, garantindo a proteção das informações e limitando seu uso às finalidades originalmente previstas, vedando sua aplicação posterior para outros propósitos.

No ordenamento jurídico brasileiro, o tratamento das informações é regulado de forma complementar pela LGPD e pela LAI, sendo cada uma voltada a finalidades específicas, porém interdependentes, conforme apresentado no Quadro 5 (Weber: Schmidt, 2023).

Quadro 5 - Abordagens internacionais sobre proteção de dados pessoais

Lei	Classificação	Exemplo
LGPD (Brasil, 2018)	Dados pessoais	Nome, CPF, endereço residencial ou eletrônico, número de telefone, imagem ou retrato, identificadores digitais.
	Dados sensíveis	Saúde, filiação religiosa ou étnica, convicções políticas ou sindicais, vida sexual, dado genético.
	Dados anonimizados	Dados que não permitem a identificação do titular.
LAI (Brasil, 2011)	Ultrassecretos	Dados referentes à soberania nacional, negociações internacionais estratégicas.
	Secretos	Dados sobre operações estratégicas envolvendo a segurança pública ou governamentais.
	Reservados	Investigações policiais, processos administrativos internos em andamento.
	Pessoal	Referentes à intimidade, vida privada, honra e imagem

Fonte: elaboração própria, 2025.

A LGPD define quatro grupos principais: os dados pessoais – permitem a identificação direta ou indireta de um indivíduo; os dados sensíveis – demandam rigor adicional por envolverem aspectos íntimos e os dados anonimizados – obtidos por técnicas que inviabilizam a associação ao titular original (Brasil, 2018).

Por sua vez, a LAI regulamenta o acesso às informações públicas considerando níveis de sigilo e prazos de restrição: ultrassecretas (até 25 anos), secretas (até 15 anos) e reservadas (até 5 anos), além de impor proteção especial às informações de caráter pessoal, que podem permanecer resguardadas por até 100 anos, salvo hipóteses legais específicas ou consentimento do titular (Brasil, 2011). Desse modo, enquanto a LGPD enfatiza a proteção da esfera privada no tratamento de dados, a LAI busca conciliar o direito à transparência com a necessidade de resguardar interesses coletivos, a segurança do Estado e a intimidade individual.

2.4 POLÍTICAS INTERNACIONAIS DE SEGURANÇA DE DADOS

A crescente complexidade do ambiente digital, impulsionada pela rápida evolução tecnológica, exigiu a criação de normas internacionais capazes de regulamentar o tratamento de dados em escala global (Lavos, 2023). Tais regulamentações tornaram-se fundamentais na prevenção de riscos e na garantia dos direitos dos titulares em um cenário digital caracterizado por sua complexidade e rápida evolução, no qual o fluxo constante de dados pessoais e corporativos passou a adquirir valores estratégicos e econômicos para organizações públicas e privadas (Lorenzon, 2021).

A *General Data Protection Regulation* (GDPR), adotada pela União Europeia em abril de 2016, representa um novo marco regulatório na proteção de dados pessoais, sendo considerada a legislação mais relevante para a segurança e a privacidade de dados na Europa e servindo de referência para legislações em outros países (Feiler; Gazaniga; Vieira, 2024). Com um período de adaptação de 24 meses, entrou em vigor em 25 de maio de 2018 e trouxe implicações globais, pois se aplica a qualquer organização, mesmo que localizada fora da UE, desde que processe dados pessoais de residentes europeus, ofereça produtos ou serviços, ou ainda monitore o comportamento de indivíduos situados no território do bloco (Monteiro, 2018).

Entre seus elementos centrais, Figura 6, estão o *Data Protection Officer* (DPO), profissional responsável por supervisionar a conformidade da organização; o Compliance, que compreende políticas e procedimentos internos para assegurar a proteção de dados; os *Data Breaches*, incidentes de vazamento ou acesso indevido de informações, obrigatoriamente reportados; e os *Personal Data*, dados pessoais que identificam direta ou indiretamente indivíduos (Alecrim, 2016). Dessa forma, a GDPR configura um sistema integrado de governança de dados, combinando responsabilidade, monitoramento contínuo e proteção dos direitos dos titulares, servindo como referência para legislações posteriores, como a LGPD (Monteiro, 2018).

Figura 6 - Sistema Integrado de governança de dados: elementos centrais da GDPR

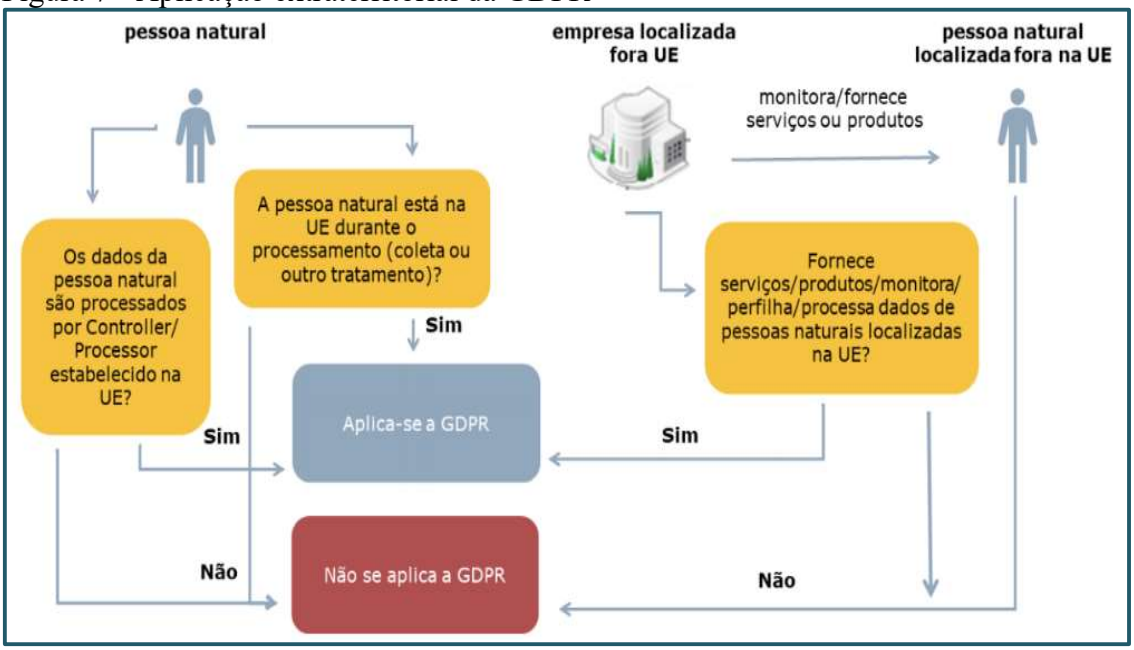
Fonte: elaboração própria, 2025 adaptada de Alecrim, 2016.

A GDPR substituiu a antiga Diretiva Europeia 95/46/EC, com o objetivo de harmonizar e modernizar as normas existentes sobre o tema entre os Estados-membros (Monteiro, 2018). Tem como um dos principais pilares, o consentimento expresso e claro dos usuários[37], que deve ser obtido antes da coleta e do uso dos dados pessoais, sendo também revogável a qualquer momento (Lorenzon, 2021). Sendo seu principal objetivo garantir aos cidadãos europeus maior controle sobre suas informações pessoais, assegurando transparência, segurança e direitos fundamentais no tratamento desses dados. Ao mesmo tempo, a regulação visa fomentar a inovação e o desenvolvimento econômico no contexto digital (Monteiro, 2018).

A Figura 7 apresenta de forma esquemática essa lógica de aplicação extraterritorial do GDPR, evidenciando as situações em que o regulamento se aplica. O fluxograma inicia com a verificação de onde ocorre o tratamento dos dados pessoais: se os dados da pessoa natural são processados por um controlador ou processador estabelecido na UE, aplica-se o GDPR. Caso contrário, deve-se verificar se a pessoa natural encontra localizada na UE durante a coleta ou outro tipo de tratamento; se a resposta for positiva, o regulamento também se aplica, desde que vinculada à oferta de bens ou serviços ou ao monitoramento do titular (Monteiro, 2018).

[37] O consentimento expresso e claro, conforme previsto no GDPR, significa que o titular dos dados deve concordar de forma livre, informada e inequívoca com o tratamento de suas informações pessoais, podendo retirar essa autorização a qualquer momento. Esse mecanismo assegura transparência e controle aos usuários sobre como seus dados são coletados, armazenados e utilizados.

Figura 7 - Aplicação extraterritorial da GDPR



Fonte: Monteiro, 2018.

De acordo com o fluxograma, quando a empresa responsável pelo tratamento está fora da UE, o critério de aplicação recai sobre a finalidade: se ela fornece serviços, produtos, monitora, perfila ou processa dados de pessoas localizadas na UE, o GDPR também se aplica. Em contrapartida, se não houver esse vínculo territorial ou funcional, conclui-se que o regulamento não é aplicável. Dessa forma, o fluxograma sintetiza como a territorialidade do GDPR ultrapassa os limites da União Europeia e alcança também entidades externas que tratam dados de indivíduos localizados em seu território (Monteiro, 2018).

Além disso, o GDPR prevê princípios como transparência, minimização de dados, portabilidade e direito ao esquecimento, reforçando a proteção integral dos dados pessoais. Essa abrangência reflete a globalização e a interconexão dos mercados digitais, ao estabelecer um padrão elevado de proteção de dados que tem influenciado legislações em diversos países (Lorenzon, 2021).

O modelo europeu tornou-se uma referência global, influenciando diretamente a formulação de legislações em outros países, inclusive fora do espaço europeu (Machado, 2020). Um exemplo emblemático é o Brasil, cuja LGPD, sancionada em 2018, foi fortemente inspirada no regulamento europeu (Lorenzon, 2021). Machado (2020) destaca, em seus estudos, a importância da GDPR como uma das bases estruturantes que apoiaram a criação da LGPD, servindo não apenas como parâmetro normativo, mas também como guia conceitual para o desenho de políticas públicas de proteção de dados.

Ao adotar princípios semelhantes aos do regulamento europeu — como a limitação da finalidade, a minimização de dados e o consentimento do titular —, o Brasil buscou alinhar-se às normas internacionais. Esse alinhamento facilita a cooperação entre países, promove a confiança no comércio digital e fortalece a proteção da privacidade dos cidadãos (Machado, 2020). Além disso, evidencia uma estratégia de inserção global, na medida em que a compatibilidade regulatória possibilita maior integração econômica e tecnológica (Marinho; Paranaguá; Piva, 2024).

Nesse sentido, tanto a GDPR quanto a LGPD compartilham a visão de que a proteção de dados pessoais deve ser entendida como um direito fundamental, essencial para o exercício pleno da cidadania na sociedade da informação, consolidando um padrão normativo que transcende fronteiras e influencia o modo como os Estados, as empresas e a sociedade civil compreendem a governança da informação.

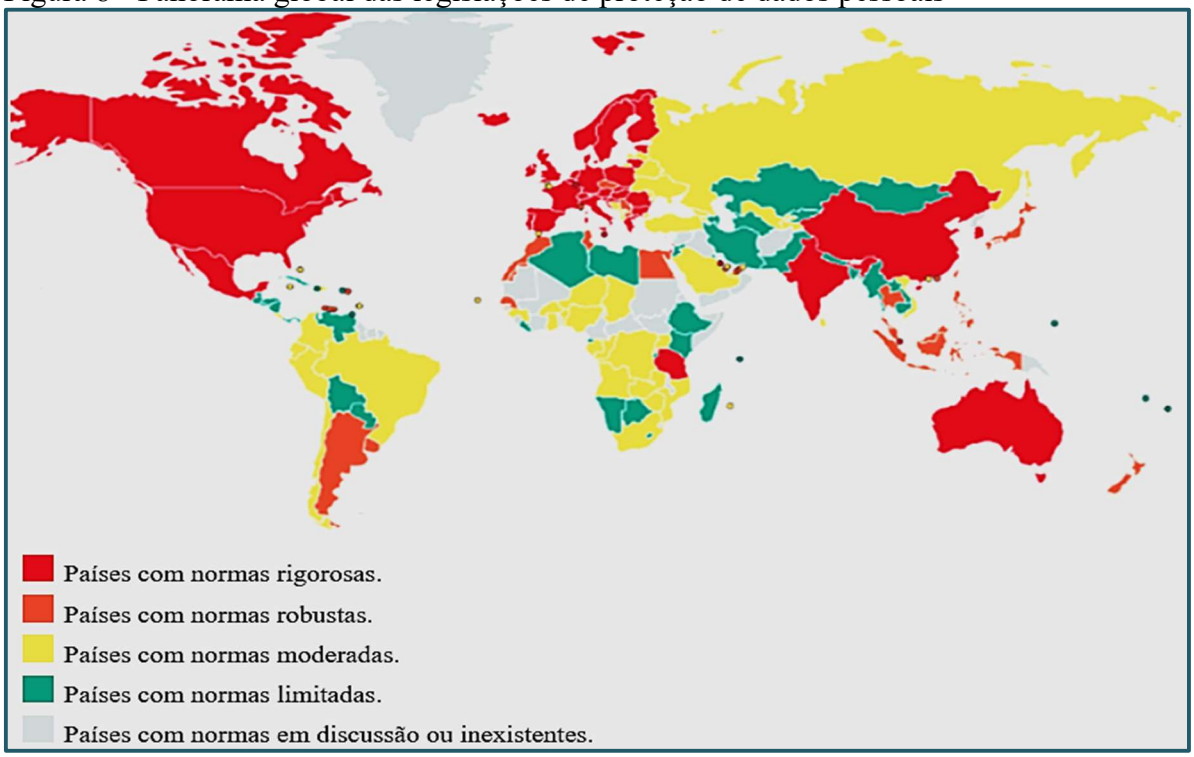
Além disso, esse movimento de harmonização normativa em torno da proteção de dados pessoais evidencia uma tendência global de valorização da privacidade e do controle dos indivíduos sobre suas informações. Mesmo países com abordagens regulatórias distintas, como os Estados Unidos, têm adotado medidas relevantes nesse campo. A legislação norte-americana, embora mais fragmentada e setorial, contempla leis específicas como a *Children's Online Privacy Protection Act* (COPPA), voltada para a proteção da privacidade infantil no ambiente digital e a *Personal Information Protection and Electronic Documents Act* (PIPEDA), vigente no Canadá, que também traz diretrizes relevantes para o tratamento de dados pessoais em ambientes eletrônicos, evidenciando uma abordagem mais setorial em comparação com a abrangência do GDPR (Feiler; Gazaniga; Vieira, 2024).

Essa expansão e consolidação desses instrumentos normativos e regulamentações internacionais, destacados por essa pesquisa, reflete um movimento mais amplo de fortalecimento da cultura da privacidade ao redor do mundo. Nesse contexto, observa-se um número crescente de países que passaram a adotar legislações específicas para proteção de dados pessoais, ainda que com diferentes níveis de abrangência e rigor (Costa; Cunha, 2023).

Conforme ilustrado a Figura 8, esse panorama global revela um cenário heterogêneo, no qual normas mais estritas convivem com legislações em estágio inicial de desenvolvimento, evidenciando as particularidades de cada contexto jurídico e social (DLA Piper[38], 2025).

[38] DLA PIPER é um escritório internacional de advocacia, fundado em 2005 a partir da fusão de grandes firmas jurídicas, com sedes em Londres (Reino Unido) e Chicago (Estados Unidos). Está presente em mais de 40 países e é reconhecido mundialmente por sua atuação em diversas áreas do direito, com destaque para temas de privacidade, proteção de dados e regulamentações internacionais.

Figura 8 - Panorama global das legislações de proteção de dados pessoais



Fonte: elaboração própria, 2025 adaptada de *DLA Piper,* 2025.

Os dados da Figura 8 evidenciam que a proteção de dados pessoais apresenta diferentes estágios de desenvolvimento ao redor do mundo. Nota-se que países da União Europeia, da América do Norte e da Oceania concentram legislações classificadas como mais rigorosas (vermelho), em consonância com padrões como o GDPR. Já na América Latina e em parte da Ásia observa-se a presença de normas robustas a moderadas (laranja e amarelo), indicando avanços significativos, mas ainda em processo de consolidação. Em contrapartida, muitos países africanos e parte do Oriente Médio permanecem com regulamentações limitadas (verde) ou mesmo inexistentes ou em discussão (cinza), o que revela desigualdades na adoção de mecanismos jurídicos voltados à privacidade e à segurança da informação DLA Piper, 2025).

Rodrigues (2024) afirma que a proteção de dados pessoais é regulada de forma diferente em cada país, variando desde legislações rigorosas até normativas básicas ou inexistentes. Como exemplo, Lorenzon (2021), Feiler, Gazaniga e Vieira (2024) destacam que o GDPR, por possuir um dos marcos regulatórios mais rigorosos do mundo, estabelece, em seu art. 83, penalidades de descumprimento para violações severas – violação de princípios básicos do tratamento de dados, transferência internacional de dados sem base legal – de até € 20 milhões ou 4% do faturamento anual. Já a LGPD, em seu art. 52, impõe multas de até 2% do faturamento, limitadas a R$ 50 milhões por infração, aplicáveis a pessoas jurídicas de direito privado (Schwaitzer, 2020).

Portanto, essas legislações, como destacam Feiler, Gazaniga e Vieira (2024), ainda que possuam particularidades em sua estrutura e alcance, convergem em um ponto central: a proteção dos direitos e das liberdades fundamentais dos indivíduos diante do avanço da sociedade digital. A criação desses marcos regulatórios, conforme os autores, busca limitar a coleta indiscriminada de informações pessoais e estabelecer parâmetros de transparência, segurança, adequação e finalidade no tratamento de dados. Nesse sentido, funcionam como um mecanismo de contenção contra práticas abusivas de instituições públicas e privadas, assegurando ao cidadão maior controle sobre seus próprios dados e reforçando a responsabilidade das organizações quanto ao seu uso adequado.

Dessa forma, observa-se que a LGPD, ao se inspirar no GDPR, passou a representar um marco importante na estruturação da proteção de dados pessoais no Brasil, adotando princípios como transparência, consentimento explícito, minimização de dados e responsabilização dos agentes de tratamento, promovendo maior segurança jurídica e proteção aos titulares de dados (Teixeira e Guerreiro, 2022). Entretanto, a segurança da informação não se limita à coleta e ao uso de dados, estendendo-se também ao seu armazenamento e descarte. Nesse sentido, a PNRS, ao tratar do ciclo de vida de EEE, torna-se relevante no contexto da proteção de dados, especialmente no que se refere à eliminação segura de ativos digitais.

2.5 POLÍTICA NACIONAL DE RESÍDUOS SÓLIDOS (PNRS)

De acordo com a *United Nations Institute for Training and Research* (UNITAR), os resíduos eletrônicos, também conhecidos como *e-lixo*[39], compreendem EEE descartados pelos proprietários sem perspectiva de reutilização, englobando qualquer equipamento com componentes elétrico ou eletrônico que, devido à sua composição complexa e volume crescente, apresentam desafios significativos para a gestão ambiental sustentável (UNITAR, 2024). A PNRS representa um marco regulatório fundamental para a gestão e o descarte de resíduos no Brasil, estabelecendo diretrizes que vão desde a geração até o descarte final, cujo objetivo é minimizar os impactos ambientais e promover a sustentabilidade. Entre suas metas, destacam-

[39] O termo *e-lixo* (ou lixo eletrônico) começou a ser utilizado a partir da década de 1990, com o aumento do consumo e descarte de equipamentos eletrônicos, como computadores, celulares e dispositivos de armazenamento. Foi especialmente a partir dos anos 2000 que o conceito ganhou maior visibilidade nas discussões ambientais, devido ao crescimento expressivo desses resíduos e aos impactos negativos que podem causar ao meio ambiente. O termo designa os resíduos provenientes de aparelhos eletrônicos descartados inadequadamente, que contêm substâncias tóxicas e componentes valiosos para a economia circular, o que reforça a necessidade de práticas responsáveis de manejo e reciclagem.

se o incentivo à reutilização, reciclagem e o descarte correto de rejeitos, visando minimizar os danos causados ao meio ambiente (Schaun *et al.*, 2023).

No contexto do descarte de EEE, a PNRS estabelece que a responsabilidade pelo gerenciamento dos resíduos é compartilhada entre os geradores, os fabricantes, os importadores, os distribuidores e os comerciantes, que devem adotar técnicas e ações capazes de garantir o controle de seus produtos até o final de sua vida útil. Esse princípio, conforme artigo 33 da PNRS, é conhecido como responsabilidade compartilhada pelo ciclo de vida dos produtos, visando assegurar que todos os envolvidos participem de forma efetiva da gestão dos resíduos, incluindo a rastreabilidade desses ativos ao longo de sua cadeia (São Bento; Carneiro, 2024). Conforme as boas práticas estabelecidas pela ISO/IEC 27002 é fundamental implementar procedimentos de gestão e rastreamento de ativos que garantam a proteção dos dados em todas as etapas do ciclo de vida dos produtos.

Schaun *et al.* (2023**)** reforçam esta perspectiva ao destacarem que a ideia central é que cada um desses participantes tenha um papel a desempenhar na minimização dos resíduos gerados e na mitigação dos impactos ambientais e à saúde pública decorrentes do ciclo de vida dos produtos. Neste sentido, a PNRS, em seu artigo 9º, estabelece a hierarquia de gestão de resíduos sólidos, priorizando a não geração, redução, reutilização, reciclagem, tratamento e pôr fim à disposição final ambientalmente adequada dos rejeitos. Além disso, o artigo 33 da referida lei determina que a responsabilidade compartilhada pelo ciclo de vida dos produtos persiste mesmo após o uso pelo consumidor (Brasil, 2010).

Segundo Miragem (2019), os fornecedores têm a responsabilidade de garantir a privacidade dos consumidores durante todo o ciclo de vida dos produtos e serviços. Isso abrange desde a fase de desenvolvimento, com a adoção de medidas de segurança adequadas, até o descarte, por meio de práticas eficazes para a conservação e eliminação segura das informações coletadas. Para o autor, é fundamental que haja uma gestão abrangente de dados que assegure a proteção contínua das informações em todas as etapas, reduzindo riscos e promovendo a conformidade com as normas de privacidade. A ISO/IEC 27040 reforça esta necessidade, ao estabelecer controles específicos para a eliminação e sanitização segura de dispositivos de armazenamento de dados, práticas que são essenciais para assegurar a remoção definitiva de dados pessoais e reduzir riscos de vazamentos ou acessos não autorizados.

Alencar (2023), complementa ao ressaltar a importância da responsabilidade solidária entre os fabricantes e as assistências técnicas autorizadas, onde eventuais vazamentos de dados podem implicar ambas as partes nos danos causados ao consumidor. Neste mesmo contexto, as

empresas devem adotar práticas de logística reversa, ou seja, os resíduos devem retornar aos fabricantes ou a centros de coleta apropriados após o fim de sua vida útil (Brasil, 2010).

No caso dos EEE, a PNRS determina que os fabricantes, importadores, distribuidores e comerciantes disponibilizem “postos de entrega de resíduos reutilizáveis e recicláveis” (Brasil, 2010, art. 33, § 3º, II). Esses pontos de coleta, conhecidos como “Pontos de Entrega Voluntária (PEVs)”, permitem que os consumidores possam descartar corretamente seus resíduos eletrônicos, que posteriormente são enviados para empresas recicladoras devidamente homologadas (Green Elétron, 2024).

Além das diretrizes legais, é importante considerar os aspectos comportamentais relacionados ao descarte de REEE. Nesse sentido, Mota *et al.* (2016) analisaram o comportamento dos usuários na zona sul da cidade de São Paulo quanto ao descarte de lixo eletrônico e identificaram baixos níveis de informação e engajamento por parte da população. Os resultados evidenciam a necessidade de campanhas educativas e ações de conscientização ambiental que incentivem a população a adotar práticas corretas de descarte. Segundo os autores, a efetividade da logística reversa e da responsabilidade compartilhada depende não apenas da estrutura legal e técnica disponível, mas também do envolvimento ativo da sociedade civil. Assim, a PNRS só alcançará seus objetivos se houver articulação entre poder público, setor produtivo e consumidores, promovendo uma cultura ambiental responsável e participativa.

Conforme ilustrado na Figura 9, é possível observar diferentes modelos de Pontos de Entrega Voluntária (PEVs), estruturas utilizadas para o descarte adequado de resíduos eletrônicos por parte dos consumidores. Esses pontos visam facilitar a logística reversa e promover práticas ambientalmente corretas, conforme preconizado pela PNRS (Jucon, [202?]).

Figura 9 - Ponto de descarte de resíduos eletrônicos

Fonte: Jucon, [202?].

A gestão compartilhada dos resíduos sólidos, em conformidade com as normas vigentes, visa reduzir ou eliminar os impactos ambientais, além de possibilitar o reaproveitamento de materiais como matéria-prima para novos produtos, gerando também economia de custos (Marques, 2017). Esse procedimento envolve várias etapas, exigindo a colaboração entre diferentes organizações, públicas e privadas, incluindo ações como: consumo consciente, descarte adequado, coleta, triagem, reciclagem e destinação final (Brasil, 2010).

Esse processo está alinhado aos princípios da "Economia Circular", que se apresenta como uma proposta alternativa ao modelo linear de produção e consumo, tendo como princípio central a eliminação do desperdício e da poluição em todas as fases do ciclo de vida dos produtos (Almeida, 2023). A autora enfatiza que, após a utilização, os resíduos devem retornar ao ciclo produtivo pelos consumidores, de forma que sejam reintegrados aos processos industriais, reduzindo a necessidade de extração de novos recursos.

Essa reintegração dos resíduos, por sua vez, depende da responsabilidade socioambiental compartilhada entre governos, empresas e sociedade civil, a qual é fundamental para viabilizar a economia circular, assegurando o uso sustentável dos recursos e o retorno adequado dos resíduos aos ciclos produtivos, promovendo a conservação ambiental e a justiça social. Nesse sentido, a economia circular propõe a redução da extração de recursos naturais por meio da reinserção de produtos, componentes e materiais nos processos produtivos, valorizando a durabilidade, a reutilização e a reciclagem como estratégias centrais para a sustentabilidade ambiental e a eficiência econômica (Almeida, 2023). Portanto, governos, empresas e sociedade civil devem atuar de forma integrada e comprometida com a preservação ambiental, promovendo o descarte responsável e sustentável dos resíduos eletrônicos. No entanto, para que essa gestão seja eficaz, é indispensável que a população esteja ciente dos danos que o descarte inadequado de lixo eletrônico pode causar ao meio ambiente.

Nesse contexto, a PNRS estabelece diretrizes voltadas à conscientização e à educação ambiental, incentivando o uso de pontos de coleta e a participação em programas de reciclagem. Tais programas são essenciais para fortalecer a responsabilidade socioambiental dos consumidores, estimulando práticas conscientes que alimentam o ciclo da economia circular, com foco na redução do desperdício e na valorização dos materiais descartados. Da mesma forma, a legislação prevê sanções penais para empresas e indivíduos que descumprirem as normas de descarte e gerenciamento de resíduos, reforçando a importância da conformidade com as diretrizes estabelecidas (Brasil, 2010).

O Anexo I do Decreto nº 10.240, de 2020 (Brasil, 2020), lista os equipamentos eletroeletrônicos que estão sujeitos à logística reversa. Para os objetivos desta dissertação, destacam-se os equipamentos capazes de armazenar dados pessoais, como:

- Câmera fotográfica digital;
- Celular;
- Computadores portáteis, como *laptop*, *netbook*, *notebook*;
- Dispositivos eletroeletrônicos para armazenagem ou transferência de dados, como *pen drives*, cartões de memória, HDD, SSD, CDs, DVDs, Disquetes;
- Gravadores de vídeo digital (DVR);
- Impressoras;
- *Tablets.*

A abordagem de responsabilidade ambiental introduzida pela PNRS oferece uma oportunidade significativa para aprimorar a gestão adequada e eficaz dos resíduos de equipamentos eletroeletrônicos. A responsabilidade compartilhada, conforme estabelecido no art. 30 da PNRS, institui uma rede de responsabilidades distintas entre os diversos agentes envolvidos na gestão integrada desses resíduos, desde a produção até o descarte final dos equipamentos (Brasil, 2010).

Assim, a PNRS, em seus 57 artigos, fornece um *framework* abrangente para o manejo e descarte de EEE no Brasil, assegurando que esses materiais sejam tratados de forma adequada para proteger o meio ambiente e promover a sustentabilidade. A observância da PNRS é essencial para reduzir os impactos negativos associados ao lixo eletrônico e para promover uma gestão responsável dos REEE (Almeida, 2023).

Xavier *et al*. (2025) mensuram que a gestão de REEE no Brasil foi regulamentada pelo Decreto n. 10.240/2020, que estabelece diretrizes para a logística reversa desses produtos, ou seja, os procedimentos destinados a assegurar que os resíduos sejam coletados, transportados e destinados de forma ambientalmente adequada. O decreto define as responsabilidades de todos os atores da cadeia — consumidores, fabricantes, importadores, distribuidores, comerciantes e entidades gestoras — quanto à destinação correta dos REEE, visando reduzir impactos ambientais e promover a sustentabilidade (Brasil, 2010).

No contexto da proteção de dados pessoais, o decreto n. 10.240/2020 reforça uma obrigação específica dos consumidores: o inciso II do art. 31 determina que, antes do descarte, devem ser removidas todas as informações e dados contidos nos dispositivos eletroeletrônicos, incluindo discos rígidos, cartões de memória e estruturas semelhantes (Brasil, 2020). Essa exigência é de extrema relevância para a SI, pois previne que dados sensíveis, pessoais ou

corporativos sejam expostos inadvertidamente, evitando riscos de vazamentos, acessos não autorizados e fraudes. Além disso, a norma contribui para a conscientização sobre a importância de práticas seguras de descarte e a responsabilidade compartilhada na proteção de informações digitais e na preservação ambiental (Xavier *et al.,* 2025).

Essa exigência tem como objetivo proteger a privacidade dos dados durante o processo de descarte e está alinhada à ISO/IEC 27040:2015, que recomenda a sanitização de dispositivos de armazenamento de dados como medida para a eliminação dos dados de forma segura. O § 1° do referido inciso determina que não subsistirá responsabilidade das empresas, das entidades gestoras ou de outro participante do sistema de logística reversa pelos dados ou pelas informações que não tenham sido excluídas pelo consumidor (Brasil, 2020).

Por outro lado, o § 2° determina que em caso de uso indevido ou não autorizado dos dados, o consumidor poderá formalizar denúncia às autoridades competentes para apuração e autoria e materialidade do fato (Brasil, 2020).

Além disso, o inciso I do art. 36 determina que os comerciantes são obrigados a informar os consumidores, no momento do recebimento dos equipamentos descartados, sobre a necessidade de remoção prévia dos dados (Brasil, 2020).

Quanto à perda da propriedade dos produtos descartados, o art. 32 dispõe que o descarte implica na perda tácita e imediata da propriedade dos bens, de forma irrevogável e irretratável, sem necessidade de formalidades adicionais, além de reconhecer que os dados neles armazenados tornar-se irrecuperáveis, sem direito a qualquer indenização, pagamento ou ressarcimento ao consumidor (Brasil, 2020).

Portanto, o descarte de ativos contendo dados pessoais deve ser realizado com total segurança, garantindo tanto a proteção de dados pessoais, quanto a responsabilidade ambiental. A implementação de diretrizes claras, alinhadas às exigências da LGPD, da PNRS e da ISO/IEC 27040:2015, bem como à fiscalização eficaz das obrigações, estabelecidas pelo Decreto nº 10.240/2020, são essenciais para minimizar riscos e promover um descarte adequado e consciente dos REEE.

Diante da relevância do descarte responsável de equipamentos eletroeletrônicos e da necessidade de proteger os dados neles contidos, torna-se essencial compreender os parâmetros normativos que orientam a segurança da informação nesse processo. Nesse contexto, destaca-se a importância da família de normas ISO/IEC 27000, que fornece diretrizes específicas para a gestão da segurança da informação, abrangendo práticas de controle, tratamento e eliminação segura de ativos digitais ao longo de seu ciclo de vida.

2.6 FAMÍLIA ISO/IEC 27000

A ISO foi fundada em 1947 a partir da fusão entre a *International Federation of the National Standardizing Associations (ISA)* e o *United Nations Standards Coordinating Committee (UNSCC)*. Com sede em Genebra, Suíça, a ISO é composta por representantes de organismos nacionais de normalização de mais de 172 organismos nacionais de normatização e tem como principal objetivo desenvolver e promover normas técnicas internacionais que contribuam para a padronização, qualidade e segurança de produtos, serviços e sistemas (ISO, 2025).

No Brasil, a responsabilidade pela adoção, tradução e difusão das normas ISO cabe à Associação Brasileira de Normas Técnicas (ABNT)[40]. Fundada em 1940, a ABNT é uma entidade privada, sem fins lucrativos, reconhecida como o Foro Nacional de Normalização. Ela representa oficialmente o país junto à ISO e atua na elaboração de normas técnicas nacionais, garantindo a adaptação dessas diretrizes internacionais à realidade brasileira (ABNT, [202?]).

As normas ISO possuem caráter não obrigatório, conforme apontam Tapia; Valdés e Gutiérrez (2021), uma vez que são elaboradas por uma organização internacional não governamental e, portanto, não têm poder coercitivo. Porém, possuem grande valor estratégico na gestão organizacional de todos os tamanhos e setores, estabelecendo diretrizes amplamente reconhecidas que visam à eficiência, segurança e conformidade de processos em diversas áreas.

Entre essas normas, destaca-se a família ISO/IEC 27000, voltada à Gestão de Segurança da Informação (GSI), que fornece princípios, requisitos e orientações para estabelecer, implementar, manter e aprimorar continuamente um SGSI. Essa estrutura permite que as organizações identifiquem e protejam seus ativos informacionais críticos, reduzindo riscos e assegurando a continuidade das operações (Magalhães, 2021).

Para que o SGSI seja eficaz, segundo a ISO/IEC 27001, é essencial o comprometimento da alta gestão, que deve garantir a liderança do processo, bem como o envolvimento de todos os setores da organização, incluindo a definição clara de papéis, responsabilidades, políticas, controles e processos que assegurem a integridade, confidencialidade e disponibilidade da informação. Portanto, a adoção das normas da família ISO/IEC 27000 permite às organizações alinhar suas práticas de segurança da informação com padrões internacionalmente

[40] A Associação Brasileira de Normas Técnicas (ABNT) é o órgão responsável pela normalização técnica no Brasil. Fundada em 1940, é uma entidade privada, sem fins lucrativos, reconhecida como o Foro Nacional de Normalização. Atua na elaboração de normas técnicas e representa oficialmente o país junto à International *Organization for Standardization* (ISO), sendo responsável por traduzir, adaptar e difundir essas normas no território nacional.

reconhecidos, promovendo confiança, transparência e resiliência operacional, especialmente em contextos que envolvem o tratamento e o descarte seguro de dados sensíveis.

2.6.1 PRINCIPAIS NORMAS DA FAMÍLIA ISO/IEC 27000

No contexto da SI, a família de normas ISO/IEC 27000 estabelece diretrizes para a implementação, auditoria e aprimoramento contínuo de SGSI. A certificação baseada nessas normas não se limita a um procedimento formal, mas representa um diferencial competitivo, pois confere reconhecimento internacional às organizações e fortalece sua credibilidade perante clientes, fornecedores, colaboradores e parceiros. Além disso, sua adoção proporciona um processo sistemático de identificação, tratamento e correção de vulnerabilidades, reduzindo riscos e aumentando a resiliência operacional (Diniz; Diniz, 2021).

O Quadro 6 apresenta exemplos das normas da série ISO/IEC 27000, destacando suas principais funções em áreas como gestão de riscos, auditoria, governança, segurança em nuvem, continuidade dos negócios, tecnologias e proteção de dados pessoais.

Quadro 6 - Lista da série ISO/IEC 27000 e funções principais

Norma ISO/IEC	**Função Principal**
27000	Termos e definições para Sistemas de Gestão de Segurança da Informação (SGSI).
27001	Requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI.
27002	Diretrizes para implementação de controles de segurança da informação.
27003	Guia para implementar um SGSI.
27004	Medição e monitoramento da eficácia do SGSI.
27005	Gestão de riscos de segurança da informação.
27006	Requisitos para órgãos que auditam e certificam SGSI.
27007	Diretrizes para auditoria de SGSI.
27008	Avaliação de controles implementados no SGSI.
27014	Diretrizes para governança de segurança da informação.
27017	Controles de segurança para serviços de nuvem.
27018	Proteção de dados pessoais em nuvens públicas.
27031	Planejamento da continuidade dos negócios em segurança da informação.
27032	Segurança cibernética e proteção contra ameaças na internet.
27033	Proteção de comunicações entre redes (dividida em várias partes).
27034	Segurança de aplicativos desenvolvidos internamente ou adquiridos/operados por 3ºs.
27035	Gestão de incidentes de segurança da informação.
27037	Preservação, coleta, manuseio e descarte de evidências digitais, incluindo equipamentos de armazenamento de dados.
27039	Implementação e gestão de sistemas de detecção e prevenção de intrusão.
27040	Técnicas de segurança para proteção de ambientes de armazenamento de dados.
27701	Gestão da privacidade e dados pessoais (expansão da ISO/IEC 27001).

Fonte: ISO/IEC, 2018

A padronização trazida pela ISO/IEC 27001, principal norma da família, assegura que as práticas de segurança não fiquem restritas a iniciativas pontuais, mas se convertam em políticas consistentes e replicáveis em diferentes contextos organizacionais. Ao estabelecer critérios objetivos e verificáveis, a certificação promove a proteção dos dados quanto à confidencialidade, integridade, disponibilidade e autenticidade, pilares indispensáveis em ambientes de armazenamento e processamento de informações (Magalhães, 2021). Em outras palavras, a padronização garante que diferentes organizações sigam parâmetros globais de boas práticas, facilitando auditorias, aumentando a confiança nas transações digitais e contribuindo para a conformidade com legislações de proteção de dados, como a LGPD e o GDPR.

Além disso, conforme Diniz e Diniz (2021), a norma ISO/IEC 27701 surge como um importante desdobramento da ISO/IEC 27001, ao introduzir controles específicos voltados à privacidade e proteção de dados pessoais. Essa norma amplia o escopo do SGSI para contemplar os princípios da proteção de dados definidos por legislações como a LGPD, contribuindo para a conformidade regulatória e a mitigação de riscos jurídicos. Para os autores, a integração entre gestão de segurança da informação e governança de dados pessoais é um passo estratégico para as organizações que desejam alinhar boas práticas internacionais aos marcos legais nacionais.

A ISO/IEC 27001 é uma das normas de SI mais conhecidas e ocupa a terceira posição entre as certificações ISO mais disseminadas no mundo, ficando atrás apenas das ISO 9001 e ISO 14001 (Culot *et al.*, 2021). Segundo Diniz e Diniz (2021), ela pode ser utilizada como uma estrutura de referência para ajudar as organizações a se adaptarem à LGPD, tornando-se, assim, uma ferramenta eficiente para gerenciar e proteger dados pessoais dentro do ambiente empresarial. Já Magalhães (2021), enfatiza que essa norma tem a finalidade de assegurar a confidencialidade, integridade, disponibilidade e autenticidade de um sistema de segurança, sendo essencial para qualquer organização que necessite proteger informações.

A ISO/IEC 27002, por sua vez, orienta sobre as boas práticas para a gestão de um SGSI, abordando aspectos como controle de acesso, segurança física e ambiental e gestão de incidentes. Já a ISO/IEC 27003, tem por objetivo orientar as empresas na criação, implementação, manutenção e aprimoramento contínuo de um SGSI. Enquanto isso, a ISO/IEC 27005, foca na gestão de riscos de SI, fornecendo diretrizes para a identificação, avaliação e tratamento de riscos específicos. Ademais, a ISO/IEC 27006 oferece diretrizes para os organismos de certificação, especificando os processos formais a serem seguidos durante a auditoria de um SGSI (Lavos, 2023).

A norma ISO/IEC 27037 estabelece diretrizes para garantir que a identificação, coleta, aquisição e a preservação de evidências digitais sejam conduzidas de maneira adequada, confiável e juridicamente aceitas (*Sudyana; Prayudi; Sugiantoro*, 2019). A norma define procedimentos sistemáticos e imparciais para investigação de dispositivos digitais assegurando sua integridade, autenticidade e admissibilidade em processos judiciais ou disciplinares. Além disso, considera que as evidências digitais podem ser extraídas de diversos equipamentos como computadores, redes, smartphones e bancos de dados (Oliveira, 2021).

A norma ISO/IEC 27040, trata diretamente da segurança no armazenamento de dados, estabelecendo diretrizes que garantem a confidencialidade, integridade, disponibilidade e autenticidade das informações. Entre suas recomendações, destaca-se a adoção de práticas adequadas de *backup*, assegurando a proteção dos dados contra perdas, acessos não autorizados e falhas no sistema, bem como procedimentos de sanitização de mídias e dispositivos de armazenamento, conforme destacado pela *Storage Networking Industry Association (*SNIA, 2018)[41].

A norma ISO/IEC 27701, estabelece diretrizes para a implementação de um Sistema de Gestão da Privacidade da Informação (SGPI) dentro de um SGSI já existente, com base na ISO/IEC 27001 (Giovanini, 2021). O objetivo dessa nova norma é regulamentar também os processos relacionados à proteção de dados pessoais, abordando aspectos como coleta, responsabilidade, disponibilidade, autenticidade, integridade e confidencialidade desses dados (Lachaud, 2020).

Lachaud (2020) destaca que a ISO/IEC 27701 oferece um *framework* abrangente que inclui desde a identificação e avaliação de riscos relacionados à privacidade até a implementação de controles e medidas para proteger dados pessoais. O autor ainda esclarece que essa norma sugere a criação de uma política de privacidade, treinamento de pessoal e a necessidade de um gerenciamento eficaz das violações de segurança e incidentes envolvendo dados pessoais (como acessos não autorizados a sistemas, roubo ou vazamento de informações sensíveis, perda de dispositivos contendo dados confidenciais).

Portanto, as diretrizes da família ISO/IEC 27000, embora sejam de adesão voluntária e focadas na SI, auxiliam as organizações na proteção de seus dados contra ameaças e vulnerabilidades (Lavos, 2023). Neste sentido, a adoção dessas normas não só facilita o cumprimento de regulamentações locais, como a LGPD, que é uma lei federal de cumprimento

[41] SNIA: Associação global sem fins lucrativos que reúne fabricantes, fornecedores e profissionais da área de tecnologia da informação, com o objetivo de desenvolver padrões, diretrizes e boas práticas relacionadas ao armazenamento e à gestão de dados em redes.

obrigatório voltado para a gestão e tratamento de dados pessoais, mas também fortalece a confiança dos clientes e parceiros comerciais, uma vez que demonstra um compromisso com as melhores práticas globais (Giovanini, 2021).

2.7 COMPUTAÇÃO FORENSE

A Ciência Forense Digital (CFD), conforme Alves (2024), é um ramo especializado da ciência forense voltado à investigação e análise de evidências armazenadas em dispositivos digitais, abrangendo desde sistemas complexos — como servidores corporativos — até tecnologias portáteis, como smartphones e *smartwatches,* além de outros dispositivos conectados. Trata-se de um campo em constante evolução, que acompanha os avanços tecnológicos e seus impactos no campo jurídico e investigativo.

Nesse contexto, a computação forense — também denominada forense digital — tem como principal objetivo localizar e preservar informações digitais que possam ser utilizadas como prova em investigações criminais, civis ou administrativas, conforme padrões técnicos internacionalmente reconhecidos (Alves, 2024). De acordo com Sudyana; Prayudi; Sugiantoro (2019), trata-se da aplicação de métodos científicos e analíticos à infraestrutura digital, com o propósito de identificar, recuperar, preservar, examinar e apresentar informações digitais de forma confiável.

A realização dessas atividades exige o cumprimento de critérios para garantir a integridade e autenticidade dos dados originais, evitando alterações que comprometam as evidências nos processos legais (Alves, 2024).

Esses procedimentos são conduzidos por profissionais especializados — os peritos — que utilizam ferramentas específicas para extração, análise e interpretação dos dados digitais (Sudyana; Prayudi; Sugiantoro, 2019). O escopo da computação forense abrange desde computadores pessoais e *smartphones* até equipamentos vinculados à Internet das Coisas (IoT)[42], como carros, casas e cidades inteligentes (Pinheiro *et al*. 2020), bem como câmeras de segurança, assistentes virtuais, lâmpadas e geladeiras inteligentes (Alves, 2024), cujo exame

[42] A Internet das Coisas (IoT) refere-se à rede de dispositivos físicos conectados à internet, capazes de coletar, transmitir e processar dados automaticamente. Exemplos incluem Smart TVs, sensores domésticos e sistemas de monitoramento, que geram grandes volumes de informações sensíveis de forma contínua. Esse cenário apresenta desafios para a privacidade e a segurança da informação, pois muitas vezes não é possível identificar claramente o responsável pelo tratamento dos dados, a coleta pode ocorrer sem o conhecimento ou consentimento do titular, e as regulamentações ainda estão em adaptação às novas tecnologias.

pode revelar informações mesmo que os dados estejam ocultos ou excluídos, técnicas especializadas possibilitam sua recuperação (Alves, 2024).

A norma ISO/IEC 27037 estabelece diretrizes detalhadas para as etapas da investigação forense digital, abrangendo a identificação, coleta, aquisição, preservação e documentação de evidências digitais. Seu foco principal é garantir a manutenção da integridade dos dados e assegurar a cadeia de custódia, elementos fundamentais para a validade das provas (Sudyana; Prayudi; Sugiantoro, 2019).

A Figura 10 ilustra as etapas da computação forense digital conforme essa norma, destacando o fluxo desde a identificação até a documentação dos dados.

Figura 10 - Etapas da computação forense digital segundo a ISO/IEC 27037

Fonte: Elaboração própria, 2025.

Cabe ao perito identificar os dispositivos ou dados que podem conter informações relevantes, que deverão ser coletadas de forma segura, com o objetivo de preservar os dados de qualquer modificação, utilizando ferramentas apropriadas e seguindo critérios técnicos e legais. Na etapa de aquisição, é realizada a cópia fiel dos dados, de forma a preservar os dados originais, garantindo sua integridade, autenticidade e confiabilidade das evidências. Todo o processo deverá ser documentado ao longo do processo, assegurando a transparência, rastreabilidade e confiabilidade do processo (Sudyana; Prayudi; Sugiantoro, 2019).

2.8 SANITIZAÇÃO EM DISPOSITIVOS DE ARMAZENAMENTO DE DADOS

A simples formatação de um dispositivo de armazenamento de dados não é o suficiente para remover de forma segura os dados contidos, pois este processo apenas apaga os identificadores dos arquivos, permitindo que ferramentas especializadas possam recuperá-las e torná-las novamente acessíveis. Para assegurar a exclusão definitiva dos dados devem ser adotados procedimentos que utilizam métodos para apagar bit a bit estes dados, de modo que impossibilite qualquer tentativa de recuperação (Moreira, 2023). Conforme o *International Data Sanitization Consortium* (IDSC, 2025), a sanitização de dados consiste na remoção ou

destruição intencional, permanente e irreversível das informações armazenadas, garantindo que não restem resíduos recuperáveis, mesmo por meio de ferramentas forenses avançadas.

A Figura 11 ilustra os principais métodos de sanitização de dispositivos de armazenamento: destruição física (trituração, fragmentação ou incineração do meio físico), apagamento criptográfico (destruição das chaves criptográfica dos dados) e apagamento lógico (IDSC, 2025).

Figura 11 - Métodos de sanitização de dispositivos de armazenamento de dados

Fonte: elaborado pelo autor, 2025.

Os métodos de sanitização apresentados cumprem funções distintas, porém complementares, na eliminação segura de dados. A destruição física, recomendada para mídias obsoletas ou danificadas, consiste na trituração, fragmentação ou incineração do dispositivo, sendo considerada irreversível. Conforme a ISO/IEC 27040:2015, esse procedimento é indicado para dispositivos que não serão reutilizados.

O apagamento criptográfico baseia-se na destruição definitiva das chaves criptográficas que protegem os dados armazenados, tornando o conteúdo inacessível mesmo que fisicamente preservado; é respaldado pela ISO/IEC 27701, conforme discutido por Chou, Albano e Almeida (2024), desde que as chaves estejam devidamente protegidas e não possam ser recuperadas.

Esse respaldo normativo é fundamental, uma vez que a ISO/IEC 27701 estabelece requisitos e diretrizes para a gestão da privacidade da informação, incluindo controles voltados ao ciclo de vida dos dados pessoais. Ao reconhecer o apagamento criptográfico como técnica válida, a norma legitima essa prática dentro de um sistema de governança da informação mais

amplo, assegurando que o procedimento esteja em conformidade com padrões internacionais de segurança e privacidade.

Dessa forma, o que Chou; Albano e Almeida (2024) destacam ganha relevância não apenas teórica, mas também prática, ao estar alinhado a um *framework* de reconhecimento global, que orienta as organizações a demonstrar responsabilidade e conformidade regulatória no tratamento de dados.

Por fim, o apagamento lógico (*overwriting),* conforme o IDSC (2025), consiste na sobrescrita dos dados com padrões binários ou sequências aleatórias por meio de *softwares* certificados, impedindo sua restauração; é amplamente empregado em HDDs, SSDs e *Pendrive,* que serão reutilizados.

O IDSC destaca três métodos principais para alcançar essa sanitização, especificados no Quadro 7, que apresenta a descrição, as vantagens e as limitações de cada um deles.

Quadro 7 - Métodos de sanitização de dados em dispositivos de armazenamento

Método	Descrição	Vantagens	Limitações
Destruição física	Inutilização permanente do dispositivo, por trituração, desmagnetização, etc.	Garantia máxima de irreversibilidade.	Destrói o dispositivo, inviabilizando seu uso.
Apagamento criptográfico	Exclusão das chaves criptográficas que protegem os dados, tornando-os inacessíveis.	Processo rápido e menos destrutivo.	Os dados permanecem fisicamente no dispositivo; algumas normas não aceitam essa prática.
Apagamento de dados	Uso de *softwares* específicos que sobrescrevem os dados com padrões aleatórios de *bits*.	Permite a reutilização do dispositivo após o processo.	Pode apresentar falsos positivos; exige métodos eficazes para garantir eliminação definitiva.

Fonte: elaboração própria, 2025 a partir de IDSC, 2025.

A título de comparação, para um melhor entendimento, a destruição física pode ser entendida de forma análoga ao uso de trituradores de papel confidencial, ou seja, uma vez que o papel é destruído em partículas minúsculas, torna-se impossível reconstituir a informação original. Da mesma forma, ao triturar fisicamente um disco rígido ou desmagnetizá-lo, o dispositivo é permanentemente inutilizado e os dados se tornam irrecuperáveis.

Já o apagamento criptográfico seria como destrancar um cofre sem a chave, ou seja, os dados continuam existindo fisicamente, mas tornam-se inacessíveis por meios convencionais, uma vez que a chave de acesso (criptográfica) foi excluída. Apesar disso, o conteúdo permanece no dispositivo, o que levanta preocupações em contextos que exigem eliminação completa da informação.

Por fim, o apagamento de dados por sobrescrição é semelhante a pintar repetidamente uma lousa com tinta opaca até apagar todo o conteúdo anterior, portanto, o dado original ainda está ali, mas coberto por novas camadas de informação (bits aleatórios). Embora isso dificulte a recuperação, há casos em que vestígios ainda podem ser detectados, especialmente se o processo não for executado com *softwares* certificados.

Essas comparações evidenciam que a escolha do método de sanitização deve considerar fatores como o grau de sensibilidade das informações, as exigências legais e normativas da instituição e a possibilidade (ou não) de reutilização dos dispositivos. Em ambientes que lidam com dados extremamente sensíveis — como instituições financeiras, órgãos públicos e empresas de tecnologia —, a destruição física tende a ser o método mais adotado, justamente por garantir a eliminação total das informações.

Malik (2023) destaca que a eliminação de dados ainda pode apresentar falsos positivos, situação em que as informações parecem ter sido removidas com segurança, mas permanecem no dispositivo. Esse problema decorre da estrutura de armazenamento dos dispositivos e da complexidade do processo de exclusão, tornando essencial a adoção de métodos eficazes para garantir a eliminação definitiva dos dados.

De acordo com o Comitê de Segurança da Informação (CSI) da Universidade Federal do Rio Grande do Sul (Universidade Federal do Rio Grande do Sul, 2023), para garantir um descarte seguro de dispositivos de armazenamento de dados é essencial seguir procedimentos eficazes. Entre as medidas recomendadas estão a realização de cópias de segurança (*backup*) para preservar informações importantes e a sanitização das mídias, que, de acordo com a ISO/IEC 27040, refere-se ao processo de remoção segura dos dados armazenados, de modo a oferecer uma garantia razoável que essas informações não possam ser facilmente recuperadas ou reconstruídas. Esses passos são fundamentais para evitar a recuperação não autorizada de informações sensíveis e assegurar a proteção dos dados durante o processo de descarte.

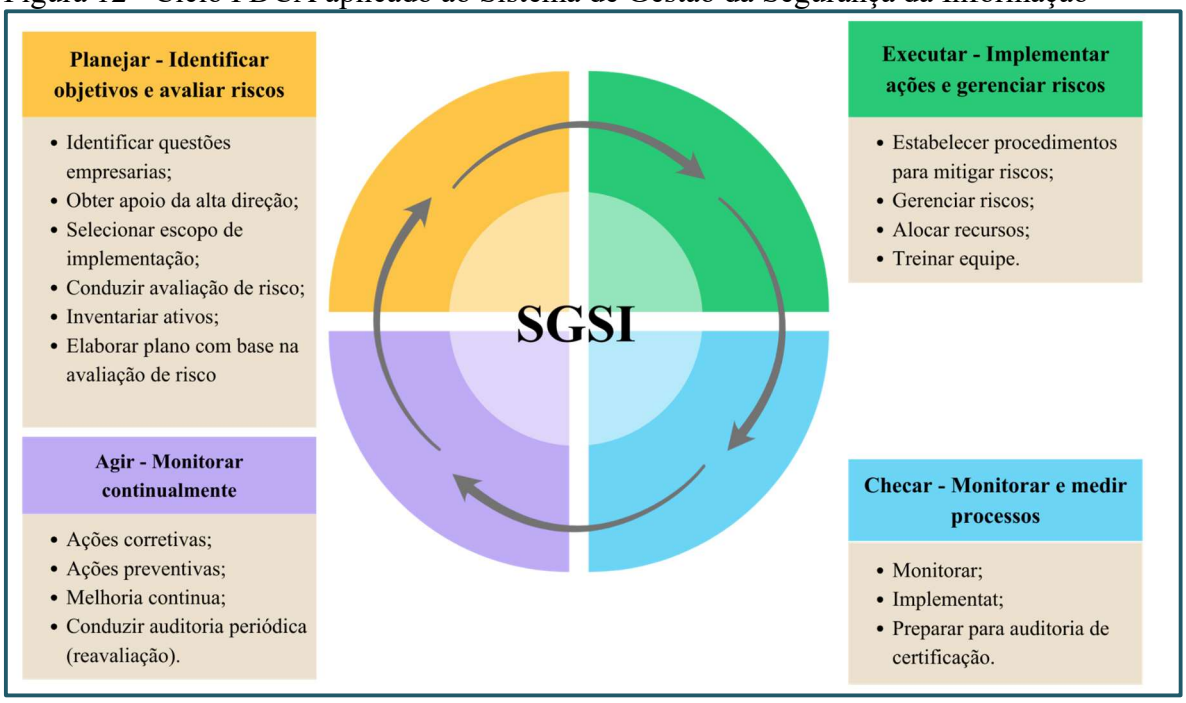
2.9 CICLO PDCA APLICADO AO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

O gerenciamento eficaz da segurança da informação exige não apenas a implementação de controles técnicos, mas também a adoção de metodologias de gestão que assegurem a melhoria contínua dos processos organizacionais. Nesse contexto, modelos consagrados de gestão da qualidade passaram a ser incorporados ao SGSI, conforme abordado por Magalhães (2021), oferecendo um arcabouço estruturado para planejamento, execução,

monitoramento e correção das práticas adotadas. Entre esses modelos destaca-se o ciclo PDCA, amplamente reconhecido por sua capacidade de sistematizar a busca por resultados consistentes, favorecer a integração entre áreas e fortalecer a cultura de prevenção e conformidade.

PDCA é uma sigla em inglês que representa um ciclo composto por quatro fases interligadas, utilizadas na gestão de processos com foco na melhoria contínua. As etapas são: ***P****lan* (planejar), ***D****o* (executar), ***C****heck* (verificar) e ***A****ct* (agir), explicadas na Figura 12, na configuração aplicada ao SGSI. Essa metodologia é utilizada na gestão de qualidade por empresas que buscam a eficácia nos processos, promovendo integração entre diferentes áreas organizacionais e consolidando práticas sustentáveis e seguras (Magalhães, 2021).

Figura 12 - Ciclo PDCA aplicado ao Sistema de Gestão da Segurança da Informação



Fonte: elaboração própria, 2025 adaptada de Magalhães, 2021.

Magalhães (2021) descreve cada uma dessas etapas do PDCA, destacadas neste estudo de forma sintética, no ponto de vista da aplicação organizacional:

- *Plan* – Fase de planejamento é aquela em que são identificados os objetos e os objetivos a serem monitorados e alcançados, além da confirmação do apoio da alta gestão. Também se define o escopo do sistema, definindo os locais onde será aplicado, bem como quais processos serão considerados. Nesta fase, deve-se ser realizada uma análise inicial para identificar e avaliar os riscos.

- *Do* – Fase de execução corresponde à implementação das ações definidas na etapa de planejamento, com foco no gerenciamento e tratamento dos riscos, bem como na adoção de políticas e procedimentos operacionais. Para a eficácia desta etapa, é fundamental garantir a capacitação e o envolvimento da equipe, além da alocação de recursos financeiros e estruturais.
- *Check* - Fase de verificação é o momento em que a organização deve monitorar e avaliar continuamente a eficácia das ações implementadas, permitindo a identificação de falhas que possam comprometer os resultados esperados, possibilitando possíveis melhorias. Além disso, essa etapa inclui as auditorias de certificação.
- *Act* – Fase Agir é a etapa na qual a organização realiza auditorias de reavaliações periódicas com o objetivo de verificar se o sistema de gestão contínua eficaz e alinhado às metas do planejamento. Caso necessário, deverão ser tomadas ações corretivas, que visam eliminar as causas de não conformidades identificadas, e ações preventivas, que têm como foco evitar a ocorrência de possíveis falhas futuras.

Essas fases, segundo Magalhães (2021), expressam o princípio da melhoria contínua, onde os processos são constantemente aprimorados, promovendo uma gestão proativa, resiliente e alinhada com as demandas legais, tecnológicas e sociais. Portanto, a adoção dessa metodologia pelas organizações facilita a identificação precoce de riscos e a implementação de melhorias contínuas, contribuindo para a redução de punições legais e fortalecendo a confiança de clientes e fornecedores. Permitindo, dessa forma, que as organizações não somente corrijam falhas, mas também aprendam com elas, aprimorando constantemente seus processos de forma eficaz.

A metodologia PDCA, portanto, é utilizada nas organizações com o objetivo de alinhar as estratégias empresariais à melhoria dos resultados, promovendo, ao mesmo tempo, o aperfeiçoamento contínuo dos processos. Ela também é conhecida como Ciclo da Qualidade, por auxiliar na identificação e resolução de problemas internos, com base em uma abordagem estruturada que envolve ruptura e controle (Gomes Filho; Gasparotto, 2019).

Segundo Brito e Brito (2020), o uso contínuo do PDCA na gestão de processos tem mostrado bons resultados, principalmente por facilitar a análise de dados e prevenir falhas recorrentes. A metodologia, composta por fundamentos básicos da administração, apresenta uma estrutura prática, acessível e aplicável em diferentes tipos de organizações. Sousa e Loos (2020) apontam que essa ferramenta permite um controle eficaz dos processos, contribuindo diretamente para a garantia da qualidade, já que suas etapas estão voltadas à detecção de erros

e à proposição de soluções. A partir desse movimento, a repetição de falhas tende a diminuir, abrindo espaço para a consolidação de novos padrões operacionais.

Gomes Filho e Gasparotto (2019), Sousa e Loos (2020) e Magalhães (2021) chamam atenção para o caráter contínuo do ciclo (cíclico e permanente), que se repete sempre que necessário até que os objetivos estabelecidos sejam plenamente atingidos. Por isso, o PDCA é amplamente utilizado em programas e práticas voltadas à melhoria constante, sendo valorizado justamente por sua natureza cíclica, adaptável e centrada no controle de processos.

Essa lógica de melhoria contínua proposta pelo ciclo PDCA mostra-se especialmente pertinente quando aplicada à gestão do ciclo de vida dos EEE, desde o momento do uso até o descarte final. No contexto da LGPD e da PNRS, adotar práticas organizadas, controladas e interativas, como as do PDCA, permite que empresas implementem rotinas eficientes de *backup*, armazenagem segura, sanitização de dados e descarte ambientalmente responsável. Ao integrar planejamento, execução, verificação e ajustes sistemáticos, é possível alinhar a proteção de dados pessoais ao cumprimento das normas ambientais, promovendo uma cultura organizacional comprometida tanto com a segurança da informação quanto com a sustentabilidade.

3 METODOLOGIA DA PESQUISA

A metodologia adotada neste estudo delineia os caminhos teórico-práticos percorridos para responder à problemática proposta e alcançar os objetivos estabelecidos. Fundamentando-se em Gil (2022), compreende-se que a definição criteriosa dos métodos e procedimentos é indispensável para garantir a coerência interna do trabalho, a validade dos resultados obtidos e a aplicabilidade das soluções apresentadas. Assim, a estrutura metodológica foi organizada de modo a articular a reflexão conceitual e normativa com a observação e a análise das práticas institucionais, permitindo a elaboração fundamentada de um Manual de Boas Práticas voltado ao descarte seguro e sustentável de ativos de tecnologia da informação.

O Manual de Boas Práticas pode ser entendido como um documento formal que reúne procedimentos, diretrizes e recomendações destinados a orientar a execução de atividades de forma padronizada, eficiente e em conformidade com requisitos legais e normativos.

Na área da SI, por exemplo, as normas da família ISO/IEC 27000 (como a ISO/IEC 27001 e a ISO/IEC 27002) oferecem diretrizes para a criação de políticas e controles que podem ser traduzidos em manuais práticos de gestão. Já no campo da qualidade, a ABNT NBR 9001 estabelece requisitos para sistemas de gestão, nos quais a documentação de processos é fundamental para garantir padronização e melhoria contínua.

3.1 ABORDAGEM INTERDISCIPLINAR DA PESQUISA

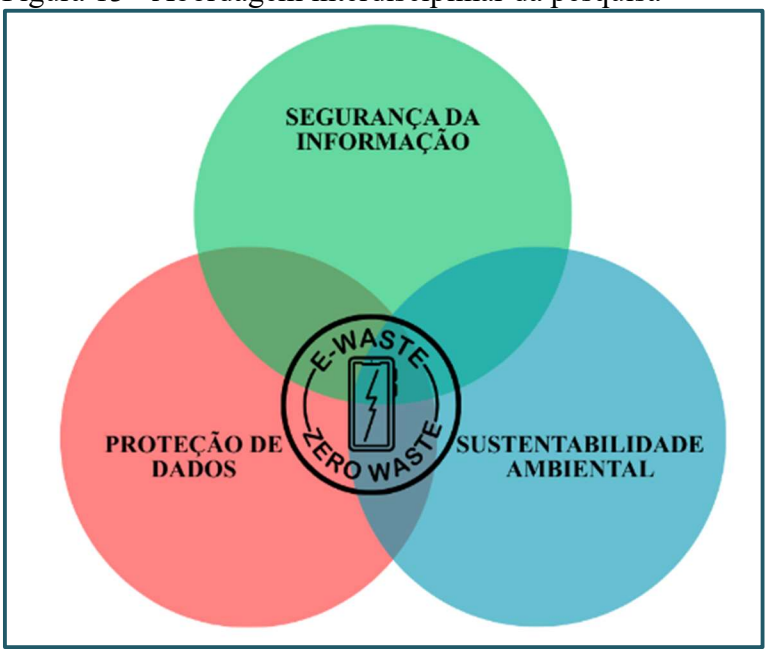
Esta pesquisa adotou uma abordagem interdisciplinar, conforme proposta por Repko e Szostak (2020), que a concebe como um processo intelectual e metodológico voltado à integração de conhecimentos, conceitos, métodos, fenômenos e teorias de diferentes áreas do saber, com vistas à construção de uma compreensão abrangente e contextualizada de problemas complexos. De acordo com o autor, a interdisciplinaridade vai além da justaposição de saberes: ela requer uma articulação crítica e intencional entre os diversos campos envolvidos, permitindo que tensões epistemológicas e lacunas conceituais sejam analisadas, reinterpretadas e superadas.

Repko e Szostak (2020) enfatizam, também, que essa abordagem se torna especialmente valiosa em situações nas quais os limites disciplinares tradicionais não são suficientes para dar conta da totalidade do fenômeno investigado. Como este estudo, no qual a opção pela interdisciplinaridade mostrou-se não apenas pertinente, mas necessária, dada a natureza multifacetada do problema analisado, que envolve simultaneamente questões jurídicas,

técnicas, ambientais e organizacionais. Portanto, há uma integração entre áreas como Direito, Segurança da Informação e Gestão Ambiental, que possibilitou uma compreensão dos desafios associados ao descarte de ativos tecnológicos e à proteção de dados, além de subsidiar a formulação de propostas que considerem, de forma equilibrada, os aspectos legais, operacionais e socioambientais implicados na temática.

No contexto deste estudo, a interdisciplinaridade foi essencial para abordar questões que envolvem simultaneamente os campos da proteção de dados pessoais, da segurança da informação (SI) e da sustentabilidade ambiental (Figura 13). O descarte de dispositivos de armazenamento de dados — *e-lixo* — demanda conhecimentos integrados sobre normativas legais (como a LGPD e a PNRS), padrões técnicos internacionais (como as normas da família ISO/IEC 27000), práticas de gestão de TI, além de princípios de responsabilidade socioambiental.

Figura 13 - Abordagem interdisciplinar da pesquisa



Fonte: elaborado pelo autor, 2025.

A abordagem interdisciplinar, ilustrada na figura, destaca o *e-lixo* — que nesta pesquisa corresponde aos ativos contendo dados que serão descartados de forma correta — como ponto de convergência entre os campos da Proteção de Dados, Segurança da Informação e Sustentabilidade Ambiental. O descarte inadequado desses ativos pode comprometer tanto a segurança e a privacidade das informações armazenadas quanto gerar impactos ambientais significativos. Por isso, o tratamento do *e-lixo* exige medidas que assegurem a eliminação

segura dos dados, combinadas com práticas ambientalmente responsáveis e em conformidade com as normas técnicas de segurança da informação.

A metodologia desta pesquisa, portanto, possui abrangência interdisciplinar, integrando diferentes áreas do conhecimento para tratar de temas relacionados a segurança da informação e a sustentabilidade ambiental, exigindo conhecimentos técnicos específicos nas áreas de eletrônica, informática e gestão de ativos de TI, especialmente no que se refere ao funcionamento dos dispositivos de armazenamento, às técnicas de sanitização de dados e aos processos de descarte e destinação final de equipamentos.

3.2 NATUREZA APLICADA E TIPO DA PESQUISA

A presente pesquisa classifica-se como aplicada, pois parte da reflexão teórica e normativa para propor uma solução prática voltada a contextos reais, qual seja a elaboração de um Manual de Boas Práticas para o Descarte Seguro e Sustentável de Ativos de Tecnologia da Informação. Conforme Gil (2022), a pesquisa aplicada visa não apenas ampliar o conhecimento, mas também produzir resultados utilizáveis em situações concretas, correspondendo diretamente ao objetivo deste trabalho.

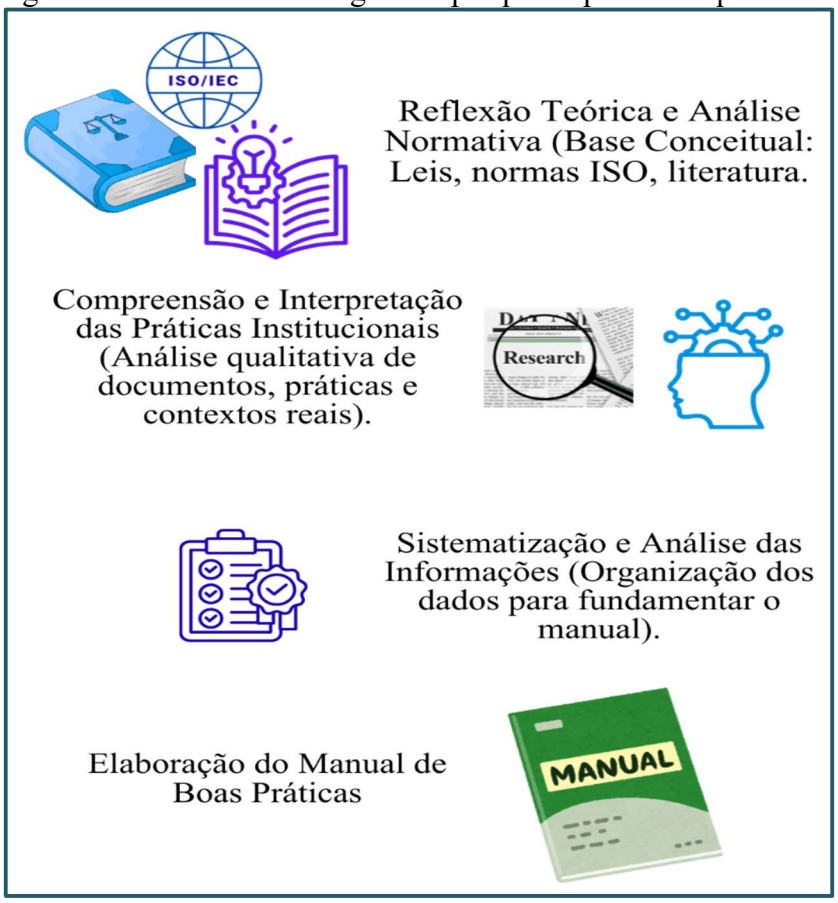
Quanto à abordagem, trata-se de uma pesquisa qualitativa, com características descritivas e analíticas. Gil (2022) destaca que a abordagem qualitativa é apropriada para estudos que buscam compreender, interpretar e descrever fenômenos em seus contextos naturais, considerando a complexidade das situações e as múltiplas dimensões envolvidas. No presente estudo, a qualitatividade justifica-se pelo interesse em compreender e interpretar as práticas institucionais, relacionadas ao descarte de ativos de tecnologia da informação que contenham dispositivos de armazenamento de dados. Já o caráter descritivo e analítico manifesta-se na sistematização das práticas existentes e na proposição de diretrizes fundamentadas em legislações, normas técnicas e literatura especializada.

O produto técnico resultante desta pesquisa, o manual, busca orientar instituições públicas e privadas quanto ao alinhamento de suas condutas às exigências legais previstas na LGPD, na PNRS e nas normas ISO/IEC da família 27000, especialmente no que se refere à gestão do ciclo de vida da informação armazenada em ativos tecnológicos.

A Figura 14 representa o fluxo metodológico da pesquisa estruturado de forma aplicada e qualitativa. O diagrama ilustra as cinco etapas que orientaram o desenvolvimento do trabalho, desde a reflexão teórica e análise normativa até a aplicação prática do manual. Esse percurso

metodológico evidenciou o compromisso da pesquisa com a integração entre teoria e prática, reforçando seu caráter propositivo e orientado à transformação de realidades institucionais.

Figura 14 - Fluxo metodológico da pesquisa aplicada – qualitativa



Fonte: elaboração própria, 2025.

Dessa forma, a metodologia adotada se configura como um instrumento fundamental para a concretização dos objetivos da pesquisa, ao garantir a articulação entre os fundamentos teóricos e as práticas institucionais, que subsidiaram o estudo, a formulação dos fluxogramas (boas práticas) e, consequentemente, na elaboração do Manual de Boas Práticas.

3.3 LEVANTAMENTO BIBLIOGRÁFICO

Realizou-se o levantamento bibliográfico por meio de buscas em bases de dados amplamente reconhecidas, como o *Google* Acadêmico, Minha Biblioteca e o Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), priorizando publicações dos últimos dez anos, assim como obras anteriores que se mostrassem relevantes para complementar o referencial teórico.

No contexto brasileiro, é importante destacar que uma parcela significativa da comunidade acadêmica tem acesso gratuito aos principais artigos científicos, devido ao investimento da CAPES. Esse acesso é facilitado pela Comunidade Acadêmica Federada (CAFe), que possibilita a utilização de *login* e senha institucionais para acessar remotamente o conteúdo assinado do Portal de Periódicos da CAPES (Brasil, 2025).

Os descritores utilizados nas buscas bibliográficas, tanto em português quanto em inglês, foram cuidadosamente selecionados para refletir a natureza interdisciplinar da pesquisa, abordando simultaneamente os campos da proteção de dados, segurança da informação e sustentabilidade ambiental. Os termos utilizados, portanto, nas bases de dados foram:

- "descarte de ativos de armazenamento de dados" / *data storage asset disposal*: utilizado para identificar estudos que abordem a fase final do ciclo de vida de dispositivos eletrônicos contendo dados sensíveis, como HDs, SSDs e dispositivos móveis.
- "proteção de dados pessoais" / *personal data protection*: empregado para localizar publicações jurídicas e técnicas que tratam da segurança jurídica dos dados no contexto da LGPD e regulamentações correlatas.
- "sanitização de dispositivos" / *device sanitization*: termo técnico voltado à busca por normas e procedimentos de eliminação segura de dados.
- "resíduos sólidos" / *solid waste*: termo associado ao campo da sustentabilidade ambiental e da Política Nacional de Resíduos Sólidos, especialmente quanto ao descarte de eletrônicos.
- "vazamentos de dados" / *data leaks*: utilizado para mapear publicações sobre incidentes de segurança, riscos e vulnerabilidades relacionados à má gestão de informações digitais.
- "normas ISO" / *ISO standards*: buscado para identificar padrões internacionais que regulamentam a segurança da informação e o tratamento de dados sensíveis (como as famílias ISO/IEC 27000).
- "*backup* de dados" / *data backup*: termo voltado à recuperação e proteção preventiva de informações armazenadas, também relevante ao ciclo de vida dos dados.

Os critérios de inclusão adotados foram: 1. Idioma: publicações em português ou inglês, garantindo maior acessibilidade e abrangência da pesquisa; 2. Relevância do tema: trabalhos que abordassem diretamente métodos e práticas de descarte de ativos de armazenamento de dados, com ênfase na conformidade com a LGPD e a PNRS; 3. Atualidade: publicações compreendidas entre os anos de 2015 e 2025, assegurando que as informações estivessem

atualizadas e pertinentes ao contexto atual de segurança da informação e gestão de resíduos. Portanto, foram critérios de exclusão estudos que não tinham acesso gratuito, duplicados, não estavam completos ou não atendiam aos critérios de inclusão.

3.4 ELABORAÇÃO DO PRODUTO TÉCNICO (MANUAL)

A metodologia adotada para a construção do manual fundamentou-se na análise documental de legislações nacionais e internacionais, normas técnicas internacionais e literatura especializada, complementada pela investigação de práticas institucionais reais, caracterizando-se como um estudo de caso aplicado. Essa combinação metodológica possibilitou a formulação de orientações claras e fundamentadas, voltadas a instituições públicas e privadas que buscam garantir a conformidade com a LGPD, a PNRS e as diretrizes das normas da família ISO/IEC 27000.

A elaboração do manual também foi orientada pela construção de seis fluxogramas ilustrativos, fundamentados no referencial teórico e normativo sistematizado ao longo da pesquisa. Esses fluxogramas foram desenvolvidos com o uso do *software* gratuito *Bizagi Modeler* (versão 4.2.0.003), escolhido por sua interface intuitiva, facilidade de uso e compartilhamento com a notação *Business Process Model and Natation* (BPMN) – padrão amplamente utilizado para representar graficamente processos de negócios e operacionais. A adoção dessa ferramenta permitiu a representação clara, padronizada e tecnicamente adequada dos procedimentos, tornando os fluxogramas acessíveis tanto aos profissionais da área técnica quanto aos gestores e equipes administrativas envolvidas com a governança de dados e a gestão de ativos de TI.

Os fluxogramas foram concebidos com o objetivo de facilitar a visualização sequencial e prática dos procedimentos relativos à gestão de ciclo de vida dos dispositivos de armazenamento de dados, incluindo as etapas de: (1) armazenamento; (2) *backup*; (3) sanitização; e (4) descarte (5) PDCA. Essa abordagem metodológica contribui para que as instituições compreendam e implementem cada etapa de maneira padronizada, transparente e alinhada às exigências legais e normativas vigentes no Brasil.

O Quadro 8 apresenta a estrutura que guiou a organização do manual, detalhando as seções temáticas e os conteúdos prioritários desenvolvidos em cada uma delas. A disposição dos temas seguiu uma lógica didática e funcional, conforme os padrões da Associação Brasileira de Normas Técnicas (ABNT NBR 14724:2024), de modo a garantir clareza, coerência e aplicabilidade prática. A estruturação do manual visou, assim, favorecer sua adoção por

organizações que desejam implementar práticas seguras, eficazes e sustentáveis no descarte de ativos de Tecnologia da Informação.

Quadro 8 - Estrutura do Manual de Boas Práticas para o Descarte de Ativos de TI

Seção	Descrição
Introdução	Apresenta os principais conceitos relacionados à LGPD, à PNRS e às normas da família ISO/IEC 27000 aplicáveis ao descarte de dispositivos de armazenamento de dados.
Procedimentos de Armazenamento	*Fluxograma 1* – representa a sequência dos passos essenciais para garantir que os dados armazenados estejam protegidos, organizados e em conformidade com as normas de segurança e privacidade (LGPD e normas ISO/IEC 27000).
Métodos de *Backup*	Aborda práticas seguras de *backup*, visando garantir a integridade e disponibilidade das informações. Inclui *Fluxograma 2*, que contempla as etapas de uma política de *backup* de dados alinhada à LGPD e às normas ISO/IEC.
Procedimentos de Sanitização	Descreve técnicas de sanitização de dados que asseguram a impossibilidade de recuperação das informações descartadas. Inclui *Fluxograma 3,* com as etapas de uma política de sanitização para dispositivos de armazenamento de dados.
Procedimentos de Descarte	Detalha as etapas para o descarte sustentável de ativos de TI, conforme as exigências ambientais e legais. Inclui *Fluxograma 4,* com uma política de descarte em conformidade com a LGPD, PNRS e normas ISO/IEC.
PDCA	*Fluxograma 5:* garante a avaliação periódica, correção de falhas e atualização das práticas conforme evolução tecnológica e regulatória.
Penalidades e Gestão de Riscos	Explica os riscos da não conformidade com a LGPD e a PNRS, incluindo sanções administrativas, multas e implicações legais.
Conscientização	Propõe estratégias de sensibilização ambiental e digital para promover uma cultura institucional de responsabilidade no descarte de ativos de TI.
Avaliação e Atualização	Estabelece um plano de revisão periódica para manter o conteúdo atualizado diante de mudanças legais, normativas ou tecnológicas.
Anexo – Fluxograma Geral	Apresenta o *Fluxograma 6,* que contempla todas as etapas de uma política de armazenamento de dados, desde o recebimento até o descarte, integrando os princípios da LGPD e normas ISO/IEC 27000.

Fonte: elaboração própria, 2025.

Além dessas etapas, é importante destacar que o Manual de Boas Práticas, elaborado neste estudo, apresenta características que o diferenciam significativamente de outros manuais disponíveis na literatura e no contexto institucional brasileiro. Enquanto muitos documentos técnicos abordam de forma isolada aspectos ambientais, jurídicos ou de segurança da informação, o presente manual adota uma perspectiva integrada, articulando simultaneamente a LGPD a PNRS e as normas técnicas internacionais da família ISO/IEC 27000. Essa convergência normativa possibilita uma abordagem completa do ciclo de vida da informação armazenada em ativos tecnológicos, contemplando desde a coleta e o armazenamento até o backup, a sanitização e o descarte ambientalmente adequados.

A integração entre essas três dimensões, constitui o principal diferencial do manual, fornecendo controles técnicos internacionalmente reconhecidos que orientam a implementação, auditoria e validação dos procedimentos. Assim, o manual proposto avança em relação a documentos tradicionais por oferecer uma visão holística e aplicável às organizações que

necessitam alinhar governança de dados, conformidade legal e responsabilidade socioambiental.

Outro elemento distintivo refere-se à utilização de fluxogramas que permite representar processos de forma clara, padronizada e compatível com metodologias de gestão amplamente utilizadas no setor público e privado. Essa opção metodológica contribui para tornar o manual acessível não apenas a especialistas em tecnologia, mas também a gestores, equipes administrativas e responsáveis por políticas institucionais.

A elaboração e validação do Manual de Boas Práticas para o Descarte Seguro e Sustentável de Ativos de Tecnologia da Informação seguiu um protocolo técnico que incluiu revisão por especialistas das áreas de Sistemas de Informação, Direito e Gestão Ambiental, assegurando a qualidade, coerência normativa e aplicabilidade prática do conteúdo proposto. Simultaneamente, a elaboração das figuras foi viabilizada por meio do *software* Canva, acessado mediante assinatura mensal, o que assegurou a padronização gráfica e qualidade visual dos elementos produzidos. As edições textuais, por sua vez, foram executadas por meio das plataformas *Google Drive* e *Microsoft Office*, concedidas gratuitamente pela UFTM mediante login e senha institucionais.

Após a defesa da dissertação, o manual foi encaminhado para depósito legal na Biblioteca Nacional, conforme os critérios da instituição, reforçando sua credibilidade e autenticidade como produto técnico-científico e inserido como apêndice nesta dissertação, a qual será hospedada na Biblioteca Digital de Teses e Dissertações (BDTD) da UFTM, garantindo acesso à comunidade acadêmica.

Por seu caráter aplicado, o produto final visa não apenas orientar práticas seguras no descarte de dispositivos de armazenamento de dados, mas também contribuir para o aprimoramento das políticas públicas relacionadas à governança de dados e à gestão sustentável de resíduos tecnológicos, em conformidade com a LGPD, a PNRS e as diretrizes da família de normas ISO/IEC 27000.

4 RESULTADOS E DISCUSSÃO

Nesta seção, apresentam-se os resultados da pesquisa de natureza documental, bibliográfica e descritiva, cujo objetivo foi identificar métodos seguros, sustentáveis e juridicamente embasados para o descarte de equipamentos que contenham dispositivos de armazenamento de dados, conforme os princípios estabelecidos pela LGPD, pela PNRS e pelas diretrizes normativas da família ISO/IEC 27000.

A Figura 15 ilustra a sequência metodológica empregada na construção dos resultados. A trajetória inicia-se com o levantamento teórico e normativo, que embasou a elaboração de fluxogramas de orientação sobre o ciclo de vida da informação em ativos de armazenamento. Em seguida, esses fluxogramas foram submetidos à análise interdisciplinar de especialistas das áreas de SI, Direito e Meio Ambiente, resultando em ajustes e validações fundamentais. O processo culmina na consolidação de modelos gráficos aprimorados, que integram o manual de boas práticas desenvolvido como produto técnico desta dissertação.

Figura 15 - Sequência de procedimentos dos resultados alcançados

Fonte: elaborado pelo autor, 2025.

Como principal produto da investigação, foram desenvolvidos seis fluxogramas que representam, de forma sistematizada e visual, as boas práticas associadas ao ciclo de vida da

informação e à gestão de ativos computacionais. Cinco fluxogramas têm foco temático e abordam etapas específicas, enquanto o sexto apresenta uma visão integrada de todo o processo. São eles:

(1) Procedimentos de Armazenamento de Dados;

(2) Procedimentos de *Backup* em Ativos contendo Dados;

(3) Procedimentos de Sanitização em Ativos contendo Dados;

(4) Procedimentos de Descarte em Ativos contendo Dados;

(5) PDCA Aplicado à Gestão de Ativos de Informação; e

(6) Visão Integrada de todo o processo.

A elaboração desses fluxogramas fundamenta-se na análise crítica das legislações e normas técnicas, aliada às boas práticas identificadas no levantamento bibliográfico. Cada fluxograma foi desenvolvido pelo pesquisador, com posterior validação técnica conduzida por especialistas técnicos convidados, sob a supervisão do orientador da pesquisa.

4.1 INTERLOCUÇÃO COM ESPECIALISTAS E VALIDAÇÃO TÉCNICA DOS FLUXOGRAMAS

A interlocução com os especialistas técnicos ocorreu de forma colaborativa, por meio de plataformas digitais de comunicação, o que possibilitou trocas dinâmicas, contínuas e interdisciplinares, pois há troca, diálogo e síntese entre os saberes das áreas. Essa estratégia contribuiu significativamente para o aprimoramento dos modelos elaborados, garantindo alinhamento com os marcos legais (LGPD e PNRS), as normas internacionais da família ISO/IEC 27000 e os princípios de sustentabilidade e segurança da informação que nortearam esta pesquisa.

Na validação técnica, conduzida por um especialista da área de informática, na primeira produção foi recomendado o uso da notação *American National Standards Institute* (ANSI)[43], com o objetivo de padronizar e tornar os fluxogramas mais claros e tecnicamente consistentes. Na segunda análise, uma de suas principais observações foi a presença recorrente do ciclo PDCA nos diagramas. Este fato motivou a sugestão de sua representação em um fluxograma específico, com enfoque na gestão periódica e na melhoria contínua.

[43] A sigla ANSI refere-se ao *American National Standards Institute*, responsável pela definição de padrões técnicos em diferentes áreas. No campo dos fluxogramas, a notação ANSI padroniza o uso de símbolos gráficos e convenções para representar processos, sistemas e fluxos de trabalho, facilitando a compreensão por profissionais de distintas áreas. O termo também se aplica a outros contextos, como a codificação de caracteres em sistemas computacionais (ANSI *code pages*) e normas para desenhos técnicos e projetos de engenharia.

Essa concepção de melhoria contínua e controle de processos, aplicada ao descarte de ativos contendo dados sensíveis, fundamentou-se nos estudos de Gomes Filho e Gasparotto (2019), que destacam a estrutura prática do PDCA como ferramenta de padronização de soluções; Sousa e Loos (2020), que reforçam seu papel no controle eficaz dos processos e na garantia da qualidade; Brito e Brito (2020), que apontam sua utilidade na análise de dados e prevenção de falhas recorrentes; e Magalhães (2021), que descreve cada etapa do ciclo sob a perspectiva organizacional, com ênfase na identificação de riscos e na promoção de uma gestão resiliente e proativa[44].

Durante a validação técnica dos fluxogramas, foi recomendada a inclusão de símbolos de decisão, com a finalidade de representar pontos críticos do processo onde podem ocorrer situações de não conformidade. Esses elementos visuais justificam-se por destacar momentos que exigem avaliação e tomada de decisão por parte da organização, reforçando a lógica de monitoramento contínuo, identificação de falhas e aplicação de medidas corretivas, conforme os princípios da melhoria contínua.

A validação jurídica, por um consultor técnico da área de Direito, mostrou-se fundamental para assegurar o alinhamento dos fluxogramas às exigências da LGPD e da PNRS. As orientações permitiram a interpretação correta de dispositivos legais, especialmente no que se refere às responsabilidades dos agentes de tratamento[45], aos cuidados exigidos antes do descarte de mídias e aos deveres de proteção e privacidade previstos no artigo 46[46] da LGPD, além do apontamento de outras leis específicas.

No âmbito ambiental, a especialista reforçou a importância de práticas alinhadas aos princípios da logística reversa e da responsabilidade compartilhada, conforme estabelecido pela PNRS. Foram enfatizadas as exigências legais para que os resíduos eletroeletrônicos sejam

---

[44] Devido à necessidade de elaboração de um fluxograma específico com a lógica do ciclo PDCA, tornou-se necessário ampliar o levantamento bibliográfico, incorporando três estudos adicionais: Gomes Filho e Gasparotto (2019), Sousa e Loss (2020) e Brito e Brito (2020). Esses autores foram incluídos com o objetivo de aprofundar a fundamentação teórica sobre a aplicação prática do PDCA na gestão de processos organizacionais, especialmente no que tange à melhoria contínua, à padronização de rotinas e à prevenção de falhas. Além desses, manteve-se como base o estudo de Magalhães (2021), já presente no levantamento inicial, cuja contribuição foi essencial para descrever detalhadamente cada etapa do ciclo (Planejar, Executar, Verificar e Agir), consolidando o embasamento necessário para a construção conceitual e técnica do fluxograma.

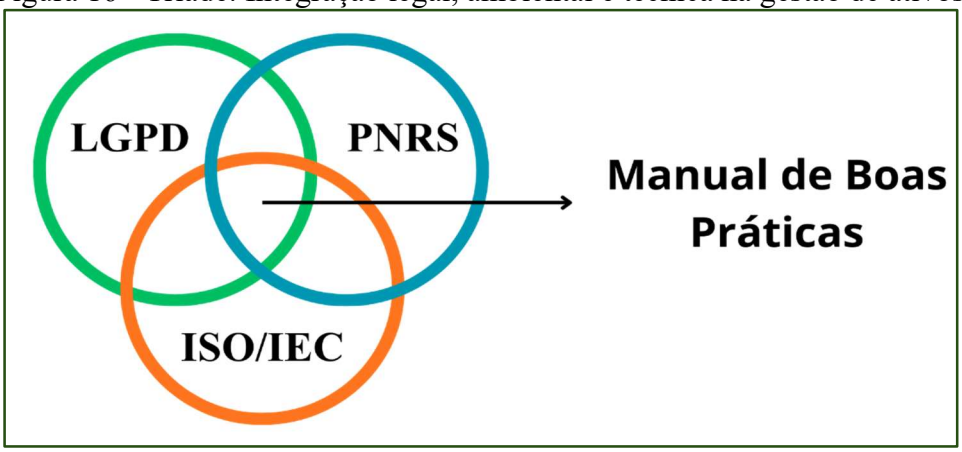
[45] Conforme a LGPD (Lei nº 13.709/2018, art. 5º, incisos VI e VII), os agentes de tratamento são o controlador e o operador. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Já o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador. Ambos possuem responsabilidades distintas, estabelecidas ao longo da legislação, especialmente no que se refere à segurança, à transparência e à prevenção de danos no tratamento de dados pessoais.

[46] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

destinados exclusivamente a empresas licenciadas, certificadas e cadastradas em órgãos ambientais, garantindo rastreabilidade, segurança e conformidade ambiental.

Diante de todo o processo de validação, os resultados consistiram nos fluxogramas em conformidade com a LGPD, em observância aos princípios da PNRS e com as boas práticas definidas pelas normas da família ISO/IEC 27000, que, constituem uma tríade de integração (Figura 16), que nesta pesquisa mostrou-se essencial para garantir que o descarte de ativos tecnológicos seja conduzido de forma segura, responsável e juridicamente adequada.

Figura 16 - Tríade: Integração legal, ambiental e técnica na gestão de ativos



Fonte: elaboração própria, 2025.

É importante ressaltar que esta metodologia de análise interdisciplinar foi fundamental para que houvesse uma lógica mais coerente na dinâmica do estudo. Primeiro, porque o descarte seguro de equipamentos com dispositivos de armazenamento de dados, assume papel central na preservação do meio ambiente e na proteção de informações sensíveis. A LGPD impõe a adoção de medidas técnicas e administrativas que assegurem a integridade, a confidencialidade e a disponibilidade dos dados, inclusive após seu uso, sendo o descarte inadequado passível de sanções e responsabilizações (Brasil, 2018).

Segundo, porque a PNRS estabelece as bases para a destinação final ambientalmente adequada, estabelecidas no artigo 9º, a ordem de prioridade na gestão de resíduos sólidos: a não geração, a redução, a reutilização e a reciclagem de resíduos, e, somente em último caso, a disposição final (Brasil, 2010).

Desta forma, os riscos jurídicos e ambientais se entrelaçam, exigindo práticas que articulem os princípios da sustentabilidade e as diretrizes da segurança da informação, em consonância com a PNRS e a LGPD. Como destacam Schaun *et al*. (2023), a gestão de REEE requer uma abordagem integrada, que considere simultaneamente os princípios da sustentabilidade e da segurança da informação.

Por último, as normas internacionais da família ISO/IEC 27000 complementam esse quadro ao estabelecer diretrizes voltadas à gestão segura da informação como ativo essencial das organizações. A norma ISO/IEC 27002 orienta sobre políticas de *backup* e medidas de proteção das informações, enquanto a ISO/IEC 27001 trata da gestão de ativos e dos controles de acesso no contexto de um SGSI (Magalhães, 2021). A ISO/IEC 27040 aborda a sanitização, o controle de acesso, a autenticação e a criptografia (SNIA, 2018), ao passo que a ISO/IEC 27701 reforça a necessidade de políticas voltadas à privacidade ao longo de todo o ciclo de vida da informação (Diniz; Diniz, 2019).

Pode-se considerar que, nesta etapa, os três especialistas convidados pela análise e validação dos fluxogramas desempenharam um papel fundamental no processo de revisão crítica e de adequação metodológica. Suas contribuições, advindas de diferentes áreas do conhecimento, possibilitaram o aprimoramento técnico, jurídico e ambiental dos modelos elaborados, assegurando que os procedimentos representados nos fluxogramas estejam não apenas em conformidade com os marcos normativos, mas também ajustados às demandas reais das organizações que lidam com dados sensíveis.

Assim, os fluxogramas validados representam instrumentos eficazes para orientar a gestão segura e sustentável dos dispositivos de armazenamento de dados, reforçando o compromisso com a proteção da informação e a responsabilidade socioambiental. Dessa forma, cada fluxograma foi cuidadosamente elaborado e apresentado a seguir, com suas respectivas explicações, fundamentações legais e normativas, evidenciando sua relevância para a composição do Manual de Boas Práticas.

4.2 FLUXOGRAMAS ELABORADOS POR PROCEDIMENTO

Nesta subseção, são apresentados os seis fluxogramas desenvolvidos com base nas etapas que compõem o ciclo de vida de ativos de armazenamento de dados, abrangendo o armazenamento, o *backup*, a sanitização, o descarte e a gestão contínua por meio do ciclo PDCA. Cada fluxograma representa uma etapa específica do processo e está acompanhado de uma explicação, fundamentação normativa e justificativa técnica, a fim de evidenciar sua aplicabilidade prática e sua contribuição para o Manual de Boas Práticas.

O fluxograma é uma técnica gráfica de representação sequencial de atividades, que permite visualizar, de forma ordenada e lógica, as etapas envolvidas na execução de um processo, onde mesmo indivíduos com conhecimentos básicos conseguem acompanhar o processo, servindo também como guia de orientação para novos colaboradores (Silva, 2020).

Essa ferramenta utiliza símbolos padronizados para descrever operações, pontos de decisão e os responsáveis por cada etapa, promovendo uma melhor compreensão do fluxo de trabalho e facilitando sua análise (Cury, 2015). Segundo Silva (2020), trata-se da representação das operações de um processo, cuja estrutura se baseia em uma sequência de atividades interdependentes, organizadas com o objetivo de traduzir graficamente a progressão de ideias e ações que compõem um procedimento técnico ou operacional.

De acordo com Silva, 2020, o fluxograma pode ser compreendido como um gráfico que representa a sequência regular de qualquer atividade, documento ou produto, possibilitando o mapeamento desde a origem até o destino das informações processadas. Embora alguns símbolos ainda apresentem variações em seu uso, há uma compreensão consolidada quanto à função de cada elemento gráfico. A autora ressalta ainda que essa ferramenta pode ser aplicada tanto em sistemas simples quanto em processos organizacionais complexos, contribuindo para a localização de falhas, a clareza de informações e a compreensão rápida de alterações ou melhorias.

Entre suas principais finalidades, destaca-se a capacidade de tornar os processos mais claros e acessíveis, contribuindo para a identificação de falhas, gargalos, redundâncias e oportunidades de melhoria (Silva, 2020). O uso de fluxogramas permite também um melhor entendimento do funcionamento interno das organizações, ao evidenciar os relacionamentos entre os diversos setores e subprocessos. Essa visualização facilita a tomada de decisões gerenciais, pois promove uma abordagem objetiva e direta sobre o modo como as atividades são executadas (Cury, 2015).

Dessa forma, compreende-se o fluxograma não apenas como um instrumento de gestão e racionalização do trabalho, mas também como um mecanismo de documentação e memória institucional. Portanto, quando aplicados à representação de procedimentos organizacionais, como ocorre nesta pesquisa, os fluxogramas ganham especial relevância. O conceito de processo, nesse contexto, pode ser entendido como um conjunto estruturado de atividades ou tarefas que, ao receberem determinados insumos — como materiais, dados, pessoas, equipamentos e métodos —, resultam na geração de produtos ou serviços com valor agregado. Essa lógica processual está presente em praticamente todas as ações realizadas por uma organização, uma vez que qualquer trabalho que envolva transformação ou entrega de valor se caracteriza como processo organizacional (Cury, 2015).

Portanto, ao representar visualmente esses processos, os fluxogramas contribuem não apenas para o controle e padronização das atividades, mas também para o aperfeiçoamento contínuo da gestão, especialmente em contextos que exigem conformidade normativa, como o

tratamento de dados pessoais, a segurança da informação e a sustentabilidade ambiental. Nesse sentido, os fluxogramas a seguir detalham as etapas fundamentais do ciclo de vida dos ativos de informação, acompanhados de suas respectivas fundamentações normativas.

A justificativa para a construção e aplicação dos fluxogramas nesta pesquisa encontra respaldo na necessidade de implementar políticas internas que promovam o controle efetivo dos processos organizacionais. Nesse sentido, a LGPD, em seu artigo 50, prevê que os agentes de tratamento podem formular regras de boas práticas e de governança, a fim de estabelecer normas de segurança, padrões técnicos e mecanismos internos de supervisão e mitigação de riscos, entre outros aspectos relevantes ao tratamento de dados pessoais (Brasil, 2018).

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Ainda conforme o artigo 50 da LGPD, os programas de boas práticas e governança devem levar em consideração a natureza e a sensibilidade dos dados tratados, o escopo das operações realizadas e o grau de risco envolvido (Brasil, 2018). Tais programas podem, portanto, incluir, entre outras medidas, ações educativas, planos de resposta a incidentes e mecanismos de monitoramento contínuo, reforçando a necessidade de uma abordagem preventiva e sistemática no tratamento de dados pessoais.

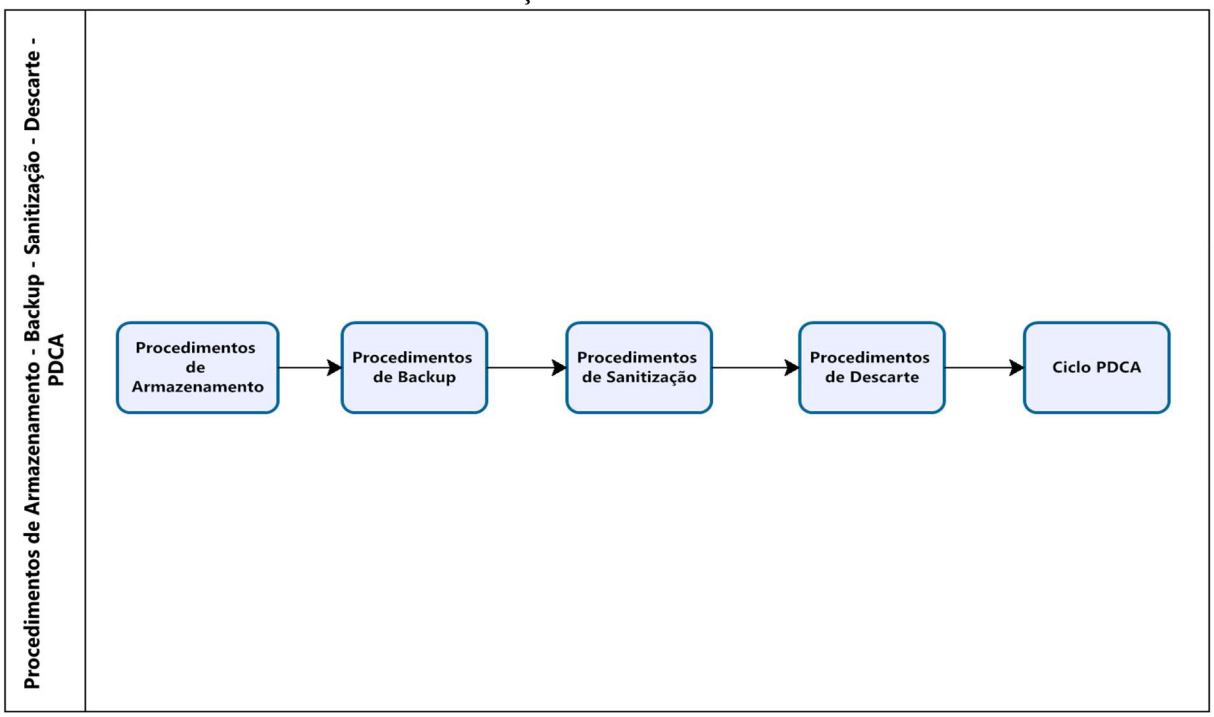
Nesse contexto, os fluxogramas apresentados nesta pesquisa foram elaborados com base em um referencial teórico sólido, além de orientações técnicas fornecidas por especialistas nas áreas de SI, Direito e Gestão Ambiental. O objetivo central de sua construção foi representar, de maneira clara, funcional e normativa, os procedimentos mais críticos relacionados ao ciclo de vida dos ativos de informação, especialmente no que se refere ao armazenamento e descarte seguro de dados.

A estruturação visual desses fluxogramas contribui para o alinhamento institucional às exigências legais, funcionando também como base para a elaboração do Manual de Boas Práticas, produto técnico vinculado a esta dissertação. O primeiro fluxograma, por exemplo, descreve o processo completo no manuseio de ativos que contenham dados sensíveis, abrangendo os procedimentos de armazenamento, *backup*, sanitização, descarte e a aplicação

da ferramenta PDCA, evidenciando o compromisso com a melhoria contínua e a conformidade normativa.

De forma sintética, a Figura 17 apresenta as cinco etapas fundamentais que compõem o ciclo de vida dos ativos de armazenamento de dados. Cada fase é disposta de maneira sequencial, evidenciando a lógica processual adotada para assegurar a rastreabilidade, a segurança da informação e a conformidade legal no tratamento de dados sensíveis, desde sua utilização até o descarte final.

Figura 17 - Manuseio de Ativos contendo dados por procedimento: armazenamento - *backup* – Sanitização – Descarte – PDCA



Fonte: elaboração própria, 2025.

Essa visão integrada evidencia a importância de se compreender os processos como partes interdependentes de um sistema organizacional orientado à melhoria contínua. O uso do Ciclo PDCA ao final do fluxo reforça o compromisso com a avaliação constante e o aperfeiçoamento dos procedimentos, especialmente em contextos que demandam alta responsabilidade jurídica e técnica, como é o caso da gestão de informações protegidas pela LGPD e orientadas pelas diretrizes de segurança estabelecidas pela família ISO/IEC 27000.

Neste contexto, os fluxogramas, conforme argumentam Silva (2020) e Cury (2015), além de facilitarem a comunicação técnica e a análise das atividades, configuram instrumentos valiosos de racionalização, padronização e documentação institucional, contribuindo para o aperfeiçoamento contínuo da gestão. Sua aplicação, neste estudo, reforça a governança da

informação e o alinhamento às exigências legais e ambientais, evidenciando a relevância de práticas organizadas, seguras e sustentáveis.

Nos tópicos seguintes, cada etapa apresentada será detalhada individualmente por meio de fluxogramas específicos, com a descrição de seus elementos críticos, objetivos e normativas correspondentes, de modo a fundamentar a proposta do Manual de Boas Práticas.

4.2.1 Procedimento de armazenamento de dados

Os procedimentos para o armazenamento seguro de dados pessoais exigem cuidados específicos, pois envolvem a proteção de um direito fundamental. Nesse contexto, a LGPD fundamenta-se em proporcionar garantias aos direitos do cidadão, ao mesmo tempo em que fornece as bases para o desenvolvimento da economia da informação, baseada nos vetores da confiança, segurança e valor (D'Angelo; Mota, 2024).

Pode-se destacar, portanto, que a proteção dos dados pessoais está intimamente ligada à defesa de direitos fundamentais do indivíduo no contexto da sociedade da informação. Com a promulgação da LGPD, o Brasil deu um passo importante para garantir a efetividade de garantias constitucionais como a privacidade, a liberdade de expressão, a dignidade da pessoa humana e o direito à informação (Sá, 2019). Direitos estes representados de forma visual na Figura 18, demonstrando como a proteção de dados está ancorada em valores constitucionais e legais que asseguram a cidadania digital e os limites para o uso de informações pessoais.

Figura 18 - Direitos fundamentais relacionados à proteção de dados pessoais

Fonte: elaboração própria, 2025 adaptada de Sá, 2019..

No contexto legal, o direito à Privacidade (1) encontra respaldo direto no art. 5º, inciso X, da CF (Brasil, 1988), que assegura a inviolabilidade da intimidade, da vida privada, da honra

e da imagem das pessoas, além de constituir um dos fundamentos da LGPD (art. 2º, I). O direito à Segurança dos Dados (2) aparece tanto na LGPD quanto em normativas como a ISO/IEC 27002:2022, que tratam de práticas e medidas para a proteção técnica e organizacional das informações pessoais. Já o direito à Informação, Comunicação e Opinião (3) está previsto no art. 5º, incisos IV e XIV, da CF, garantindo a liberdade de manifestação e o acesso à informação. A Defesa do Consumidor (4), por sua vez, é assegurada pelo art. 5º, inciso XXXII, da CF, e regulamentada pelo CDC (art. 6º, III e IV), vinculando-se diretamente à transparência e à proteção de dados nas relações de consumo. Por fim, a Liberdade, Dignidade e Cidadania (5), fundamentos da República previstos no art. 1º, incisos II e III, da CF, conectam-se à forma como os dados são tratados por organizações públicas e privadas, reafirmando o caráter de direito fundamental da proteção de dados pessoais.

Nesse sentido, todos esses elementos compõem o que se entende por "cidadania digital"[47], reafirmando o direito de cada indivíduo ao controle sobre suas informações pessoais e à interação consciente, segura e responsável no ambiente digital (Equipe TOTVS, 2023). Tais direitos sustentam a regulação do uso dos dados pessoais no Brasil e refletem uma concepção ampliada da proteção à pessoa, que vai além da privacidade, abarcando sua autonomia informacional e sua dignidade.

Conforme destacado por Miragem (2019), a integração entre a LGPD e o CDC evidencia a responsabilização das organizações como mecanismo central para garantir a proteção dos dados pessoais nas relações de consumo. Já Sá (2019), Leme; Blanck (2020) e Pinheiro *et al*. (2020), destacam que os desafios técnicos e regulatórios da aplicação da LGPD em setores sensíveis, como a IoT, onde questões relacionadas à privacidade, à segurança da informação e à dignidade do consumidor ganham complexidade devido ao elevado volume e sensibilidade dos dados tratados.

Contribuindo com uma visão sistêmica, Burkart (2021) chama atenção para a necessidade de efetiva implementação da LGPD nas rotinas institucionais, destacando que a conformidade legal não pode ser apenas formal, mas deve-se traduzir em práticas concretas que minimizem vulnerabilidades. Por fim, Galvão *et al.* (2024) alertam que, mesmo após a entrada em vigor da LGPD, os riscos de vazamentos de dados persistem, sendo necessário que as organizações adotem medidas técnicas eficientes e invistam na capacitação contínua de

[47] Cidadania digital é a capacidade de participar ativamente da sociedade no ambiente digital de forma positiva, justa, consciente, segura e ética. É saber usar as ferramentas tecnológicas para se informar, se comunicar, se expressar, se educar, se divertir e se relacionar com os outros, com respeito aos direitos e deveres de todos (Equipe TOTVS, 2023).

profissionais48 responsáveis pelo tratamento e armazenamento de dados e Rodrigues (2024) alerta para possíveis sanções e danos à reputação organizacional. Nesse contexto, torna-se essencial a adoção de procedimento estruturado para a classificação da informação.

Complementando a etapa de classificação, foi elaborado o Fluxograma de Procedimentos de Armazenamento de Dados, figura 19, que contempla as etapas essenciais para o armazenamento adequado de informações em ambientes organizacionais.

Ao realizar uma leitura visual do fluxograma, pode-se observar que o procedimento se inicia com a verificação da real necessidade de armazenamento, conforme determina o princípio da minimização de dados previsto na LGPD (Brasil, 2018). A ISO/IEC 27040:2015 corrobora esse entendimento ao destacar que o armazenamento desnecessário eleva riscos e custos operacionais, sobretudo em relação ao espaço, consumo de energia e à necessidade de monitoramento contínuo dos sistemas.

Na sequência, o fluxograma prevê a ***avaliação do local de armazenamento***, considerando critérios técnicos e classificações da informação, conforme orienta a ISO/IEC 27002:2022. Essa norma estabelece que dados mais sensíveis exigem níveis mais altos de proteção e medidas de controle proporcionais à sua criticidade.

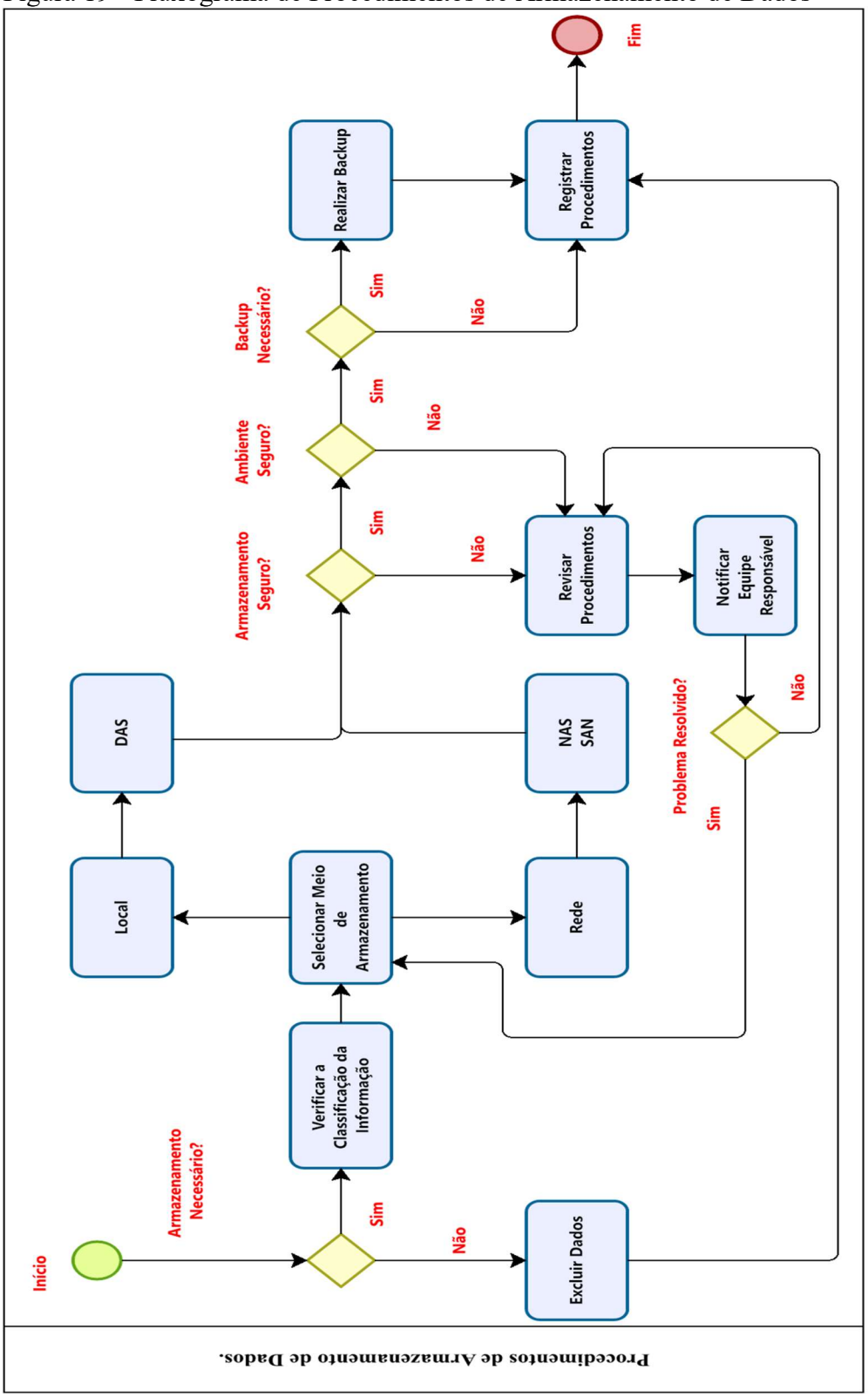
Assim, define-se o ***meio de armazenamento mais apropriado*** — local (*Direct-Attached Storage* – DAS) ou em rede (NAS ou SAN) — conforme os fatores operacionais (como por exemplo, capacidade de armazenamento, custos, disponibilidade de infraestrutura, frequência de acesso), a sensibilidade da informação (criticidade/confidencialidade) e a finalidade do tratamento (motivo pelo qual os dados estão sendo armazenados). A ISO/IEC 27040:2015 detalha essas opções, descrevendo suas arquiteturas, vantagens, riscos e medidas de segurança associadas.

Na etapa seguinte, o foco recai sobre a ***implantação de controles físicos e lógicos de segurança,*** incluindo autenticação, criptografia, registros de acesso e monitoramento. As normas ISO/IEC 27001:2024, ISO/IEC 27002:2022 e ISO/IEC 27040:2015 oferecem diretrizes específicas para a implementação desses controles, sendo que essa última estabelece a proteção física no armazenamento de dados, promovendo um ambiente confiável, auditável e alinhado às melhores práticas internacionais.

---

[48] Entende-se por profissionais responsáveis pelo tratamento e armazenamento de dados aqueles envolvidos diretamente na coleta, uso, armazenamento, proteção e gestão das informações pessoais dentro de uma organização. Entre eles destacam-se o Encarregado de Dados (DPO), profissionais da área de Tecnologia da Informação (TI), especialistas em Segurança da Informação, equipes de *Compliance* e Jurídico, além de analistas de processos e responsáveis por treinamentos corporativos, todos com papéis fundamentais na aplicação da LGPD e na mitigação de riscos relacionados à privacidade e segurança da informação.

Figura 19 - Fluxograma de Procedimentos de Armazenamento de Dados



Fonte: elaboração própria, 2025.

Após esta etapa, é fundamental assegurar que o ambiente ofereça níveis adequados de segurança, restringindo o acesso com a implementação de políticas administrativas que incluem gestão de acesso, monitoramento e melhoramento contínuo do processo que deverá ser

registrado e auditado periodicamente, conforme estabelece a ISO/IEC 27001:2024, além de controles lógicos que envolvem autenticação de usuários e criptografia conforme estabelecido na ISO/IEC 27002:2022.

Dependendo da criticidade das informações armazenadas, deve ser verificada a necessidade de cópias de segurança (*backup*), com base nos critérios de segurança e continuidade dos negócios estabelecidos pela ISO/IEC 27001:2024, os quais orientam que a disponibilidade da informação deve ser garantida mesmo em situações adversas. Esses cuidados visam assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações, conforme previsto no art. 46 da LGPD, que determina que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Brasil, 2018).

De acordo com a ISO/IEC 27040:2015, nos casos em que forem identificadas falhas no ambiente de armazenamento, seja por meio de auditorias, relatórios de monitoramento, testes de conformidade ou incidentes de segurança, é essencial que as equipes responsáveis sejam notificadas e que os procedimentos adotados sejam prontamente verificados e revisados. Essa revisão deve envolver uma análise criteriosa de cada etapa executada, incluindo os critérios de seleção dos meios de armazenamento, os controles implementados e os registros realizados. A ISO/IEC 27001:2024 estabelece que o SGSI deve ser periodicamente auditado e melhorado, garantindo que os controles permaneçam eficazes diante de novos riscos e mudanças tecnológicas. Esse processo de revisão deve ser documentado e acompanhado de planos de ação corretiva e indicadores que permitam avaliar a efetividade das medidas implementadas.

Por fim, o fluxograma contempla a ***etapa de verificação e revisão periódica do ambiente de armazenamento***, baseada em auditorias e relatórios de conformidade. Caso sejam detectadas não conformidades, os procedimentos devem ser atualizados, conforme previsto no ciclo de melhoria contínua prevista na ISO/IEC 27001:2024. Essa etapa garante que as práticas permaneçam eficazes diante de novos riscos e tecnologias, promovendo a atualização constante do SGSI (Magalhães, 2021)

Na elaboração do fluxograma a escolha desse encadeamento de etapas — iniciando com a verificação da necessidade, passando pela definição técnica do local e do meio de armazenamento, pela aplicação de controles de segurança e pela previsão de *backups* e revisões periódicas — teve como finalidade assegurar que cada decisão organizacional seja tomada com base no risco envolvido, no valor da informação e nas exigências legais. Trata-se de um percurso lógico e preventivo, voltado à mitigação de falhas e à promoção da conformidade

normativa, técnica e ambiental. Essa representação visual auxilia a compreender a articulação entre as decisões técnicas e jurídicas envolvidas no tratamento da informação. Assim, o fluxograma complementa os fundamentos normativos e legais discutidos nesta pesquisa, reforçando a importância de um processo de armazenamento baseado na classificação da informação e no gerenciamento seguro de seu ciclo de vida.

4.2.2 Procedimentos de *Backup* em Ativos contendo Dados

O procedimento de *backup* de dados é a etapa essencial da governança em segurança da informação, diretamente relacionado à garantia da continuidade dos serviços, à preservação da integridade dos dados e à prevenção de perdas decorrentes de incidentes tecnológicos, fator humano, desastres naturais e inacessibilidade (Vakulov, 2023). Nesse sentido, práticas consolidadas como a estratégia 3-2-1 — que recomenda manter três cópias dos dados, em dois tipos de mídia diferentes, sendo uma fora do local — são amplamente reconhecidas por sua eficácia (Gillis; Castagna, 2024).

Como já mencionado, esse procedimento reforça a aplicação das disposições da LGPD e se alinha especialmente ao disposto no art. 46, que determina a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Marinho; Paranaguá; Piva, 2024). A realização de backups contribui diretamente para a aplicação desse dispositivo, uma vez que permite a recuperação de dados em caso de falhas, ataques ou desastres.

Nesse contexto, a Figura 20 comunica, de forma visual, os principais requisitos para a realização de backups em ambientes organizacionais: segurança (representada pelo escudo e cadeado), automação (ícone do *notebook* com sincronização), redundância (armazenamento local e em nuvem) e gestão eficiente (engrenagens). Na elaboração da imagem foi planejado que cada elemento visual carregasse um significado técnico e simbólico.

Figura 20 - Procedimentos de *backup* em ativos contendo dados

Fonte: elaboração própria, 2025.

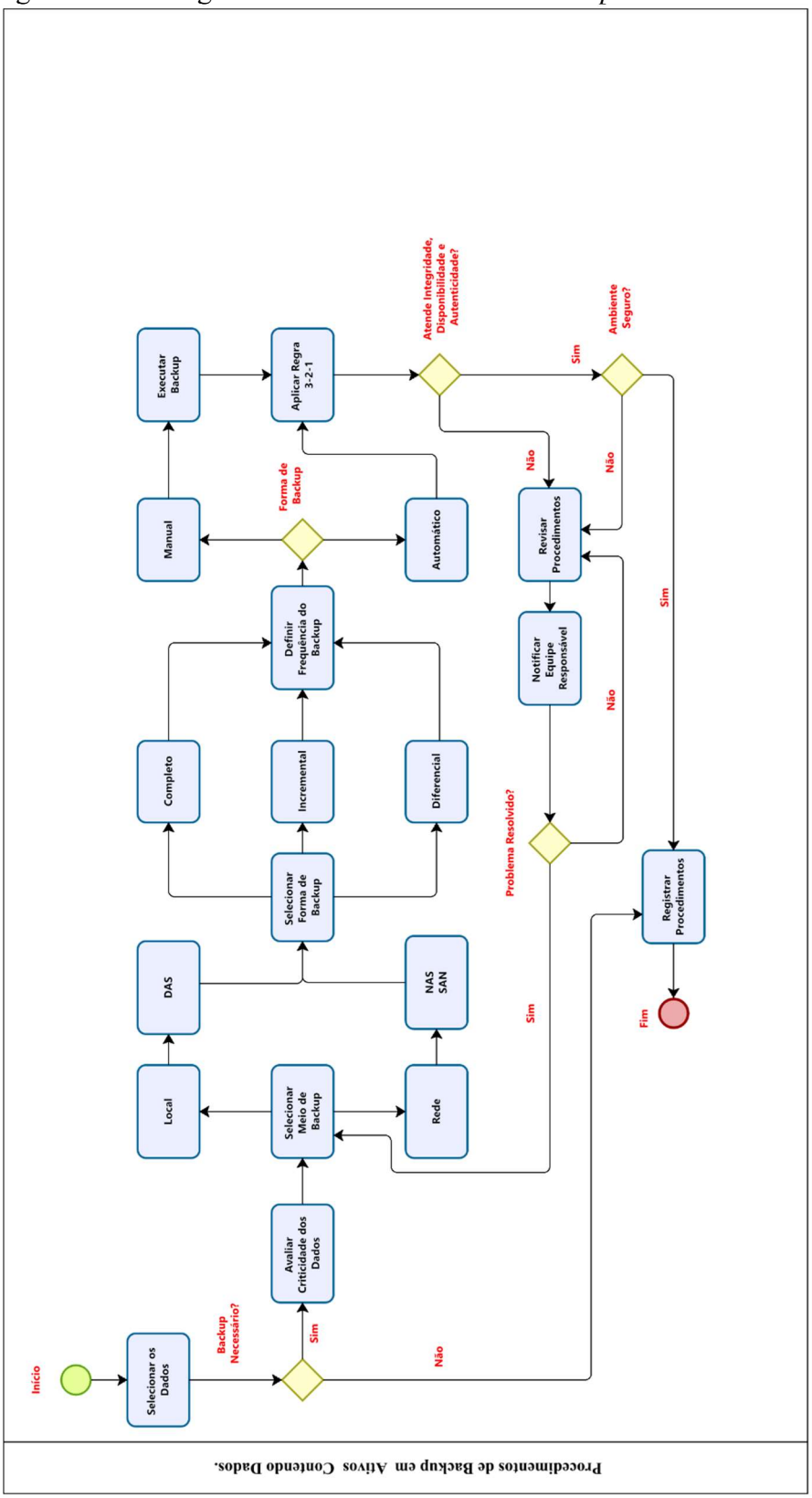
Para melhor entendimento, a nuvem com uma seta para baixo representa o armazenamento em nuvem, indicando a transferência de dados para ambientes remotos e seguros. Os discos sobrepostos simbolizam os servidores locais ou data centers, isto é, estruturas físicas destinadas ao armazenamento interno dos dados.

O *notebook* com um ícone de documento e uma seta circular remete ao processo de *backup* automático, sugerindo a realização contínua ou periódica de cópias sincronizadas das informações. O escudo com um sinal de verificação reforça o compromisso com a segurança da informação e a conformidade com boas práticas, indicando que os dados estão protegidos contra acessos indevidos. As engrenagens remetem ao funcionamento dos sistemas, apontando para a existência de rotinas automatizadas e mecanismos estruturados de gestão tecnológica. Por fim, o cadeado simboliza o controle de acesso e a proteção dos dados armazenados, assegurando a confidencialidade e a integridade da informação.

No contexto da governança da informação, a realização de cópias de segurança – backup – assume relevância não apenas técnica, mas também jurídica, ao dialogar com princípios e garantias fundamentais (Amancio *et al*., 2024). Nesse sentido, relaciona-se ao princípio da necessidade, que visa reduzir a coleta de dados ao mínimo indispensável para o alcance de suas finalidades (LGPD, art. 6º, III), e ao princípio da segurança (LGPD, art. 6º, VII), que determina a adoção de medidas técnicas e administrativas contra acesso não autorizados ou situações acidentais ou ilícitas (Brasil, 2018).

Diante desses conceitos legais e considerando critérios técnicos e jurídicos, foi elaborado o Fluxograma de Procedimentos de *Backup* em Ativos Contendo Dados (Figura 21).

Figura 21 - Fluxograma de Procedimentos de *Backup* em Ativos Contendo dados



Fonte: elaboração própria, 2025.

O fluxograma tem início com a seleção dos dados a serem resguardados. Em seguida, verifica-se a necessidade de *backup*, conforme o princípio da minimização de dados. Caso o *backup* seja justificado, passa-se à avaliação da criticidade das informações, passo previsto na ISO/IEC 27002:2022, que define que dados de maior sensibilidade requerem estratégias mais robustas de proteção.

Com base nessa avaliação, define-se a arquitetura de *backup* mais adequada (DAS ou NAS/SAN)[49], conforme descrito na ISO/IEC 27040:2015, que detalha arquiteturas e práticas seguras de armazenamento e *backup*. A escolha deve considerar a escalabilidade, o tempo de recuperação, os riscos ambientais - tais como ameaças externas e internas - e os custos operacionais associados.

A etapa subsequente envolve a definição da forma de *backup* (completo, incremental ou diferencial), de acordo com a natureza das informações, os recursos disponíveis e os objetivos estratégicos da organização. Essa escolha deve estar fundamentada em diretrizes técnicas e critérios operacionais estabelecidos na norma ISO/IEC 27040:2015, que orienta a proteção e a recuperação de dados em ambientes organizacionais.

Entre os principais fatores a serem considerados para a definição da forma de backup mais adequada, destacam-se como parâmetros essenciais à continuidade das operações: o *Recovery Time Objective* (RTO), que representa o tempo máximo aceitável para a recuperação dos sistemas após uma falha e o *Recovery Point Objective* (RPO), que indica a quantidade máxima de dados que a organização admite perder entre o último backup bem-sucedido e a ocorrência do incidente (Andrade, 2023).

O RTO, conforme Vakulov (2023), corresponde ao período máximo em que um sistema ou informação pode permanecer indisponível, enquanto o RPO define o intervalo de tempo máximo que a organização considera aceitável para a perda da informação, ou seja, o limite temporal até o qual os dados podem ser recuperados sem comprometer a continuidade das operações ou a integridade dos processos críticos da empresa. A ISO/IEC 27040:2015, recomenda que a definição da estratégia de *backup* esteja diretamente alinhada aos parâmetros estabelecidos no plano de continuidade de negócios da organização, assegurando que, diante de falhas, incidentes ou desastres, os dados possam ser restaurados dentro dos limites de tempo e perda aceitáveis, conforme a criticidade das operações e a natureza das informações envolvidas.

No processo seguinte à definição da forma de backup, estabelece-se a frequência com que as cópias de segurança serão realizadas, considerando a dinâmica das atualizações, a

[49] Essas duas formas encontram-se explicadas e ilustradas na seção do referencial teórico, tópico 2.2 Gestão de Armazenamento e *Backups, do referencial teórico.*

criticidade das informações e os objetivos estratégicos da organização, conforme estabelecidas pela ISO/IEC 27040:2015. Em seguida, procede-se à escolha entre a realização do backup manual — executado deliberadamente por um operador, em horários ou situações específicas — ou automático, realizado por sistemas programados em intervalos regulares e com menor interferência humana, de acordo com a capacidade técnica da instituição (Gillis; Castagna, 2024).

A definição da periodicidade do backup é uma decisão estratégica que deve ser orientada por uma análise criteriosa de riscos, sensibilidade das informações processadas, metas de continuidade do negócio e exigências legais aplicáveis. De acordo com a norma ISO/IEC 27040:2015, essa periodicidade deve estar alinhada com o tempo máximo admissível de perda de dados entre um *backup* e outro, conforme estabelecido previamente pela organização com base na criticidade das atividades.

Além disso, a LGPD estabelece que o tratamento de dados deve observar princípios como a segurança, a prevenção e a responsabilização, exigindo dos agentes de tratamento a adoção de medidas técnicas e administrativas para prevenir acessos não autorizados, perdas ou alterações indevidas de dados pessoais (Sá, 2019). Assim, uma frequência de *backup* inadequada pode comprometer tanto a continuidade operacional quanto a conformidade legal da organização.

A escolha entre *backup* manual e automático envolve também políticas administrativas e controles operacionais. A norma ISO/IEC 27002 recomenda a adoção de mecanismos automatizados nos processos de *backup* como forma de reduzir falhas humanas e garantir maior consistência, rastreabilidade e confiabilidade nas cópias de segurança. A automação facilita, ainda, o cumprimento de políticas internas e de requisitos regulatórios, contribuindo para a integridade e disponibilidade das informações ao longo do tempo.

Ainda que as soluções automatizadas sejam preferenciais, há cenários operacionais em que a realização de *backups* manuais permanece necessária. Isso ocorre, por exemplo, em ambientes domésticos, pequenas empresas ou em situações emergenciais nas quais o sistema automatizado esteja indisponível (Gillis; Castagna, 2024). Nesses casos, a ISO/IEC 27002:2022 orienta que os procedimentos manuais estejam devidamente documentados, com responsáveis designados e geração de registros formais, de modo a garantir a rastreabilidade das ações realizadas e a integridade da informação em todas as fases do seu ciclo de tratamento.

Portanto, a realização de backups manuais ou automáticos devem seguir os critérios estabelecidos pela estratégia 3-2-1 (Figura 22), que recomenda manter ao menos três cópias dos dados, armazenadas em dois tipos distintos de mídia, sendo uma delas localizada fora do

ambiente principal (Gillis; Castagna, 2024). Essa prática está conceitualmente alinhada aos princípios da norma ISO/IEC 27040, que enfatiza a importância da redundância, da diversidade tecnológica e da separação física ou lógica entre as cópias, como forma de mitigar riscos de perda, comprometimento ou indisponibilidade da informação.

Complementarmente, a norma ISO/IEC 27002 recomenda que as organizações adotem políticas formais de *backup* que definem não apenas a frequência e o tipo das cópias, mas também mecanismos de proteção contra falhas físicas, acessos não autorizados e eventos adversos, garantindo que as cópias estejam armazenadas em locais distintos e seguros.

Figura 22 - Estratégia de *Backup* 3-2-1

Fonte: elaboração própria, 2025.

Essa estratégia é respaldada por autores como Gillis; Castagna (2024) e Vakulov (2023), que a reconhecem como uma das boas práticas mais recomendadas no campo da segurança da informação. Embora eles destacam que ela não elimina por completo a possibilidade de comprometimento dos dados, reforçam que a regra 3-2-1 reduz significativamente os riscos ao evitar a dependência de um único ponto de falha. Isso significa que, mesmo diante de problemas como falhas técnicas, corrupção de arquivos, desastres naturais ou eventos como furtos ou incêndios, a organização ainda terá alternativas para recuperar suas informações, garantindo maior resiliência e continuidade operacional.

Na fase de verificação da integridade, disponibilidade e autenticidade dos dados, o processo de *backup* é submetido a uma checagem criteriosa para garantir que as informações armazenadas não foram corrompidas, estão acessíveis quando necessário e mantêm sua origem fidedigna. Esse procedimento está alinhado ao princípio da segurança previsto no Art. 6º,

LGPD, e aos controles de verificação da ISO/IEC 27001:2024, que reforçam a importância de assegurar a confiabilidade dos sistemas. Portanto, realiza-se uma validação de conformidade com os requisitos de segurança para verificar se o *backup* atende aos princípios de integridade, disponibilidade e autenticidade (ISO/IEC 27001:2024) e se está alocado em ambiente seguro (ISO/IEC 27040:2015). Se alguma dessas condições não for atendida, o procedimento deve ser revisado e reaplicado, até alcançar a conformidade plena.

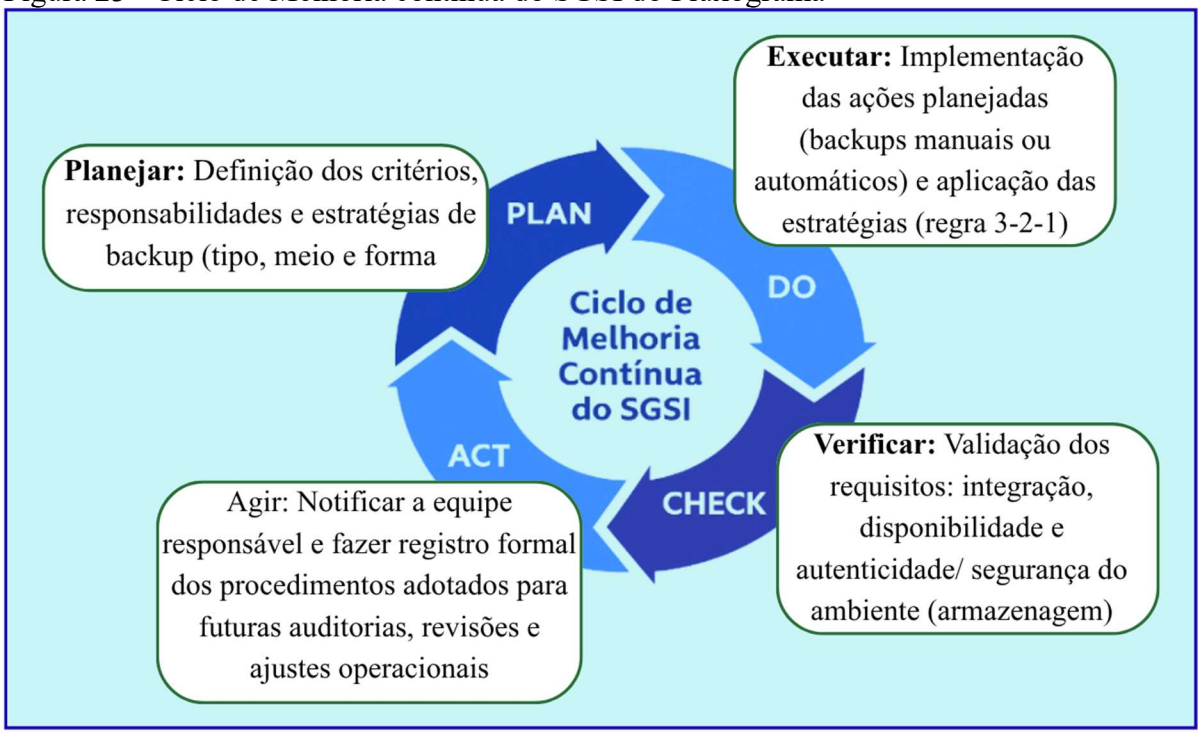
A etapa seguinte envolve a execução de testes de recuperação, fundamentais para garantir que os dados possam ser restaurados de maneira eficaz, mesmo em cenários de falha ou incidente. Essa medida está alinhada com os princípios da ISO/IEC 27031, voltada à continuidade dos serviços. Ademais, a LGPD, em seu Art. 18, estabelece que os titulares têm direito ao acesso facilitado às suas informações pessoais (Brasil, 2018), o que reforça a necessidade de ambientes controlados, protegidos contra falhas de *hardware*, ataques cibernéticos e outras ameaças que possam comprometer a disponibilidade dos dados (Vakulov, 2023).

Por fim, a auditoria e o registro dos procedimentos são etapas decisivas para consolidar a conformidade e a rastreabilidade de todo o processo. A auditoria interna, conforme orienta a ISO/IEC 27001:2024, permite identificar falhas e aperfeiçoar os controles existentes, sendo também uma evidência de boas práticas segundo o Art. 50 da LGPD (Brasil, 2018). Já o registro detalhado das ações realizadas cumpre um papel estratégico tanto na governança da informação quanto na rastreabilidade dos fluxos de descarte previstos na PNRS, garantindo que mídias obsoletas recebam uma destinação ambientalmente adequada e documentada (Brasil, 2010).

Assim, ao final do processo, conforme representado nas etapas “Notificar Equipe Responsável” e “Registrar Procedimentos” do fluxograma (Figura 23), estabelece-se uma conexão direta com o ciclo de melhoria contínua do SGSI, conforme preconizado pela norma ISO/IEC 27001:2024. Esse ciclo visa assegurar que os procedimentos adotados permitam ajustes contínuos, com base em auditorias internas, revisões periódicas e evolução tecnológica, garantindo a conformidade das práticas de segurança da informação.

Considerando o fluxograma elaborado, ou seja, a importância de estruturar o procedimento de *backup* de dados como uma prática sistemática e integrada à gestão da informação, torna-se necessário destacar estudos como os de Burkart (2021) e Cardoso; Régis (2024) que apontam que estratégias de *backup* eficazes não devem se restringir à adoção de ferramentas tecnológicas, mas precisam estar articuladas a políticas institucionais claras, contemplando capacitação das equipes, controle rigoroso de acessos, realização periódica de testes de restauração e revisão contínua das rotinas.

Figura 23 - Ciclo de Melhoria contínua do SGSI do Fluxograma



Fonte: elaboração própria, 2025.

Além disso, Galvão *et al.* (2024) e Pinheiro *et al*. (2020) alertam que falhas em processos de *backup* estão entre as principais causas de exposição indevida de dados pessoais, especialmente em casos de incidentes cibernéticos e vazamentos. Tais falhas, muitas vezes, decorrem da ausência de padronização nos procedimentos, da negligência em revisões regulares e da insuficiência de treinamentos sobre boas práticas.

Do ponto de vista técnico, estudos como os de Amancio *et al.* (2024) e Schneider *et al.* (2021) destacam a necessidade de atenção redobrada na execução de *backups* locais, bem como na sanitização adequada das mídias após o descarte, para evitar o acesso indevido de dados sensíveis. Ambos os aspectos evidenciam a importância de rotinas formalizadas e auditáveis.

Portanto, o fluxograma elaborado não apenas traduz os requisitos da LGPD e das normas da família ISO/IEC 27000, como também promove uma lógica processual coerente e preventiva. Ele busca garantir que o backup de dados pessoais ocorra de forma eficiente, juridicamente segura e tecnicamente eficaz, promovendo a proteção do titular, a continuidade institucional e a conformidade com as legislações nacionais e internacionais vigentes.

4.2.3 Procedimentos de Sanitização em Ativos contendo Dados

Os procedimentos de sanitização de ativos que armazenam dados pessoais são essenciais para garantir a eliminação segura dessas informações ao final de seu ciclo de vida (IDSC, 2025). Conforme as diretrizes da LGPD, a necessidade de adotar medidas eficazes nesse processo decorre das obrigações legais impostas aos agentes de tratamento, que devem prevenir o acesso indevido ou a recuperação indevida dos dados, mesmo após o descarte de mídias e equipamentos (Brasil, 2018).

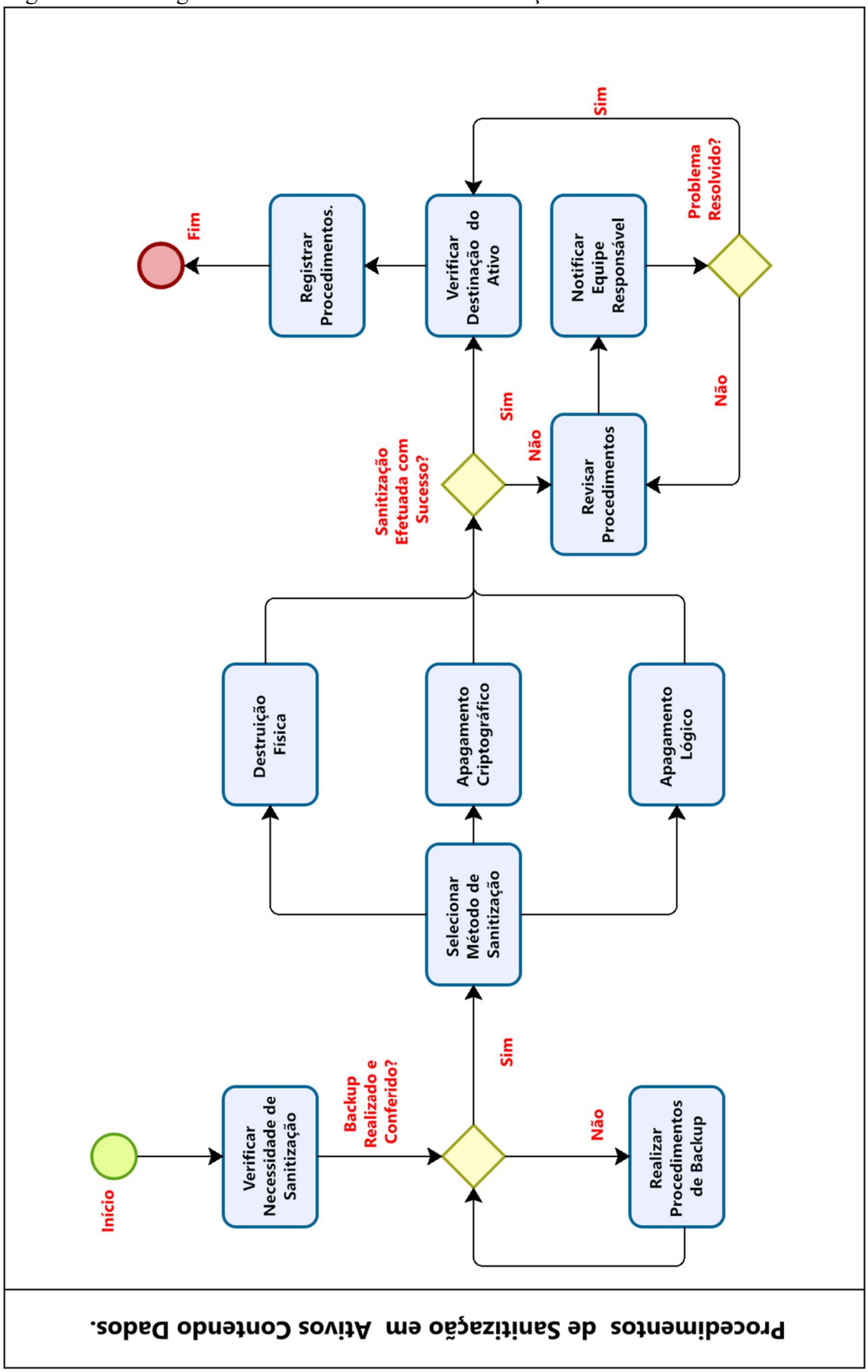
Nesse contexto, o fluxograma apresentado na Figura 24, que descreve os Procedimentos de Sanitização em Ativos Contendo Dados, inicia-se com a verificação da real necessidade de exclusão das informações e a confirmação da existência de cópias de segurança (backup) atualizadas e válidas. Antes da execução de qualquer método de sanitização, conforme ISO/IEC 27040:2015 e ISO/IEC 27002, é imprescindível assegurar que os dados armazenados nos dispositivos tenham sido devidamente resguardados, por meio de processos de backup realizados de forma adequada, com base nos princípios de integridade, disponibilidade, autenticidade e confiabilidade.

Essa análise envolve a verificação de que as cópias estão completas, íntegras, acessíveis e armazenadas em ambientes seguros, conforme exigido tanto pela LGPD, (art. 6º, incisos VII e X) quanto pelas diretrizes normativas. Tal etapa é fundamental para garantir que informações relevantes sejam preservadas antes da exclusão definitiva dos dados do ativo, evitando perdas acidentais e assegurando a continuidade operacional da organização.

Em caso de ausência de backup, o procedimento de sanitização deve ser imediatamente suspenso até que a cópia de segurança seja devidamente realizada, verificada e validada. A norma ISO/IEC 27040 orienta que os backup*s* sejam conferidos antes da exclusão definitiva de qualquer dado, como forma de mitigar riscos de perda de informações essenciais.

Superada essa etapa, passa-se à definição do método de sanitização mais adequado ao dispositivo e à natureza dos dados. Essa escolha deve considerar variáveis como o tipo de mídia, a sensibilidade das informações armazenadas, os riscos de exposição e os objetivos institucionais. O processo deve garantir a eliminação completa dos dados, de modo que não possam ser recuperados por nenhuma técnica disponível, conforme as recomendações da ISO/IEC 27040:2015. Adicionalmente, o artigo 46 da LGPD reforça a obrigação legal de adoção de medidas técnicas e administrativas eficazes para a proteção dos dados pessoais durante todo o seu ciclo de vida (Brasil, 2018).

Figura 24 - Fluxograma de Procedimentos de Sanitização em Ativos Contendo Dados



Fonte: elaboração própria, 2025.

A destruição física é indicada para mídias obsoletas, danificadas ou cuja reutilização não seja possível ou desejada. Trata-se de uma prática que elimina de forma definitiva qualquer possibilidade de recuperação dos dados, por meio de técnicas como a fragmentação mecânica, a trituração ou a incineração do meio físico (IDSC, 2025). Por exemplo, a destruição física é indicada para dispositivos que não serão reutilizados, especialmente quando contêm dados sensíveis, jurídicos ou financeiros, cuja recuperação deve ser absolutamente impedida.

O apagamento criptográfico, por sua vez, baseia-se na destruição segura e definitiva das chaves criptográficas que protegem os dados. Embora o conteúdo permaneça fisicamente presente no dispositivo, ele se torna inacessível. Esse método é eficaz quando os dados foram previamente criptografados com algoritmos robustos e as chaves são devidamente inutilizadas, sendo recomendado em ambientes corporativos que utilizam criptografia em disco como padrão (IDSC, 2025).

Já o apagamento lógico (ou sobrescrita de dados) é executado por meio de softwares especializados, que substituem os dados originais por padrões binários — como zeros, uns ou sequências aleatórias — sendo mais apropriado para mídias reutilizáveis (IDSC, 2025)

Após a aplicação do método de sanitização escolhido — seja destruição física, apagamento criptográfico ou lógico —, torna-se obrigatória a verificação de sua efetividade, conforme as orientações da norma ISO/IEC 27040:2015. Essa etapa visa comprovar que os dados foram de fato eliminados, prevenindo o risco de recuperação indevida por técnicas avançadas.

Confirmada a eficácia da sanitização, procede-se à verificação da destinação do ativo, seja para reutilização, descarte ou reencaminhamento, em conformidade com a política interna de gestão de ativos. Essa decisão deve ser formalmente autorizada e documentada, conforme exigido pela ISO/IEC 27001:2024, que estabelece que o descarte de ativos de informação seja controlado, com procedimentos definidos e a aprovação institucional necessária.

A adequada gestão desse processo, conforme menciona a ISO/IEC 27040:2015, demanda a documentação minuciosa de todas as etapas realizadas — incluindo a data, o método de sanitização empregado, o responsável técnico e os resultados obtidos. Essa documentação é fundamental para garantir a rastreabilidade das ações, possibilitar auditorias internas e externas e demonstrar a conformidade com o princípio da responsabilização e prestação de contas previsto no art. 6º, inciso X, da LGPD (Brasil, 2018).

Além da execução técnica, é essencial que as políticas institucionais sobre sanitização de ativos sejam periodicamente revisadas, especialmente diante de atualizações tecnológicas ou

do surgimento de novas ameaças (Lavos, 2023). Essa prática está alinhada ao modelo de melhoria contínua, recomendado pela ISO/IEC 27001:2024 e aos programas de governança de dados previsto no art. 50 da LGPD (Brasil, 2018).

A verificação, a auditoria e o monitoramento contínuo dos procedimentos também são indispensáveis, permitindo identificar falhas, aprimorar controles e garantir a conformidade. Tais ações podem ser realizadas tanto por meio de auditorias internas quanto externas, especialmente em processos de certificação, conforme previsto na LGPD (art. 6º, incisos VII e X) e na ISO/IEC 27001:2024. Por fim, é prioritário atuar proativamente na correção de falhas, adotando novas tecnologias, fortalecendo os procedimentos e capacitando as equipes envolvidas, em consonância com os princípios de melhoria contínua e gestão de mudanças previstos pelas normas internacionais (Magalhães, 2021).

A sanitização de dados, conforme detalhado no fluxograma, transcende a simples exclusão de informações em ativos digitais, configurando-se como um processo complexo, interdisciplinar e estratégico, que exige rigor técnico, jurídico e ambiental.

No âmbito do Direito, a norma ISO/IEC 27040:2015 orienta que a sanitização de dispositivos de armazenamento de dados é fundamental para o cumprimento das boas práticas, prevenindo riscos legais decorrentes da exposição indevida de dados pessoais, que podem implicar sanções severas e danos reputacionais às organizações. Além disso, a responsabilização legal impõe que as políticas e práticas no tratamento de informações pessoais sejam claras, atualizadas e documentadas, garantindo a proteção efetiva dos direitos dos titulares de dados ((Marinho; Paranaguá; Piva, 2024).

No campo da segurança da informação, conforme evidencia a ISO/IEC 27040:2015, a sanitização integra a gestão técnica essencial para a proteção dos ativos de informação. O ciclo PDCA, recomendado pela ISO/IEC 27001:2024, estrutura um processo contínuo de planejamento, execução, verificação e ação corretiva para garantir a efetividade das práticas de sanitização, de modo que a atualização tecnológica, o monitoramento constante e a capacitação das equipes constituem requisitos indispensáveis para mitigar vulnerabilidades e prevenir incidentes de segurança (Magalhães, 2021).

No que concerne à sustentabilidade ambiental, a sanitização adequada de dados está intimamente ligada ao descarte responsável de dispositivos eletrônicos. A remoção segura das informações antecede a reciclagem ou destinação correta do lixo eletrônico, evitando impactos ambientais decorrentes do descarte inadequado. Assim, as práticas de sanitização colaboram para a logística reversa e o ciclo sustentável dos resíduos eletroeletrônicos, promovendo

responsabilidade compartilhada entre organizações, consumidores e o meio ambiente D'Angelo; Mota, 2024).

Dessa forma, o fluxograma elaborado não apenas detalha as etapas técnicas da sanitização, mas também reflete a convergência de princípios e exigências de diferentes áreas do conhecimento, integrando normas legais, padrões técnicos e práticas ambientais. Seguir com rigor esse fluxograma é garantir: (i) conformidade legal com a LGPD e demais normativas pertinentes, prevenindo riscos jurídicos; (ii) segurança e integridade das informações, alinhadas às melhores práticas de governança da informação; (iii) a contribuição para a sustentabilidade ambiental por meio do manejo responsável dos dispositivos eletrônicos; (iv) a melhoria contínua dos processos organizacionais, por meio do ciclo PDCA, assegurando eficácia, eficiência e adaptação a novas demandas.

Assim, a elaboração e a aplicação sistemática deste fluxograma configuram um instrumento essencial para a gestão responsável dos dados pessoais e dos ativos de informação, traduzindo-se em vantagem competitiva, mitigação de riscos e fortalecimento da confiança dos titulares e demais *stakeholders*[50].

4.2.4 Procedimentos de Descarte em Ativos contendo Dados

Antes de apresentar o fluxograma elaborado, é fundamental compreender os aspectos legais, técnicos e ambientais que envolvem o descarte de ativos contendo dados. Tal procedimento exige condutas seguras e responsáveis, considerando a proteção das informações, a conformidade com a legislação vigente e os princípios da sustentabilidade.

Neste contexto, destaca-se o Decreto n. 10.240/2020 que regulamenta a logística reversa de produtos eletroeletrônicos e seus componentes, estabelecendo diretrizes que também impactam diretamente a proteção de dados e a responsabilidade dos envolvidos nesse processo. Na Figura 25 tem-se um esquema deste decreto, considerando o que confere ao consumidor, ou seja, este tem como responsabilidade remover previamente todos os dados pessoais e informações privadas dos equipamentos (1), como forma de garantir a proteção da privacidade e prevenir eventuais violações. Cumprida essa exigência, o decreto isenta as empresas e entidades gestoras da responsabilidade por dados remanescentes, transferindo ao consumidor os riscos decorrentes de eventual omissão (2). O decreto reforça o dever legal dos comerciantes

[50] *Stakeholders* são todas as partes interessadas ou afetadas por um determinado processo, projeto ou organização. Isso inclui, entre outros, clientes, funcionários, fornecedores, acionistas, órgãos reguladores e a comunidade em geral, que têm interesse direto ou indireto nos resultados e impactos das ações realizadas.

de informar o consumidor, no momento da entrega do equipamento, sobre a obrigatoriedade da exclusão dos dados (3). Por fim, destaca-se à perda tácita, imediata e irrevogável da propriedade dos bens descartados (4), o que implica na irrecuperabilidade dos dados neles contidos e na inexistência de qualquer direito à indenização, mesmo que os dispositivos venham a ser reutilizados por terceiros (Brasil, 2020).

Figura 25 - Obrigações legais dos consumidores no descarte de produtos eletrônicos

Fonte: elaboração própria, 2025.

Enquanto, a Figura 26, de forma integrada, ilustra as principais diretrizes legais, técnicas e ambientais que devem orientar o descarte responsável de ativos contendo dados. Ela reforça a necessidade de remoção prévia de informações pessoais, a irreversibilidade da perda da propriedade no ato do descarte e a importância de avaliar alternativas como o reuso e manutenção antes da destinação final, conforme exigem a LGPD, o Decreto nº 10.240/2020 e a PNRS.

Nesta representação visual estão evidenciadas as diretrizes principais para o descarte responsável de ativos com dados: (1) a remoção prévia dos dados é obrigatória; (2) o consumidor perde automaticamente a propriedade sobre o bem no ato do descarte; (3) empresas e entidades gestoras não respondem por dados não excluídos; e (4) eventuais usos indevidos

podem ser denunciados às autoridades, sem previsão de indenização (Brasil, 2020). Portanto, antes de encaminhar qualquer dispositivo para descarte, devem ser esgotadas todas as possibilidades de reaproveitamento, em consonância com os princípios da ecoeficiência e do desenvolvimento sustentável. Medidas de prolongamento da vida útil, como reuso interno e doação, devem ser priorizadas (Brasil, 2010).

Figura 26 - Diretrizes para o descarte responsável de ativos com dados

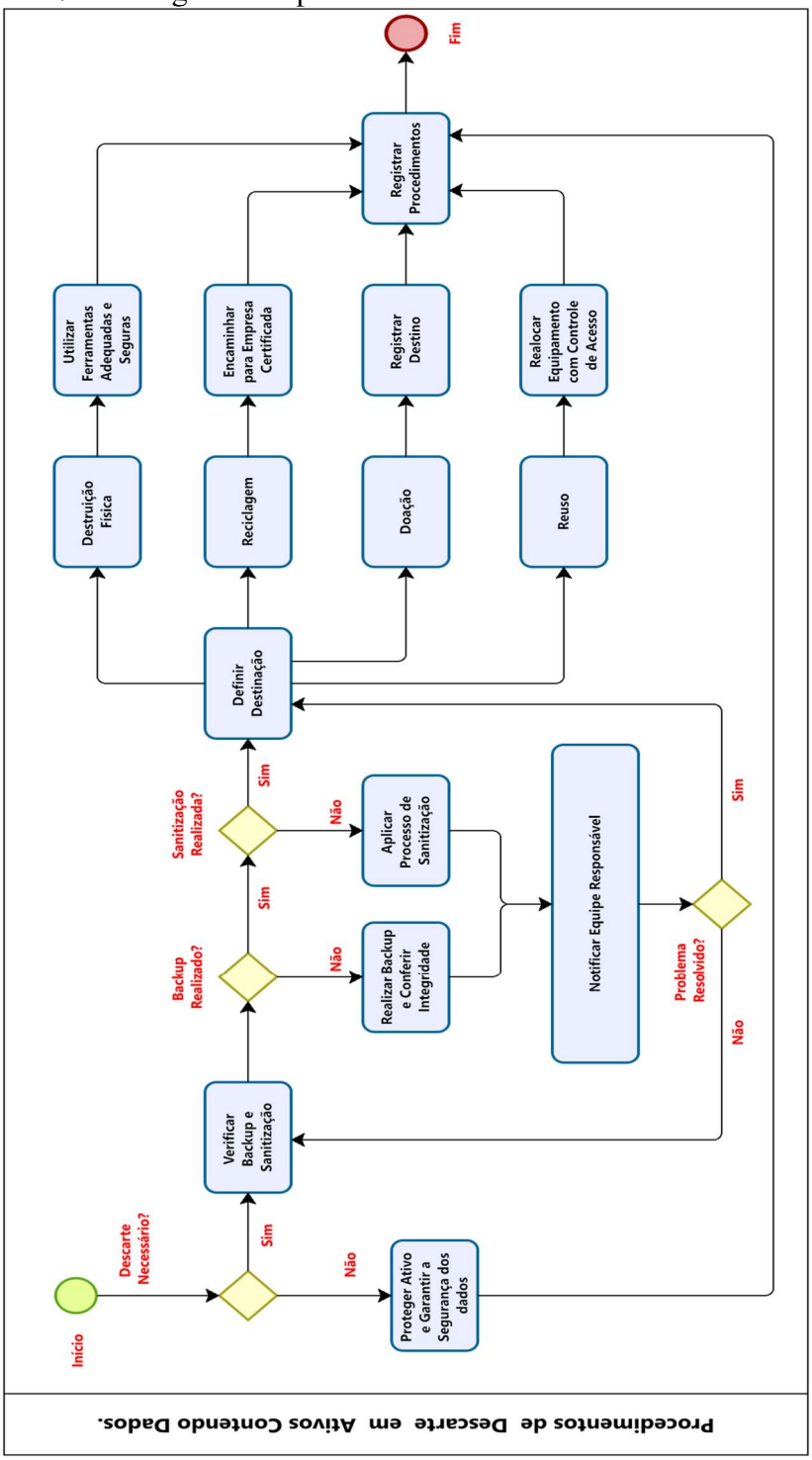
Fonte: elaboração própria, 2025.

Depois de destacar as obrigações do consumidor e as diretrizes do descarte, apresenta-se, na Figura 27, o Fluxograma elaborado de Procedimentos de Descarte em Ativos Contendo Dados. O fluxograma sintetiza visualmente todas as etapas envolvidas no processo de descarte de ativos contendo dados, conforme os princípios e as diretrizes discutidas. O início parte da pergunta “Descarte necessário?”. Portanto, antes de qualquer procedimento, é imprescindível realizar uma avaliação criteriosa da real necessidade de descarte de ativos de armazenamento de dados, considerando fatores como obsolescência tecnológica, falhas físicas irreparáveis ou o esgotamento do ciclo de vida útil do equipamento.

Ao ser realizada a avaliação e constatar-se que o descarte não precisa ser realizado ou não há autorização para fazê-lo, é indispensável à adoção de medidas que mitiguem os riscos de acesso não autorizado, perda de integridade ou uso indevido das informações armazenadas.

Na prática o objetivo é “Proteger ativo e garantir a segurança dos dados”, ou seja, manter o ativo protegido e assegurar a segurança dos dados armazenados. Isso significa que o equipamento continuará em uso ou será armazenado temporariamente, exigindo medidas que evitem o acesso não autorizado, a perda de integridade das informações e possíveis violações de confidencialidade.

Figura 27 - Fluxograma de procedimentos de descarte em ativos contendo dados



Fonte: elaboração própria, 2025.

Nessa situação, devem ser aplicados os controles recomendados pela norma ISO/IEC 27002, que orienta sobre a proteção de ativos inativos ou fora de uso imediato, e atendidos os princípios da LGPD — especialmente os relativos à segurança e à prevenção (art. 6º, incisos VII e VIII). Além disso, é indispensável o registro formal dos procedimentos adotados, como forma de garantir rastreabilidade e conformidade, como estabelecem tanto a LGPD (art. 37) quanto às boas práticas de governança da ISO/IEC 27037, que recomenda a documentação de evidências para assegurar a transparência das decisões relacionadas ao ciclo de vida dos ativos informacionais.

Neste propósito assegura-se o que é imposto pela LGPD, de salvaguardar para todo o ciclo de vida dos ativos informacionais (Brasil, 2018). A ISO/IEC 27002, por sua vez, orienta a implementação de controles que assegurem a confidencialidade, a integridade e a disponibilidade dos dados, inclusive em equipamentos inativos. Além disso, o artigo 9º da PNRS determina que a disposição final ambientalmente adequada só deva ser adotada depois de esgotadas as alternativas de não geração, redução, reutilização e reciclagem (BRASIL, 2010). Medidas de prolongamento da vida útil devem ser previamente consideradas (Schaun *et al.*, 2023).

Com base na avaliação inicial sobre a necessidade — ou não — de descarte, inicia-se o processo representado no fluxograma dos Procedimentos de Descarte em Ativos Contendo Dados, elaborado para orientar decisões seguras e responsáveis. A partir dessa primeira definição, desenvolvem-se etapas estruturadas e interligadas, fundamentadas em três eixos principais: conformidade legal, segurança da informação e sustentabilidade ambiental. Esses eixos adotados como linha de ação deste estudo, garantem que o descarte ocorra de forma ética, técnica e ambientalmente adequada, evitando riscos e promovendo boas práticas institucionais.

Em consonância com a PNRS, devem ser priorizadas medidas que promovam a não geração e a redução de resíduos, evitando o descarte prematuro de equipamentos ainda recuperáveis (Brasil, 2010). Entre essas medidas, destacam-se o prolongamento da vida útil dos ativos, por meio de políticas de manutenção corretiva e preventiva, e a racionalização das aquisições, com base em um planejamento criterioso das necessidades tecnológicas institucionais. Essa abordagem preventiva contribui para a sustentabilidade ambiental e a otimização dos recursos financeiros, alinhando-se aos princípios da responsabilidade compartilhada e do uso eficiente de recursos.

Confirmada a necessidade de descarte do ativo, a etapa seguinte indicada no fluxograma refere-se à “Execução de medidas preventivas: *Backup* e Sanitização”. Trata-se de uma fase

crítica para garantir a proteção das informações armazenadas e o cumprimento das exigências legais e normativas.

As ações nessa etapa envolvem, primeiramente, a verificação da existência e da integridade do *backup*, seguida da sanitização dos dados. Esse processo é guiado pelas seguintes interrogações: *Backup* realizado? Se não, realizar e conferir integridade; Sanitização realizada? → Se não, aplicar o processo adequado. Uma vez concluídas essas ações, cabe à equipe responsável registrar e notificar a execução, possibilitando a continuidade segura do fluxo.

Na prática, caso o *backup* não tenha sido realizado, o processo de descarte deve ser interrompido até que essa etapa esteja devidamente concluída, em conformidade com os princípios da segurança, integridade e disponibilidade dos dados, conforme estabelecido no art. 6º da LGPD (Brasil, 2018).

Já a sanitização de dados consiste na remoção definitiva e irreversível das informações armazenadas nos ativos. Essa ação deve ser conduzida com base na sensibilidade dos dados e em conformidade com as diretrizes da norma ISO/IEC 27040:2015, utilizando técnicas seguras como a eliminação física, o apagamento criptográfico ou a sobrescrição[51].

Após a realização do backup e da sanitização dos dados, a próxima etapa é "Definir a destinação do descarte dos ativos", que deve ser baseada em critérios técnicos, legais e ambientais. Entre as opções possíveis estão: a destruição física, a reciclagem, a doação e o reuso (ISO/IEC 27040), conforme apresentadas sinteticamente na Figura 28. A escolha da destinação deve considerar critérios técnicos e legais, como o nível de sensibilidade das informações (ISO/IEC 27005), o valor residual do equipamento e os princípios da responsabilidade ambiental (Brasil, 2010).

Figura 28 - Destinação final de ativos de tecnologia da informação

Fonte: elaboração própria, 2025.

[51] Essas técnicas são explicadas no tópico "2.8 Sanitização em Dispositivos de Armazenamento de Dados".

A destruição física corresponde à eliminação definitiva do equipamento por meio do uso de ferramentas apropriadas e seguras, devendo ser acompanhada da emissão de certificado que comprove a realização do procedimento, conforme orientações da ISO/IEC 27002 e de Freitas (2019). De acordo com o fluxograma, na escolha desta opção devem ser utilizadas ferramentas adequadas e seguras para sua execução, como fragmentadoras industriais, prensas hidráulicas, trituradores, moinhos de martelo e equipamentos de desmagnetização (D'Angelo, 2024).

A opção pela reciclagem deve ser realizada por empresa tecnicamente capacitada, devidamente licenciada pelos órgãos ambientais competentes e, preferencialmente, certificada segundo a norma ISO 14001, que estabelece diretrizes para sistemas de gestão ambiental.-Essa exigência visa garantir o compromisso em identificar, monitorar e controlar os impactos ambientais, promovendo a transparência e a responsabilidade ambiental (Lavos, 2023). De acordo com o artigo 20 da PNRS, a destinação ambientalmente adequada deve assegurar o reaproveitamento dos materiais recicláveis, evitando a contaminação do meio ambiente e a exposição a riscos (Brasil, 2010). Portanto, a reciclagem deve ser precedida da sanitização dos dados, respeitando as normas de segurança da informação, para que os ativos sejam encaminhados à cadeia de reaproveitamento sem comprometimento de dados sensíveis ou confidenciais.

Quanto à opção pela doação, é necessário que haja registro formal da transferência do bem, incluindo o destinatário, a data e os termos da cessão. Além disso, devem ser asseguradas garantias documentadas de que os dados anteriormente armazenados foram tornados irrecuperáveis, por meio de processos adequados de sanitização. Tais exigências estão alinhadas aos princípios da ecoeficiência[52] e da responsabilidade social, conforme destacado por Schaun *et al.* (2023), e atendem às diretrizes da LGPD (Brasil, 2018), especialmente no que tange ao dever de evitar o tratamento indevido de dados pessoais, mesmo após a descontinuação do uso do ativo. Adicionalmente, a PNRS reforça que a doação deve observar a responsabilidade compartilhada pelo ciclo de vida dos produtos, o que inclui o correto tratamento das informações armazenadas e a destinação ambientalmente adequada dos bens transferidos (Brasil, 2010).

No caso do reuso, a prática consiste em realocar o equipamento com controle de acesso e rastreabilidade, podendo ocorrer em duas modalidades: reuso interno ou externo. No reuso interno, exige-se um controle rigoroso de acesso, rastreabilidade do equipamento e aplicação

[52] Ecoeficiência: capacidade de produzir bens e serviços utilizando menos recursos naturais, buscando reduzir a geração de resíduos, incentivando a reciclagem.

de procedimentos de sanitização, conforme estabelecido pela norma ISO/IEC 27001:2024 e pelo artigo 46 da LGPD (Brasil, 2018). Essa modalidade inclui, ainda, o reaproveitamento de componentes de equipamentos obsoletos na manutenção de outros ativos, bem como a realização de *upgrades* que prolonguem sua vida útil e otimizem o desempenho (Marques, 2017). Equipamentos com menor performance, por exemplo, pode ser destinado a funções menos críticas ou ambientes com baixa demanda computacional, contribuindo para a racionalização de recursos e a sustentabilidade institucional.

Já o reuso externo envolve a transferência do ativo para terceiros, somente após a realização de sanitização segura e irreversível dos dados, em conformidade com as boas práticas previstas nas normas da família ISO/IEC 27000. De acordo com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), um exemplo frequente consiste na doação para instituições sem fins lucrativos, como telecentros, escolas públicas e bibliotecas, promovendo inclusão digital e responsabilidade social (Brasil, 2018).

Conforme estabelece o Art. 14 do Decreto n. 9.373/2018:

> A doação de equipamentos de informática por órgãos e entidades da administração pública federal observará a destinação preferencial a instituições de ensino públicas, organizações não governamentais e demais entidades que tenham finalidade social, devendo ser precedida da avaliação da adequação dos equipamentos e da execução de procedimentos de limpeza e sanitização dos dados (Brasil, 2018).

Independentemente do tipo de destino adotado, o procedimento é finalizado com o registro documental de todas as etapas executadas, assegurando rastreabilidade, governança e conformidade com os princípios da transparência e da prestação de contas exigidos pela LGPD (art. 37) e reforçados pela ISO/IEC 27002:2022. Tal registro inclui desde a verificação do *backup* e da sanitização até a documentação da destinação final, garantindo que o processo de descarte ocorra de forma segura, ética e ambientalmente responsável.

É importante ressaltar que a PNRS, não especifica diretamente a exigência de certificações como ISO 14001 ou ISO/IEC 27001, nem detalha os procedimentos para emissão do Atestado de Destinação Final (ADF). No entanto, a legislação estabelece diretrizes gerais para a gestão ambiental e a responsabilidade compartilhada pelo ciclo de vida dos produtos, que implicam na necessidade de práticas de gestão ambiental adequadas. A PNRS também determina que as empresas devem elaborar e implementar Planos de Gerenciamento de Resíduos Sólidos (PGRS), conforme o artigo 33 da lei (Brasil, 2010).

A emissão do ADF é regulamentada pelo Sistema Nacional de Informações sobre a Gestão dos Resíduos Sólidos (SINIR), que integra o sistema de monitoramento da Política Nacional de Resíduos Sólidos. Esse sistema exige que as empresas responsáveis pela destinação final de resíduos estejam devidamente licenciadas e cadastradas no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras e Utilizadoras de Recursos Ambientais (CTF/APP), conforme previsto no art. 33 da Lei nº 12.305, de 2 de agosto de 2010 (Brasil, 2010).

Portanto, para garantir conformidade com a PNRS, é fundamental que a empresa responsável pela destinação final de resíduos possua licenciamento ambiental, esteja cadastrada no CTF/APP, apresente como boas práticas, certificações como ISO 14001 e ISO/IEC 27001, e emita o ADF por meio do SINIR, conforme ilustrado a Figura 29.

Figura 29 - Encaminhamento de dispositivos para empresas certificadas

Fonte: elaboração própria, 2025.

Inicialmente, deve-se realizar a verificação do licenciamento ambiental da empresa receptora (art. 20), bem como a confirmação de seu registro ativo no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais (CTF/APP) (art. 17, §1º), conforme dispõe a Lei n. 15.190 (Brasil, 2025). A terceira etapa envolve a avaliação das certificações internacionais, como a ISO 14001, que atesta a conformidade com sistemas de gestão ambiental, e a ISO/IEC 27001, voltada à segurança da informação — ambas contribuindo para a confiabilidade do processo. Por fim, exige-se o fornecimento do Atestado de Destinação Final (ADF) ou documento equivalente (art. 9º, IV), previsto na mesma legislação, como comprovação de que o descarte foi realizado de forma ambientalmente adequada.

Todas as etapas do processo devem ser documentadas para assegurar rastreabilidade, governança, prestação de contas e auditoria. A LGPD exige o registro das operações de tratamento de dados pessoais; a ISO/IEC 27001 orienta a manutenção de evidências de

conformidade; a ISO/IEC 27002:2022 recomenda o uso de ferramentas automatizadas para identificar, classificar e registrar ativos. Do ponto de vista ambiental, a PNRS impõe o controle e registro do fluxo de resíduos, garantindo rastreabilidade até a destinação final. O ciclo de descarte se encerra quando todas as etapas são cumpridas, assegurando conformidade legal, técnica e ambiental, e garantindo que o processo atendeu aos requisitos de segurança da informação, proteção de dados e gestão ambiental, concluindo-se de forma responsável e sustentável.

O registro das decisões e dos procedimentos adotados é uma etapa indispensável no ciclo de descarte de ativos contendo dados. A norma ISO/IEC 27037 recomenda a manutenção de evidências documentais que assegurem a auditabilidade, a conformidade e a integridade dos processos (Oliveira, 2021), enquanto o artigo 37 da LGPD determina o registro das operações de tratamento de dados pessoais (Brasil, 2018). Esses registros devem conter, no mínimo: data da operação, identificação do ativo descartado, destino definido, método de sanitização utilizado e responsável técnico, garantindo a governança da informação e permitindo auditoria futura, conforme estabelecido pela LGPD, ISO/IEC 27037 e PNRS.

Por fim, o ciclo de descarte somente se encerra quando todas as etapas forem devidamente executadas e documentadas de forma transparente, em conformidade com os princípios da segurança da informação, da proteção de dados pessoais e da sustentabilidade ambiental. Trata-se, portanto, de um procedimento interdisciplinar que exige a articulação coordenada entre os setores técnico, jurídico e administrativo da organização, conforme estabelecido pela Lei Geral de Proteção de Dados Pessoais (Brasil, 2018).

O fluxograma de Procedimentos de Descarte em Ativos Contendo Dados, ao sintetizar visualmente todas as etapas e decisões envolvidas, configura-se como uma ferramenta estratégica essencial para a governança institucional. Ele não apenas orienta o cumprimento das obrigações legais previstas na LGPD, na PNRS e em normas técnicas internacionais, como também promove uma cultura organizacional baseada na segurança da informação, na responsabilidade socioambiental e na transparência dos processos.

Sua importância reside justamente na capacidade de articular, de forma didática e operacional, o tripé que sustenta o descarte ético e responsável: a conformidade legal, que assegura a observância dos marcos normativos; a segurança da informação, que garante a proteção integral dos dados ao longo de todo o ciclo de vida dos ativos; e a sustentabilidade ambiental, que prioriza práticas que minimizem impactos negativos e maximizam o reaproveitamento de recursos.

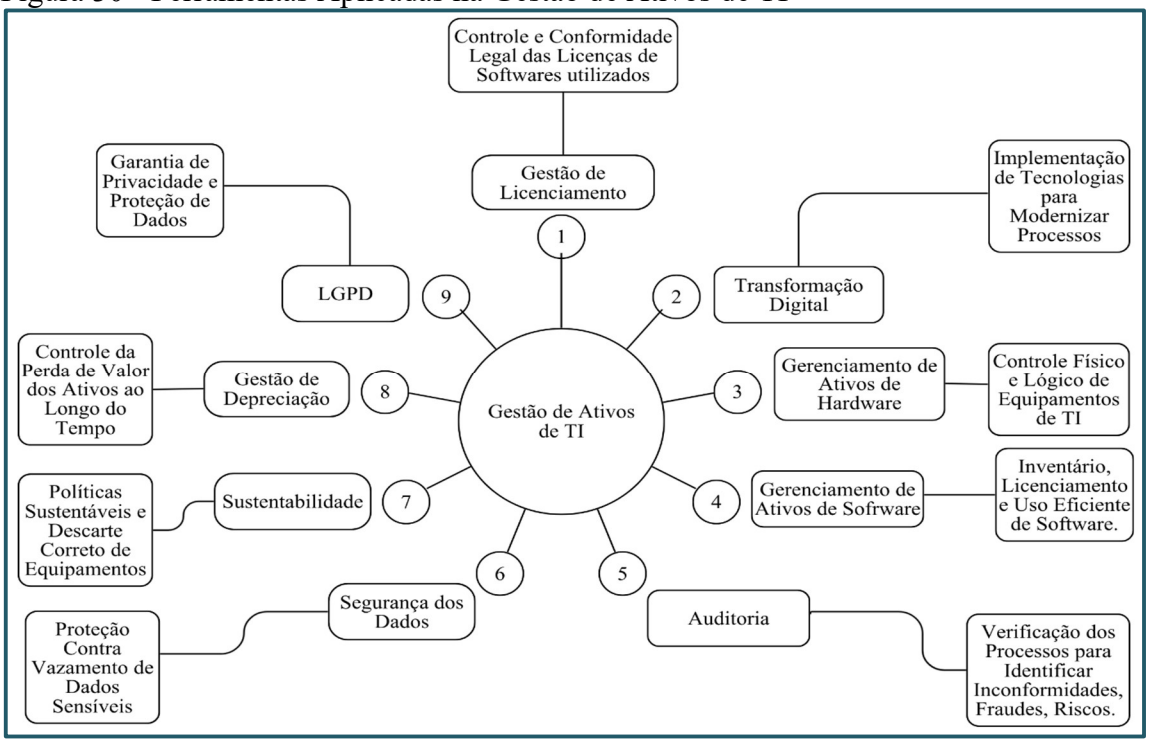
Assim, o fluxograma não é apenas um guia de boas práticas, mas um instrumento que viabiliza a tomada de decisões embasadas, mitigando riscos operacionais, jurídicos e

reputacionais. Ele contribui diretamente para a eficiência organizacional, o cumprimento da legislação e o fortalecimento da responsabilidade institucional frente aos desafios contemporâneos da gestão de ativos e dados. Portanto, sua adoção sistemática deve ser entendida como um compromisso estratégico com a proteção da informação, a sustentabilidade e a ética no uso da tecnologia.

4.2.5 PDCA Aplicado à Gestão de Ativos de Informação

Antes de iniciar a apresentação do processo de elaboração dos fluxogramas desenvolvidos, torna-se necessário destacar uma visão conceitual da Gestão de Ativos de TI, com foco nos principais eixos temáticos que orientam as boas práticas identificadas ao longo da pesquisa. A Figura 30 apresenta uma representação visual que atua como mapa conceitual da abordagem interdisciplinar adotada, relacionando aspectos técnicos, jurídicos e ambientais. Nessa representação, observa-se um conjunto integrado de nove ferramentas desenvolvidas pela empresa Magma3 (s.d.), voltadas à Gestão de Ativos de Tecnologia da Informação. Essas ferramentas abrangem dimensões legais, operacionais, ambientais e de segurança, promovendo a conformidade, a eficiência e a sustentabilidade dos processos organizacionais.

Figura 30 - Ferramentas Aplicadas na Gestão de Ativos de TI



Fonte: elaboração própria, 2025 adaptada de Magma3 [2025][53] .

[53] Magma3 trata-se de ferramentas de gestão de TI desenvolvidas pela empresa Magma.

Considerando o demonstrado na Figura 30, descrevem-se formalmente os elementos representados pelos números:

1) LGPD: Trata-se da aplicação dos princípios e exigências da LGPD, com ênfase na garantia da privacidade e proteção dos dados pessoais e sensíveis armazenados nos ativos de TI. Essa ferramenta envolve o controle de acesso, o tratamento legítimo das informações e a adoção de medidas técnicas e organizacionais para mitigar riscos de vazamento e uso indevido. Alinha-se diretamente às diretrizes da ISO/IEC 27701, complementando o SGSI com práticas voltadas à proteção da privacidade.

2) Gestão de Licenciamento: Refere-se ao controle e à conformidade legal das licenças de *software* utilizadas pela organização. Essa ferramenta busca evitar o uso indevido ou não autorizado de programas, reduzindo os riscos de penalidades legais e assegurando que os contratos com fornecedores de *software* estejam sendo respeitados. Está em conformidade com os princípios de responsabilização e prestação de contas da LGPD, bem como com os controles recomendados na ISO/IEC 27002, relacionados à gestão de ativos e conformidade regulatória.

3) Transformação Digital: Consiste na implementação de tecnologias que visam à modernização dos processos internos da organização. A ferramenta propicia ganhos em eficiência e inovação, por meio da digitalização, automação e integração de sistemas, favorecendo uma atuação mais dinâmica e alinhada às demandas contemporâneas. Este processo, quando realizado com atenção à proteção de dados e à segurança da informação, encontra respaldo nas diretrizes da ISO/IEC 27001, especialmente quanto ao planejamento e controle de mudanças no ambiente digital.

(4) Gerenciamento de Ativos de *Hardware:* Abrange o controle físico e lógico dos equipamentos de TI, desde a aquisição até o descarte. Envolve o inventário detalhado dos ativos, a rastreabilidade de sua localização e o monitoramento do estado operacional dos equipamentos, com o objetivo de garantir sua disponibilidade e prolongar sua vida útil. Essa prática está alinhada à ISO/IEC 27002, que orienta a gestão de ativos físicos e de informação, e à PNRS, que estabelece a responsabilidade compartilhada pelo ciclo de vida dos produtos, especialmente quanto ao descarte ambientalmente adequado.

5) Gerenciamento de Ativos de *Software:* Responsável pelo inventário, licenciamento e uso eficiente dos *softwares* instalados nos ambientes corporativos. Essa ferramenta visa otimizar custos, evitar redundâncias e garantir que os sistemas utilizados estejam atualizados e em conformidade com as políticas internas e exigências legais. Está em conformidade com a

ISO/IEC 27002, quanto ao controle de *software* autorizado, e atende à LGPD, por assegurar que os dados processados estejam sob a gestão transparente e responsável.

6) Auditoria: Trata-se da verificação sistemática dos processos relacionados à gestão de ativos de TI, com foco na identificação de inconformidades, fraudes, riscos e oportunidades de melhoria. A auditoria contribui para a integridade dos processos e para a manutenção da governança corporativa. A conformidade com a ISO/IEC 27001 e ISO/IEC 27006 é fundamental para garantir que os processos sejam auditáveis, seguros e baseados em evidências, e que a organização esteja em conformidade com a LGPD e demais legislações pertinentes.

7) Segurança de Dados: Envolve a proteção contra o vazamento de dados sensíveis, por meio da aplicação de políticas e controles técnicos voltados à confidencialidade, integridade e disponibilidade das informações. Podem ser adotadas medidas como criptografia, controle de acessos, autenticação robusta e monitoramento contínuo. Essa ferramenta segue os princípios da LGPD e é amplamente estruturada com base nas normas ISO/IEC 27001, 27002 e 27040, que estabelecem requisitos e controles para garantir a segurança da informação, incluindo ambientes de armazenamento físico e em nuvem.

8) Sustentabilidade: Refere-se à adoção de práticas sustentáveis no uso e descarte dos ativos de TI, alinhando-se à PNRS. Essa ferramenta promove o reuso de equipamentos, a reciclagem e, ainda, o descarte ambientalmente correto, minimizando os impactos negativos ao meio ambiente e favorecendo a economia circular. A conformidade com a PNRS também reforça os princípios de responsabilidade ambiental e logística reversa, integrando aspectos sociais e ecológicos à gestão de ativos.

9) Gestão de Depreciação: Diz respeito ao controle da perda de valor dos ativos ao longo do tempo, permitindo que a organização planeje adequadamente a substituição de equipamentos obsoletos e avalie o custo-benefício de sua manutenção. Essa ferramenta também contribui para o planejamento financeiro e para a valorização contábil dos ativos. Está alinhada à ISO/IEC 27001, no que se refere à gestão do ciclo de vida dos ativos, e aos princípios de eficiência operacional exigidos pela LGPD e pela PNRS, ao evitar o uso prolongado de equipamentos que possam comprometer a segurança das informações e o meio ambiente.

A integração das nove ferramentas descritas, na gestão de ativos de TI desenvolvida pela empresa Magma3, evidencia uma abordagem multidimensional, capaz de alinhar tecnologia, segurança, legalidade, sustentabilidade e governança organizacional. Cada uma das ferramentas cumpre um papel estratégico na conformidade com a LGPD, com a PNRS e com as diretrizes da família ISO/IEC 27000, fortalecendo os pilares da proteção da informação, da responsabilidade socioambiental e da gestão eficiente dos recursos tecnológicos.

Ao contemplar desde a proteção de dados até a depreciação patrimonial, passando pela segurança, licenciamento, auditoria, sustentabilidade e transformação digital, a solução promove uma gestão integrada e proativa dos ativos de TI. Tal abordagem contribui não apenas para o cumprimento de requisitos legais e normativos, mas também para a construção de uma cultura organizacional voltada à transparência, eficiência operacional, mitigação de riscos e responsabilidade corporativa.

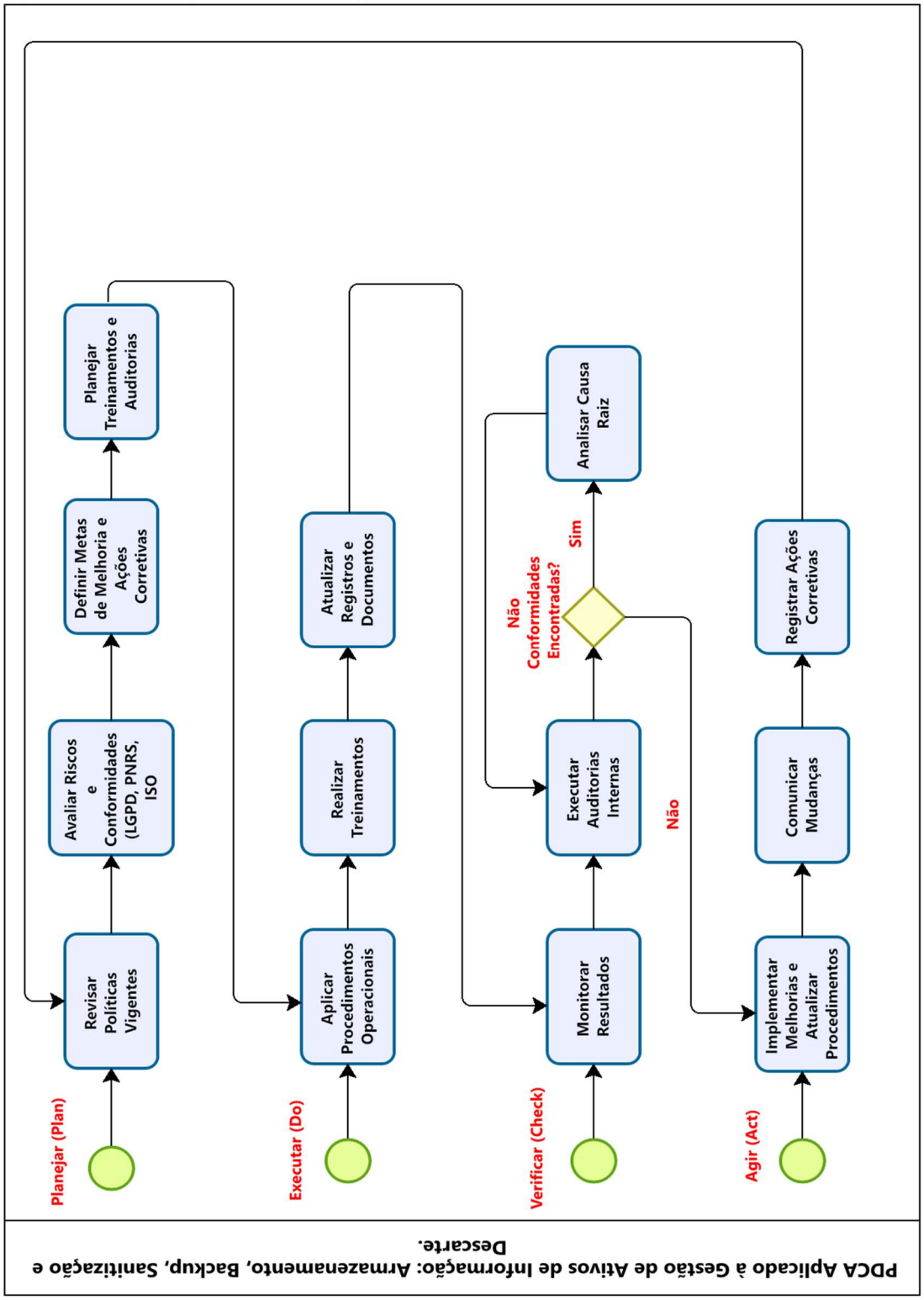
Dessa forma, a aplicação dessas ferramentas, citadas como exemplo, representa um modelo de boas práticas, que pode ser aplicado por organizações públicas e privadas em um cenário cada vez mais exigente quanto à segurança da informação, à proteção de dados pessoais e ao impacto ambiental do ciclo de vida dos EEE. A experiência da empresa Magma3, portanto, constitui uma referência relevante na busca por soluções inovadoras, sustentáveis e juridicamente alinhadas às normas vigentes.

Na pesquisa a escolha dos cinco procedimentos específicos — armazenamento, *backup*, sanitização, descarte e gestão com PDCA — foi orientada pela necessidade de abordar etapas críticas que, em conjunto, formam o percurso completo de uso, proteção e descarte de dispositivos contendo dados sensíveis. Esses procedimentos foram selecionados por corresponderem às fases que apresentam maior risco de exposição indevida de informações e que exigem, portanto, cuidados rigorosos de segurança da informação, alinhados à LGPD e normas internacionais. Além disso, trata-se de práticas que, quando mal executadas, podem acarretar impactos ambientais, em desacordo com os princípios da PNRS.

Quanto a ordem sequencial adotada — Armazenamento → *Backup* → Sanitização → Descarte → Gestão Cíclica com PDCA — reflete a lógica natural do ciclo de vida de ativos de dados, considerando tanto a cronologia das ações quanto os níveis de controle exigidos em cada etapa, construindo o percurso estratégico necessário para garantir a segurança dos dados e a responsabilidade ambiental no manejo de equipamentos obsoletos.

O fluxograma da Figura 31 baseia-se no ciclo PDCA aplicado à gestão de ativos de informação. Estrutura utilizada para a gestão de processos com foco na melhoria contínua e na governança de sistemas organizacionais. A abordagem da gestão de ativos de informação, conforme proposta nesta pesquisa, foi organizada de maneira integrada à lógica do ciclo PDCA, proporcionando uma estrutura contínua voltada à proteção de dados e à sustentabilidade no uso de dispositivos tecnológicos.

Figura 31 - Fluxograma PDCA Aplicado à Gestão de Ativos de Informação



Fonte: elaborado pelo autor, 2025.

O modelo ilustrado compreende quatro etapas principais, cada uma com funções específicas e complementares, permitindo o alinhamento entre os eixos técnicos, jurídicos e ambientais que permeiam o ciclo de vida dos ativos informacionais.

A primeira etapa do fluxograma, denominada “Planejar / *Plan*”, corresponde ao momento de estruturação estratégica e normativa das ações que conduzirão o processo de descarte responsável de ativos contendo dados. Essa fase inicial é essencial para garantir que todas as etapas subsequentes estejam em conformidade com os marcos legais, técnicos e ambientais aplicáveis.

Nesse estágio, são executadas quatro ações. A primeira é *Revisar Políticas Vigentes*, sobretudo aquelas relacionadas à gestão do ciclo de vida de ativos, segurança da informação e sustentabilidade. A segunda é *Avaliar Riscos e Conformidades*, com foco na identificação de vulnerabilidades, impactos legais, operacionais e ambientais decorrentes do descarte inadequado de ativos. Portanto, é feita a verificação de conformidades com a LGPD — em especial os princípios previstos no artigo 6º, que tratam da finalidade, necessidade, segurança, prevenção, responsabilização e prestação de contas no tratamento de dados pessoais — e com a PNRS, notadamente os dispositivos que priorizam a não geração, redução, reutilização, reciclagem e tratamento de resíduos sólidos antes da disposição final ambientalmente adequada. Também cabe o alinhamento às normas internacionais ISO/IEC, como a 27001 (sistema de gestão da segurança da informação), a 27002 (controles de segurança da informação) e a 27701 (extensão da 27001 voltada à privacidade da informação).

Com base nessas diretrizes, a terceira ação é *Definir Metas de Melhoria e Ações Corretivas*. Essa atividade tem por objetivo estabelecer indicadores mensuráveis de desempenho e identificar lacunas nos processos atuais, propondo medidas que corrijam falhas ou riscos identificados nas fases de avaliação e diagnóstico. No caso do fluxograma elaborado entre as ações corretivas possíveis estão, por exemplo, a atualização de protocolos de sanitização de dados que estejam obsoletos, a revisão de fluxos de aprovação para o descarte de ativos com dados sensíveis, ou ainda a criação de procedimentos específicos para tratamento diferenciado de equipamentos com maior criticidade informacional. Ao definir metas claras, como reduzir o tempo médio de descarte ou aumentar o percentual de ativos reaproveitados, a instituição orienta suas práticas à melhoria contínua e à conformidade normativa.

A quarta e última ação desta etapa corresponde ao *Planejamento de Treinamentos e Auditorias*. Os treinamentos têm como finalidade capacitar as equipes envolvidas — tanto técnicas quanto administrativas — nos procedimentos exigidos para o descarte responsável, incluindo critérios legais, ambientais e de segurança da informação. Já as auditorias internas visam verificar o cumprimento das diretrizes definidas, identificar não conformidades e promover a rastreabilidade de todas as decisões e ações executadas ao longo do processo. Essas

auditorias também fortalecem a governança institucional, demonstrando compromisso com os princípios da LGPD e da PNRS.

Enfim, como se pode ressaltar na primeira etapa do PDCA, planejar adequadamente significa, portanto, estabelecer uma base sólida e documentada para todo o processo de descarte, orientando as ações futuras com foco na legalidade, na eficiência operacional, na minimização de riscos e na promoção da sustentabilidade ambiental e institucional. A fase de planejamento é determinante para o alinhamento entre objetivos institucionais e exigências normativas, sobretudo em ambientes onde a governança da informação impacta diretamente direitos fundamentais.

Seguindo o fluxo do PDCA, a segunda etapa, "Executar / Do", compreende três ações principais: aplicar procedimentos operacionais, realizar treinamentos e atualizar registros e documentos. A primeira ação refere-se à *Aplicação dos Procedimentos Operacionais* definidos na fase de planejamento. São operacionalizados os procedimentos técnicos que correspondem diretamente aos fluxogramas apresentados nesta dissertação. Isso inclui a verificação da necessidade de descarte, a realização de *backup*, a sanitização dos ativos, a definição da destinação (reuso, doação, reciclagem ou descarte final) e o respectivo registro das ações executadas. Também são executadas práticas de armazenamento seguro, descaracterização física, descarte ambientalmente adequado e comunicação com as partes envolvidas, conforme os critérios estabelecidos pelas normas ISO/IEC 27040 e ISO 14001 e pelos artigos 6º e 46 da LGPD.

A segunda ação compreende a realização dos *Treinamentos Previamente Planejados*. Esta atividade busca garantir que os colaboradores envolvidos na gestão e no descarte de ativos com dados estejam capacitados para executar as tarefas com segurança, precisão e em conformidade com marcos legais. Além dos treinamentos técnicos, podem ser promovidos encontros interdisciplinares para abordar aspectos legais, ambientais e éticos do descarte, reforçando a cultura institucional de responsabilidade e prevenção.

A terceira ação consiste na *Atualização de Registros e Documentos*. Após a execução das atividades, é necessário formalizar os procedimentos realizados, registrando datas, responsáveis, métodos aplicados e evidências da conformidade técnica e legal. Essa documentação garante a rastreabilidade, a prestação de contas *(accountability*) e a possibilidade de auditoria dos processos, conforme orientam Miragem (2019) e as diretrizes da ISO/IEC 27701:2020. A manutenção desses registros também se articula com o princípio da responsabilização e prestação de contas previsto no artigo 6º da LGPD, fortalecendo a governança de dados da instituição.

A etapa *Do* representa, portanto, a materialização prática dos planejamentos e políticas formulados anteriormente, transformando diretrizes abstratas em ações concretas e mensuráveis. Ao executar os procedimentos definidos com rigor técnico e documental, a instituição avança em direção à conformidade legal, à segurança da informação e à sustentabilidade ambiental.

A terceira etapa do ciclo é *Verificar / Check* e tem como objetivo avaliar os resultados obtidos na execução dos procedimentos e identificar eventuais falhas. No fluxograma elaborado foram estabelecidas duas ações diretas: monitorar os resultados e executar auditorias internas. Caso os procedimentos não estejam em conformidade, realiza-se a análise da causa raiz e, após sua correção, executam-se novamente as auditorias internas para, então, seguir à última etapa do ciclo PDCA (*Act*).

A ação de *Monitorar os Resultados* ocorre por meio da observação e análise de indicadores previamente definidos, que permitem medir o desempenho dos processos e identificar desvios. Esses indicadores podem incluir, por exemplo, a quantidade de equipamentos descartados sem sanitização adequada, o tempo médio para execução dos *backups* ou o número de registros formalizados por descarte.

Em seguida, inicia-se a *Realização das Auditorias Internas*, conforme previsto nas normas ISO/IEC 27001 e 27002. As auditorias devem verificar se os procedimentos foram executados conforme os planos estabelecidos, se os registros foram devidamente atualizados e se os critérios de conformidade técnica, legal e ambiental foram cumpridos.

Em caso de não conformidades, o processo segue para a *Análise da Causa Raiz*, permitindo compreender as origens dos desvios e elaborar respostas mais eficazes. Esse aspecto é um dos principais diferenciais do ciclo PDCA em relação aos fluxogramas anteriores: ele incorpora mecanismos de controle interno que possibilita a retroalimentação do sistema e o aprimoramento contínuo. Segundo Burkart (2021), a verificação sistemática da conformidade é essencial para mitigar riscos e evitar sanções legais, sobretudo em contextos regulados por legislações como a LGPD.

A importância dessa etapa também reside no fato de que tanto a LGPD quanto a PNRS impõem obrigações contínuas de monitoramento e responsabilização. O artigo 6º da LGPD estabelece os princípios da segurança e da prestação de contas, exigindo que os agentes de tratamento comprovem a adoção de medidas eficazes para proteção dos dados. Já o artigo 9º da PNRS exige o controle dos processos de gerenciamento de resíduos, priorizando ações preventivas e corretivas com vistas à sustentabilidade. As normas ISO, por sua vez, reforçam a

importância da avaliação periódica, auditorias e ajustes contínuos, promovendo a integridade e a eficácia dos sistemas de gestão.

Por fim, a etapa *Act* encerra o ciclo com três ações principais: *Implementar Melhorias e Atualizar os Procedimentos Operacionais; Comunicar as Mudanças às Equipes Envolvidas; e registrar formalmente as ações corretivas* adotadas. A primeira ação refere-se à incorporação prática das lições aprendidas nas etapas anteriores, revisando os protocolos à luz dos resultados verificados e das não conformidades identificadas. Um exemplo é a revisão de rotinas de sanitização caso auditorias tenham apontado falhas no uso de ferramentas homologadas, o que exige atualização de procedimentos conforme a ISO/IEC 27040.

A ação de *comunicação das mudanças* visa garantir que todos os setores impactados estejam cientes das atualizações, promovendo alinhamento institucional e evitando a reincidência de falhas — como no caso da divulgação de novos critérios para descarte, conforme alterações na PNRS ou em regulamentos ambientais estaduais.

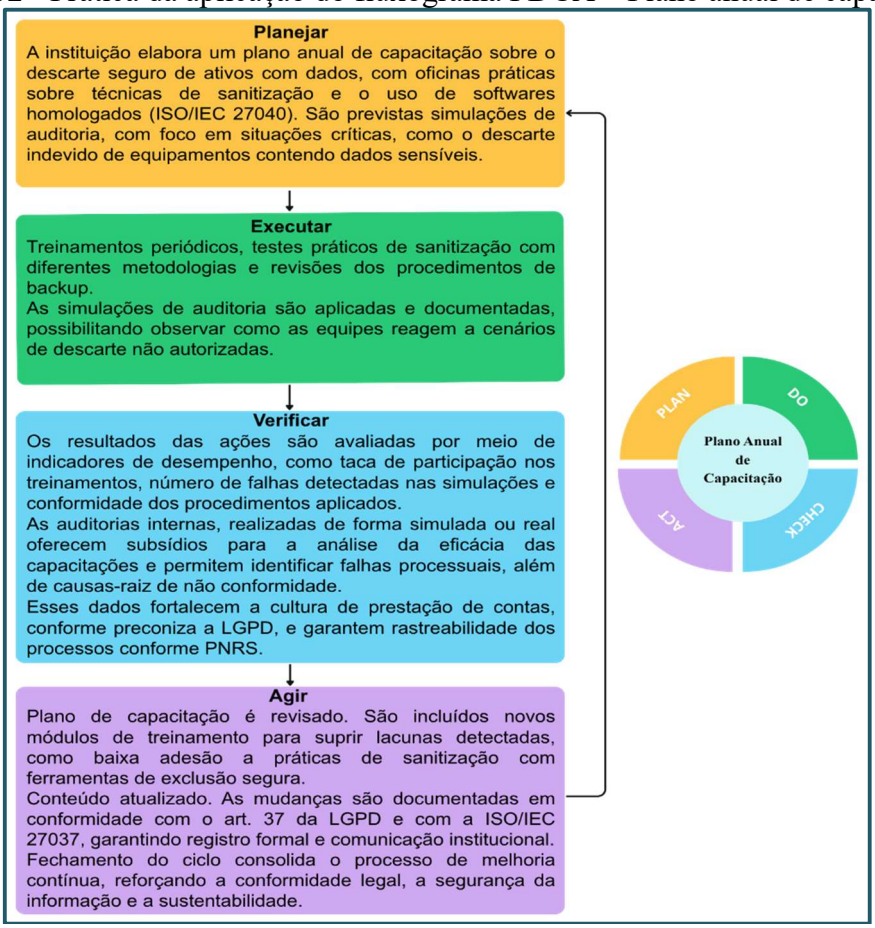
Por fim, o registro formal das ações corretivas, por sua vez, assegura a rastreabilidade e a transparência do processo, em alinhamento com o artigo 37 da LGPD, que exige o registro das operações de tratamento de dados pessoais, inclusive sua exclusão definitiva. Além disso, esse registro atende às recomendações da ISO/IEC 27037 quanto à preservação de evidências de conformidade.

Ao estabelecer um retorno estruturado à etapa de planejamento, o ciclo PDCA promove a melhoria contínua, permitindo a evolução dos procedimentos e a adaptação constante às mudanças tecnológicas, normativas e ambientais. Conforme argumentam Leme e Blanck (2020), a efetividade de sistemas de proteção de dados depende diretamente da capacidade organizacional de responder ativamente às transformações, ajustando seus protocolos e fortalecendo a cultura institucional de segurança da informação.

Portanto, o fluxograma PDCA aplicado à gestão de ativos de informação — armazenamento, *backup*, sanitização e descarte — representado na Figura 32 consolida os procedimentos anteriormente tratados — de forma isolada — em uma estrutura integrada de governança, que orienta a gestão dos ativos de informação por meio de um ciclo contínuo de planejamento, execução, verificação e ação.

Diante do exposto, como exemplo de uma boa prática aplicável ao fluxograma PDCA, pode-se citar a criação de um Plano Anual de Capacitação sobre Descarte Seguro de Ativos de Dados, ilustrado na Figura 32.

Figura 32 - Prática da aplicação do fluxograma PDCA – Plano anual de capacitação



Fonte: elaboração própria, 2025.

Conforme o exemplo, na etapa *Plan*, a instituição elabora o Plano Anual, incorporando oficinas práticas sobre sanitização e uso de *softwares* homologados, alinhadas às orientações da ISO/IEC 27040:2015. Esse plano pode incluir também a simulação de auditorias para avaliar a resposta das equipes a situações críticas, como o descarte não autorizado de equipamentos com dados sensíveis, promovendo a cultura de prevenção e a conformidade contínua com as normas vigentes.

Dando continuidade ao exemplo citado, o Plano Anual pode ser executado na *Do.* Esta fase ocorre por meio de cronogramas de treinamentos periódicos, simulados de descarte, testes de sanitização com diferentes metodologias e revisões práticas de protocolos de *backup*. Ainda, a simulação de auditorias pode ser registrada e avaliada, servindo como insumo para a próxima etapa do ciclo. Essa prática contribui para criar um ambiente institucional que valoriza a prevenção de incidentes e assegura a conformidade dos procedimentos executados, consolidando a efetividade da política de descarte responsável de ativos com dados.

Na sequência, na etapa *Check*, os resultados dessas ações são monitorados por meio de indicadores de desempenho e auditorias internas, permitindo avaliar a adesão, a eficácia dos

treinamentos e a conformidade dos procedimentos executados. A simulação de auditorias, além de promover a cultura de prevenção, fornece registros valiosos que, ao serem analisados, possibilitam identificar falhas e realizar a análise da causa raiz. Essa abordagem fortalece a conformidade com a LGPD, que exige prestação de contas e segurança contínua, e com a PNRS, que demanda controle e rastreabilidade dos processos. Dessa forma, a verificação sistemática consolida a efetividade da política de descarte responsável e fornece insumos para as ações corretivas e de melhoria contínua que caracterizam a última etapa do ciclo PDCA.

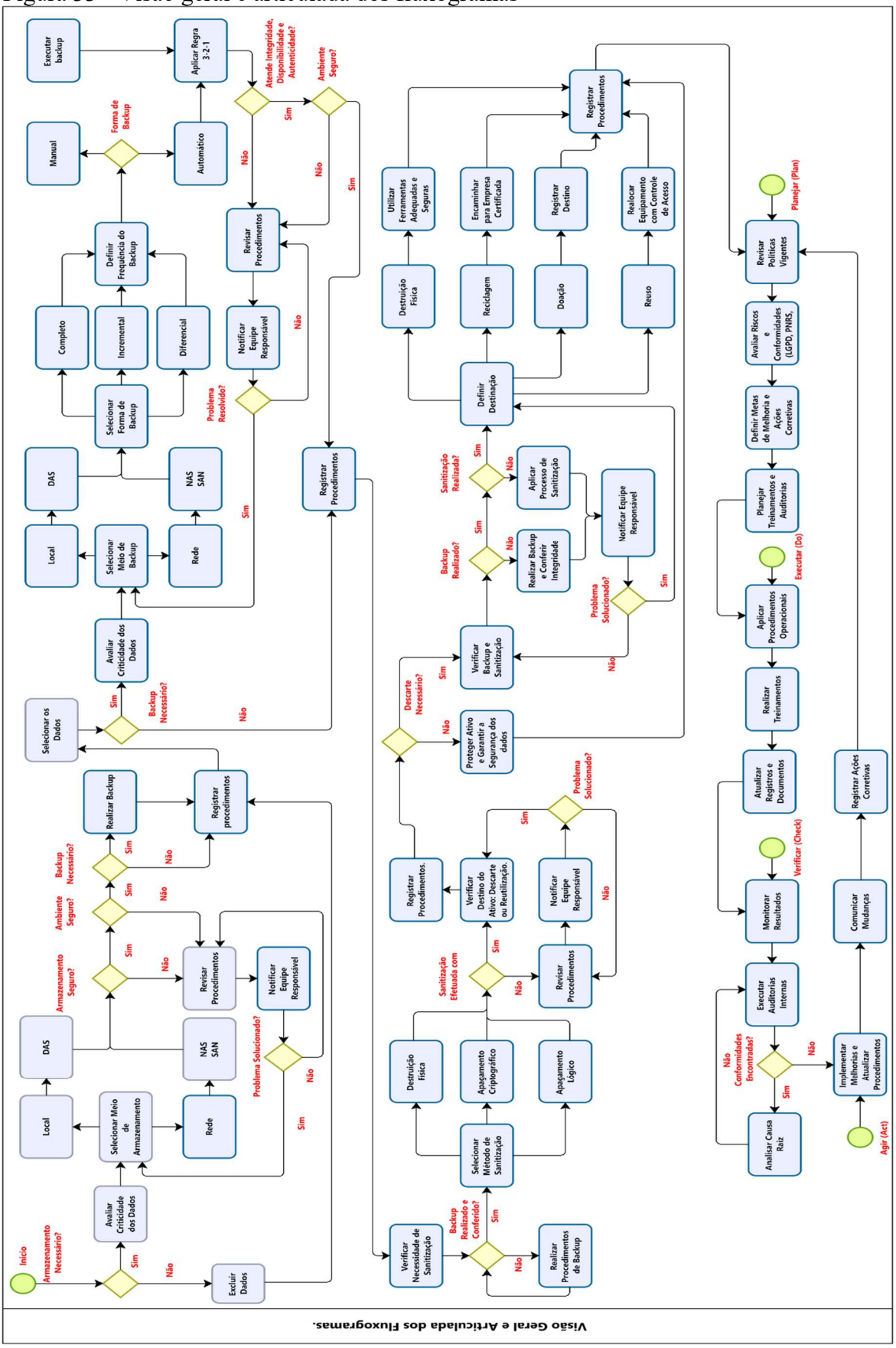
Na etapa *Act*, o Plano Anual é revisado com base nos resultados monitorados na fase anterior. A partir dos indicadores de desempenho e das análises das auditorias simuladas realizadas na etapa *Check*, identificam-se pontos de melhoria, como conteúdos que não foram plenamente assimilados pelas equipes, oficinas com baixa efetividade prática ou necessidade de reforçar determinados procedimentos, como a sanitização de mídias obsoletas. Com essas evidências, o conteúdo do plano é atualizado, novos módulos de treinamento são incluídos — por exemplo, abordando alterações normativas recentes ou incorporando falhas reais identificadas nos simulados — e o cronograma é ajustado para contemplar lacunas de capacitação.

As modificações são formalmente documentadas, atendendo ao artigo 37 da LGPD e à ISO/IEC 27037, e comunicadas às equipes responsáveis, assegurando a disseminação institucional do conhecimento atualizado. Esse fechamento cíclico permite o aprimoramento contínuo da prática educativa, reforça a cultura de prevenção e garante maior aderência aos princípios da LGPD e aos compromissos da PNRS, promovendo uma política de descarte de ativos com dados cada vez mais eficazes e responsiva.

Pela explicação do fluxograma e pelo exemplo de boa prática, pode-se considerar que ao propor esse modelo, a pesquisa reforça a necessidade de adoção de mecanismos institucionais que articulem os diferentes eixos da proteção informacional: a conformidade legal (LGPD), a segurança técnica (ISO/IEC) e a responsabilidade socioambiental (PNRS). Trata-se, assim, de um modelo interdisciplinar que qualifica a gestão institucional dos dados e dos dispositivos, promovendo tanto a proteção de direitos quanto à sustentabilidade organizacional.

O último fluxograma apresenta uma visão geral e consolidada das práticas voltadas ao descarte seguro e sustentável de ativos. Ele integra os fluxogramas anteriores em um modelo unificado, no qual os cinco processos — armazenamento, backup, sanitização, descarte e ciclo PDCA — estão representados de forma articulada, mas também podem ser executados de maneira independente, conforme a necessidade de cada organização, conforme Figura 33.

Figura 33 - Visão geral e articulada dos fluxogramas



Fonte: elaboração própria, 2025.

5 CONSIDERAÇÕES FINAIS

A presente dissertação atingiu seu objetivo central ao identificar e analisar tanto as exigências legais quanto às boas práticas ambientais e técnicas relacionadas ao descarte seguro e sustentável de ativos contendo dados. A partir dessa abordagem interdisciplinar, demonstrou-se que a proteção de dados pessoais, a segurança da informação e a sustentabilidade ambiental constituem dimensões indissociáveis na gestão do ciclo de vida de ativos de Tecnologia da Informação. Essa análise culminou na elaboração de um Manual de Boas Práticas, fundamentado na LGPD, na PNRS e nas diretrizes da família de normas ISO/IEC 27000.

A construção e validação dos fluxogramas orientativos possibilitam representar sistematicamente procedimentos-chave — como *backup*, armazenamento, sanitização e descarte final — essenciais para garantir a rastreabilidade, integridade e conformidade em todas as fases do ciclo PDCA. Dessa forma, tais fluxogramas reforçaram a melhoria contínua, o caráter preventivo e a capacidade de resposta das organizações diante de riscos operacionais, regulatórios e ambientais, consolidando uma política institucional de governança de dados. Assim, constatou-se que o descarte de ativos contendo dados não se resume a uma prática operacional, mas se consolida como uma política estratégica de governança da informação, essencial para organizações que buscam conformidade legal, segurança informacional e responsabilidade socioambiental.

Nesse sentido, os fluxogramas elaborados e validados, além de orientarem tecnicamente os procedimentos internos, expressam uma visão integrada que reconhece a responsabilidade das organizações perante a sociedade, o meio ambiente e a legislação vigente. Essa perspectiva reforça a necessária articulação entre os campos jurídico, tecnológico e ambiental na gestão do descarte de ativos contendo dados. Nesse contexto, a LGPD encontra respaldo nas diretrizes internacionais da família de normas ISO/IEC 27000 e exige que instituições públicas e privadas adotem salvaguardas técnicas e organizacionais que assegurem a confidencialidade, integridade e disponibilidade das informações ao longo de todo o ciclo de vida dos ativos, especialmente no que se refere à segurança da informação e à gestão de riscos.

Sob o aspecto legal, a LGPD impõe obrigações quanto à finalidade, necessidade, transparência e responsabilização nas operações de tratamento de dados, incluindo sua exclusão. No campo técnico, as normas ISO/IEC — especialmente as séries 27001, 27002, 27037, 27040 e 27701 — oferecem diretrizes robustas para assegurar a rastreabilidade, a confidencialidade e a integridade das informações, desde a coleta até o descarte. Já no eixo ambiental, a PNRS e o Decreto nº 10.240/2020 reforçam um modelo de gestão ambientalmente

responsável, no qual se preza o compromisso com a destinação final adequada, a prevenção da poluição digital e o reuso ou reciclagem de equipamentos, respeitando o princípio da responsabilidade compartilhada.

A integração entre proteção de dados, segurança da informação e sustentabilidade ambiental, portanto, não deve ser compreendida como sobreposição de obrigações, mas como uma estratégia convergente importante de uma gestão ética e sustentável dos dados e ativos de informação. Ao promover esse procedimento interdisciplinar, este estudo contribui não apenas para o debate acadêmico sobre proteção de dados e descarte de ativos, mas também para o aprimoramento prático das políticas internas de tratamento de dados, fortalecendo a cultura organizacional de prevenção, responsabilidade e melhoria contínua.

Dessa forma, como concretização prática da contribuição dessa pesquisa para a implementação efetiva das políticas de descarte seguro e responsável de ativos tecnológicos, idealizou-se o Manual de Boas Práticas. Esse manual se fundamentou na associação entre um olhar socialmente cuidadoso sobre a proteção dos dados e as obrigações impostas pela LGPD, aliado às normativas recomendadas pela família ISO/IEC para garantir a segurança das informações e qualidade dos serviços técnicos e à responsabilidade ambiental compartilhada proposta pela PNRS, que visa mitigar impactos ambientais a partir de práticas eficazes e destinação final adequada.

5.1 LIMITAÇÃO DO ESTUDO

O estudo contribuiu para o avanço da compreensão sobre o descarte adequado de ativos de tecnologia da informação, considerando os marcos regulatórios da LGPD, da PNRS e das normas da família ISO/IEC 27000. Entretanto, algumas limitações precisam ser reconhecidas.

A investigação restringiu-se à análise bibliográfica e documental, não contemplando estudos de caso ou pesquisas empíricas que permitissem verificar, em contextos reais, a aplicabilidade prática das diretrizes e fluxogramas propostos. Essa ausência de validação em campo limita a aferição da efetividade das recomendações em diferentes tipos de organizações, sejam públicas, privadas, de grande ou pequeno porte.

Além disso, a pesquisa priorizou práticas consolidadas de *backup*, sanitização e descarte, sem aprofundar soluções tecnológicas emergentes, como *blockchain* e inteligência artificial, que podem ampliar a rastreabilidade e a governança de dados. Também não foram explorados os impactos da rápida obsolescência tecnológica, fator crítico que acelera a geração de resíduos eletrônicos e impõe desafios adicionais à sua gestão sustentável.

Outro limite refere-se à ausência de uma análise comparativa internacional. Embora o estudo tenha se apoiado nas normas ISO/IEC, não foram investigadas políticas ou experiências estrangeiras que poderiam enriquecer a discussão e oferecer parâmetros para avaliar a realidade brasileira.

Por fim, variáveis socioeconômicas e culturais que influenciam diretamente a gestão de resíduos eletrônicos no país — como desigualdades regionais na infraestrutura de reciclagem, baixa conscientização social e insuficiente integração de políticas públicas voltadas à inclusão digital e à economia circular — não foram objeto de aprofundamento.

5.2 TRABALHOS FUTUROS

Como perspectiva para pesquisas futuras, considera-se pertinente a realização de investigações empíricas que avaliem, de forma comparativa, o grau de conformidade de organizações públicas e privadas em relação às exigências legais, ambientais e técnicas que regem o descarte de ativos de tecnologia da informação.

Nesse contexto, destaca-se a necessidade de aprofundar a análise sobre a aplicabilidade de tecnologias emergentes, como a inteligência artificial voltada à sanitização de dispositivos, o uso de *blockchain* para assegurar a rastreabilidade dos processos de descarte e reciclagem, bem como a investigação de novos métodos de destruição lógica e física de dados, alinhados às melhores práticas internacionais.

Adicionalmente, estudos futuros podem contemplar análises comparativas com políticas e experiências internacionais, a fim de oferecer parâmetros de avaliação para a realidade brasileira. Sugere-se também o desenvolvimento de estratégias educacionais e programas de conscientização voltados tanto a gestores e colaboradores quanto à sociedade em geral, como meio de consolidar uma cultura de proteção de dados e responsabilidade socioambiental que transcenda o cumprimento normativo e se configure como prática organizacional e cidadã permanente.

REFERÊNCIAS

ALECRIM, E. **O que é GDPR e que diferença isso faz para quem é brasileiro**. [*S. l.*]: Tecnoblog, 2016. Disponível em https://tecnoblog.net/responde/gdpr-privacidade-protecao-dados/. Acesso em: 5 ago. 2025.

ALENCAR, M. G. **Vazamento de dados pessoais em assistência técnica**: responsabilidades e implicações. São Paulo: LGPD brasil.com, 2023. Disponível em: https://www.lgpdbrasil.com.br/vazamento-de-dados-pessoais-em-assistencia-tecnica-responsabilidades-e-implicacoes/. Acesso em: 2 jul. 2024.

ALMEIDA, N. M. C. de. **Resíduos eletroeletrônicos de computadores e periféricos**: mapeamento e análise da gestão no município de Natal-RN. Orientadora: Luciana Figueiredo Lopes Lucena. 2023. 54 f. Trabalho de Conclusão de Curso (Graduação em Ciências e Tecnologia) - Escola de Ciência e Tecnologia, Universidade Federal do Rio Grande do Norte, Natal, 2023. Disponível em: https://repositorio.ufrn.br/items/1c028948-b501-4e73-9a07-16e2d489a581. Acesso em: 3 jul. 2024.

ALVES, C. G. dos S. **Um estudo de ferramentas open-source para perícia forense em dispositivos com Android 14**. 2024. 62 f. Trabalho de Conclusão de Curso (Graduação em Segurança da Informação) – Universidade Federal do Ceará, Itapajé, 2024. Disponível em: https://repositorio.ufc.br/handle/riufc/78917. Acesso em: 3 ago. 2024.

AMANCIO, R.; TREVIZANO, W. A.; PEREIRA, A. A. de S.; DAIBERT, M. S. Monitoramento de backup: conferência de erros durante a realização do backup local. **Revista Científica UNIFAGOC – Multidisciplinar**, Ubá, v. 9, n. 1, 2024. Disponível em: https://revista.unifagoc.edu.br/multidisciplinar/article/view/1216. Acesso em: 7 out. 2025.

AMARAL, A. F. F. **Redes de computadores**. Colatina: Instituto Federal do Espírito Santo, 2012. Disponível: https://proedu.rnp.br/bitstream/handle/123456789/710/Rede%20de%20Computadores_COR_CAPA_FICHA_ISBN_20120229.pdf?sequence=3. Acesso em: 2 ago. 2024.

ANDRADE, L. S. de. **Política de backup e restauração: um estudo de caso em uma cooperativa de trabalho médico**. 2023. 73 f. Monografia (Graduação em Engenharia da Computação) - Instituto de Ciências Exatas e Aplicadas, Universidade Federal de Ouro Preto, João Monlevade, 2023. Disponível em: https://monografias.ufop.br/handle/35400000/6073. Acesso em: jul. 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **ABNT NBR 14724**:2024: Informação e documentação: Trabalhos acadêmicos: Apresentação. Rio de Janeiro, 2023. Disponível em: https://tpp-uff.com.br/wp-content/uploads/2025/02/ABNT_NBR_14724_2024-1.pdf. Acesso em: dez. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **ABNT NBR ISO 9001**:2015: Sistemas de gestão da qualidade: Requisitos. Rio de Janeiro, 2015. Disponível em: http://associacaodeinspetores.com.br/arquivos/arquivo_informativo/c2c76186249e40f1f5da5c8b09582702.pdf. Acesso em: set. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **Sobre a ABNT**: descubra nossa história, missão e valores. Rio de Janeiro: ABNT, [202?]. Disponível em: https://abnt.org.br/institucional/sobre-abnt-2/. Acesso em: jul 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. **Perguntas frequentes – Adequação à LGPD**. 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes/perguntas-frequentes. Acesso em: jan. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: jun. 2025.

BARRETO, J. S.; ZANIN, A.; MORAIS, I. S.; VETTORAZZO, A. S. **Fundamentos de segurança da informação**. Porto Alegre: SAGAH, 2018. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788595025875/. Acesso em: jan. 2025.

BARTOLOMEO, F. **Guia comentado da Lei Geral de Proteção de Dados**: LGPD (13709/18). [*S. l.*]: Direito Digital – Aurum, 2021. Disponível em: https://www.aurum.com.br/blog/lgpd/. Acesso em: jun. 2024.

BESERRA, B. C.; SANTOS, E. R. R. dos.; AMARAL, M. M. do. Invasão de dispositivos informáticos no Ordenamento Jurídico Brasileiro: II Mostra Científica Interdisciplinar do Vale do Araguaia. **Revista Eletrônica Interdisciplinar Barra do Garças – MT**, Barra do Garças-MT, v. 12, ed. Especial, p. 302-305, 2020. Disponível em: http://revista.sear.com.br/rei/article/view/165. Acesso em jun. 2024.

BIZAGI. **Bizagi Modeler**: versão 4.2.0.003. Londres: Bizagi Limited, 2023. Disponível em: https://www.bizagi.com/pt/platform/modeler. Acesso em: jul. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: set. 2024.

BRASIL. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). **Obter acesso ao Portal de Periódicos da CAPES**. Brasília: Capes, 2025. Disponível em: https://www.gov.br/capes/pt-br/acesso-a-informacao/acoes-e-programas/carta-de-servicos-ao-usuario/obter-acesso-ao-portal-de-periodicos-da-capes. Acesso em: 8 out. 2025.

BRASIL. Decreto nº 10.240, de 12 de fevereiro de 2020. Regulamenta a logística reversa de produtos eletroeletrônicos de uso doméstico e seus componentes. **Diário Oficial da União**, Brasília, DF, 13 fev. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10240.htm. Acesso em: set. 2024.

BRASIL. Decreto nº 9.177, de 19 de outubro de 2017. Regulamenta a Lei nº 12.305, de 2 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos. **Diário Oficial da União**: seção 1, Brasília, DF, 20 out. 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9177.htm. Acesso em: set. 2025.

BRASIL. Lei n. 12.305, de 2 de agosto de 2010. Institui a Política Nacional de Resíduos Sólidos; altera a Lei n. 9.605, de 12 de fevereiro de 1998; e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, ano 147, n. 147, p. 3-7, 3 ago. 2010. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12305.htm. Acesso em: set. 2024.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: set. 2024.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: set. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Dispõe sobre o uso da internet no Brasil e estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. **Diário Oficial da União**, Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: set. 2024.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). Lei nº 9.373, DE 11 de maio de 2018. **Centros de Recondicionamento de Computadores – CRCs**. Brasília: MCTI, 2018. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/comunicacao/SETEL/inclusao_digital/CRCs/CRCs.html. Acesso em: jul. 2025.

BRITO, F. R. DE.; BRITO, M. L. de A. Impacto do ciclo PDCA no processo de atendimento aos clientes em empresas de aviamentos. **E-Acadêmica**, Vargem Grande Paulista, v. 1, n. 3, 2020. Disponível em: https://eacademica.org/eacademica/article/view/10. Acesso em fev. 2025.

BURKART, D. V. V. **Proteção de dados e o estudo da LGPD**. 2021. 141 f. Dissertação (Mestrado em Mídia e Tecnologia da Faculdade de Artes, Arquitetura e Comunicação) - Universidade Estadual Paulista Júlio de Mesquita Filho, Bauru, 2021. Disponível em: https://repositorio.unesp.br/server/api/core/bitstreams/bd12b4d0-87b7-4705-9e5d-423cd938a42a/content. Acesso em: 8 set. 2024.

CARDOSO, C. de M.; RÉGIS, J. C. Direito Comparado: LGPD e o Marco Civil da Internet. **Revista de Direito**, [*S. l.*], v. 16, n. 01, p. 1-23, 2024. DOI: 10.32361/2024160116495. Disponível em: https://periodicos.ufv.br/revistadir/article/view/16495. Acesso em: set. 2024.

CARVALHO, A. P. **Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD)**: um estudo de caso para prevenção a fraude no contexto de Big Data. 2021. 215 f. Dissertação (Mestrado Profissional em Engenharia Elétrica) - Universidade

de Brasília, Brasília, 2021. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/01/PPEE.MP_.012-1.pdf. Acesso em out. 2024.

CHOU, E. N. R.; ALBANO, C. J.; ALMEIDA, P. H. de. Lei Geral de Proteção de Dados: uma análise da ISO 27701 como ferramenta de controle para LGPD. **Revista IFES Ciência**, Vitória, v. 10, n. 1, p. 1-15, 2024. Disponível em: https://ojs.ifes.edu.br/index.php/ric/article/view/2445/1132. Acesso em: jun. 2024.

COSTA, I. R.; PINTO, L. F. C. **A evolução dos dispositivos de armazenamento de dados na perspectiva da história**. 2017. Trabalho de Conclusão de Curso (Graduação em Licenciatura em Informática do Campus de Codó) - Universidade Federal do Maranhão, São Luís, 2017. Disponível em: https://monografias.ufma.br/jspui/handle/123456789/2830. Acesso em: jun. 2024.

COSTA, R. A.; CUNHA, C. R. A Lei Geral de Proteção de Dados: um estudo descritivo e exploratório da sua aplicação no Brasil e no cenário internacional. **JURIS FIB**, Bauru, v. 14, n. 14, (Fluxo Contínuo), 21 dez. 2023. DOI: https://doi.org/10.59237/jurisfib.v14i14.653. Disponível em: https://revistas.fibbauru.br/jurisfib/article/view/653. Acesso em: set. 2024.

CULOT, G; NASSIMBENI, G.; PODRECCA, M.; SARTOR, M. A norma de gestão de segurança da informação ISO/IEC 27001: revisão de literatura e agenda de pesquisa baseada em teoria. **The TQM Journal**, [*S. l.*], v. 33, n. 7, p. 76-105. Disponível em: https://www.emerald.com/tqm/article/33/7/76/459175/The-ISO-IEC-27001-information-security-management. Acesso em jan. 2025.

CURY, A. **Organização e métodos**: Uma visão holística. São Paulo: Atlas, 2015.

D'ANGELO, L. G. G.; MOTA, M. P. **Boas práticas no descarte de unidades HDDs e SSDs**. 2024. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Segurança da Informação) – Faculdade de Tecnologia de Americana "Ministro Ralph Biasi", Americana, 2024. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/29722/1/20242S_Lucas%20Gabriel%20Gama%20D%60Angelo_OD2486.pdf. Acesso em: jul. 2025.

DINIZ, A. L. B.; DINIZ, D. P. A ABNT NBR ISO/IEC 27701: 2019 e a segurança da informação. **Revista Eletrônica de Computação Aplicada**, [*S. l.*], v. 2, n. 2, p. 21-39, 2021. Disponível em: http://periodicos.unifacef.com.br/reca/article/view/2302/1604. Acesso em: ago. 2024.

DLA PIPER. **Leis de Proteção de Dados do Mundo**. Portsmouth: iapp, [202?]. Disponível em: https://iapp.org/resources/article/dla-piper-data-protection-laws-of-the-world/. Acesso em: ago. 2025.

DUARTE, T. X. D. **Tecnologia, uso, coleta e tratamento de dados**: o futuro do poder econômico? 2020. 122 f. Dissertação (Mestrado em Direito) - Universidade Nove de Julho, São Paulo, 2020. Disponível em: https://bibliotecatede.uninove.br/bitstream/tede/2399/2/Thaile%20Xavier%20Dantas%20Duarte.pdf. Acesso em: nov. 2024.

ESCOLA SUPERIOR DE REDES. **Fundamentos da segurança da informação**: módulo 1 – conceitos básicos. Brasília: Escola Virtual do Governo, 2025. Disponível em:

https://cdn.evg.gov.br/cursos/1256_EVG/html/modulo01_html01/index.html. Acesso em: abr. 2025.

FEILER, A. R.; GAZANIGA, F.; VIEIRA, T. A. M. O valor fundamental dos dados pessoais: uma análise comparativa entre a LGPD e GDPR sob a ótica da análise econômica do direito. **Revista de Direito**, [*S. l.*], v. 16, n. 02, p. 1-29, 2024. DOI: 10.32361/2024160217158. Disponível em: https://periodicos.ufv.br/revistadir/article/view/17158. Acesso em: dez. 2024.

FERRARI, G. C. B. **Dados pessoais e o lixo**. Belo Horizonte: Centro de Pesquisa em Direito, Tecnologia e Inovação - Centro DTI BR, 2021. Disponível em: https://www.dtibr.com/post/dados-pessoais-e-o-lixo. Acesso em: jun. 2024.

FERREIRA, K. B. P. da S.; VILARINHO, D. C. A. Crimes cibernéticos: avanços trazidos com a Lei Carolina Dieckmann. **JNT - Facit Business and Technology Journal**, Araguaína – TO, v. 3, n. 39, p. 279-294, ago. /out. 2022. Disponível em: https://revistas.faculdadefacit.edu.br/index.php/JNT/article/view/1893. Acesso em: out. 2024.

FREITAS, L. **A importância do armazenamento de dados operacionais em nuvem e da gestão do conhecimento para continuidade do trabalho a longo prazo**. 2025. 24 p. Trabalho de Conclusão de Curso (Bacharelado em Administração) - Instituto Federal do Espírito Santo, Colatina, 2025 Disponível em: https://repositorio.ifes.edu.br/handle/123456789/5787?show=full. Acesso em: ago. 2025.

FREITAS, R. Um ensaio prático do descarte de HDS (Discos Rígidos) com informações acessíveis ou recuperáveis. *In*: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT, São Paulo, 2019. **Anais** […]. São Paulo: CONTECSI USP, 2019. Disponível em: https://slackspace.com.br/um-ensaio-pratico-do-descarte-de-discos-rigidos-com-informacoes-acessiveis-ou-recuperaveis/. Acesso em: ago. 2024.

GALVÃO, H. L.; OLIVEIRA, A. L. de; GINO, B. de S. B. D.; VIANA, H. J.; ARAÚJO, F. G. L. BENEVINUTO, N. M. S.; SILVA, D. L. F. da. Incidentes de Segurança: Regulação e Prática de Vazamento de Dados Pessoais Frente à LGPD. **Revista de Psicologia**, [*S. l.*], v. 18, n. 72, p. 179-197, 2024. Disponível em: https://idonline.emnuvens.com.br/id/article/view/4042. Acesso em jun. 2025.

GIL, A. C. **Como elaborar projetos de pesquisa**. 7. ed. São Paulo: Atlas, 2022. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559771653. Acesso em: 2 maio 2024.

GILLIS, A. S.; CASTAGNA, R. **Estratégia de backup 3-2-1 explicada**: é eficaz? London: TechTarget, 2024. Disponível em: https://www.techtarget.com/searchdatabackup/definition/3-2-1-Backup-Strategy. Acesso em: abr. 2025.

GIOVANINI, W. Entenda a diferença entre a LGPD e a ISO 27701. **Compliance Total**, Porto Alegre, 27 dez. 2021. Disponível em: https://www.compliancetotal.com.br/conteudos/detalhe/302/entenda-a-diferenca-entre-a-lgpd-e-a-iso-27-701. Acesso em: set. 2024.

GOMES FILHO, V.; GASPAROTTO, A. M. S. A importância do ciclo PDCA à produtividade da indústria no Brasil. **Interface Tecnológica**, Taquaritinga, v. 16, n. 2, p. 383-392, 2019. Disponível em:

https://revista.fatectq.edu.br/interfacetecnologica/pt_BR/article/view/660. Acesso em: 8 out. 2025.

GOUVEIA, L. B. Desafios da segurança da informação: uma reflexão no contexto da ciência da informação. **Arade - Revista do Arquivo Municipal de Lagoa**, [*S. l.*], Ano 2, n. 2, p. 233-247, 2023. Disponível em: http://hdl.handle.net/10284/12459. Acesso em: 8 out. 2024.

GREEN ELETRON. **Gestora para Logística Reversa de Eletrônicos**. São Paulo: Green Eletron, 2024. Disponível em: https://greeneletron.org.br/. Acesso em: 8 out. 2025.

HELDER, D.; BOLZANI, I. **Por que o ataque hacker a instituições financeiras é um dos mais graves já registrados no Brasil, segundo especialistas**. São Paulo: G1, 3 jul. 2025. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/07/03/por-que-o-ataque-hacker-a-instituicoes-financeiras-e-um-dos-mais-graves-ja-registrados-no-brasil-segundo-especialistas.ghtml. Acesso em: 8 out. 2025.

INTERNATIONAL DATA SANITIZATION CONSORTIUM (IDSC). **Terminologia e definições de higienização de dados**. [*S. l.*]: IDSC, [2025]. Disponível em: https://www.datasanitization.org/data-sanitization-terminology/#data-sanitization. Acesso em: 8 out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 14001**: 2015: Environmental management systems: Requirements with guidance for use. Geneva: ISO, 2015. Disponível em: https://www.iso.org/standard/60857.html. Acesso em: 8 out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27000**: 2018: Information technology: Security techniques: Information security management systems: Overview and vocabulary. Geneva: ISO/IEC, 2018. Disponível em: https://www.iso.org/standard/73906.html. Acesso em: 8 out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27001**: 2022: Information technology: Security techniques: Information security management systems: Requirements. Geneva: ISO/IEC, 2022. Disponível em: https://www.iso.org/standard/27001. Acesso em: 8 out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27002**: 2022: Information technology: Security techniques: Code of practice for information security controls. Geneva: ISO/IEC, 2022. Disponível em: https://www.iso.org/standard/75652.html. Acesso em: 8 out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27005**:2018: Information technology: Security techniques: Information security risk management. Geneva: ISO/IEC, 2018. Disponível em: https://www.iso.org/standard/80585.html. Acesso em: 8 out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27006**:2015: Information technology: Security techniques: Requirements for bodies providing audit and certification of information security management systems. Geneva: ISO/IEC, 2015. Disponível em: https://www.iso.org/standard/82908.html. Acesso em: 8 out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27031**:2011: Information technology: Security techniques: Guidelines for information and communication technology readiness for business continuity. Geneva: ISO/IEC, 2011. Disponível em: https://www.iso.org/standard/2703. Acesso em: 5 set. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27037**:2012: Information technology: Security techniques: Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO/IEC, 2012. Disponível em: https://www.iso.org/standard/44381.html. Acesso em: 8 out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27040**:2015: Information technology: Security techniques: Storage security. Geneva: ISO/IEC, 2015. Disponível em: https://www.iso.org/standard/80194.html. Acesso em: 8 out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27701**:2019: Information technology: Security techniques: Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management: Requirements and guidelines. Geneva: ISO/IEC, 2019. Disponível em: https://www.iso.org/standard/71670.html. Acesso em: 8 out. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27001:2024** – Information technology – Security techniques – Information security management systems – Requirements. Geneva: ISO/IEC, 2022. Disponível em: https://www.iso.org/standard/27001. Acesso em: 15 out. 2025.

JUCON, S. **Saiba como descartar seu lixo eletrônico de forma adequada**. [*S. l.*]: ecowords, [202?]. Disponível em: https://ecowords.com.br/saiba-descartar-seu-lixo-eletronico-de-forma-adequada/. Acesso em: jun. 2025.

LACHAUD, E. **Certificação de terceiros e fluxos transfronteiriços no GDPR**: qual opção viável? Preprint, 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3686132. Acesso em: jul. 2024.

LAVOS, S. L. **Implementação de um sistema de gestão de segurança de informação (SGSI) baseado na norma ISO/IEC 27001 na EIB, SA**. 2023. 333 f. Projeto (Mestrado em Cibersegurança e Informática Forense do Instituto Politécnico de Leiria) - Escola Superior de Tecnologia e Gestão, Leira, 2023. Disponível em: http://hdl.handle.net/10400.8/9598. Acesso em: 8 ago. 2024.

LEME, R. S.; BLANK, M. Lei Geral de Proteção de Dados e segurança da informação na área da saúde. **Caderno Ibero Americano de Direito Sanitário**, Brasília, v. 9, n. 3, p. 210-224, jul./set. 2020. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/690. Acesso em: set. 2024.

LEMOS, R. Epidemia de dispositivos de armazenamento e backup inseguros é uma dádiva para os cibercriminosos. **Security Week**, 22 mar. 2023. Disponível em:

https://www.darkreading.com/cyber-risk/epidemic-insecure-storage-backup-devices-cybercriminals. Acesso em: 2 mar. 2025.

LENOVO. **O que é memória volátil?** Indaiatuba: Lenovo, 2025. Disponível em: https://www.lenovo.com/br/pt/glossary/volatile-memory/. Acesso em: 5 abr. 2025.

LORENZON, L. N. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. **Revista do Programa de Direito da União Europeia**, Rio de Janeiro, v. 1, p. 39-52, 2021. Disponível em: https://periodicos.fgv.br/rpdue/article/view/83423. Acesso em: 8 out. 2025.

MACHADO, C. **LGPD**: Frameworks de apoio ao Sistema DP & P. LinkedIn: Carlos Machado, 2020. Disponível em: https://pt.linkedin.com/pulse/lgpd-frameworks-de-apoio-ao-sistema-dpp-carlos-machado. Acesso em: jun. 2025.

MADUREIRA, V.; GOULART, E. **Grupo hacker reivindicou autoria de ataque ao governo federal**. Teresina: UOL Piauí, 11 dez. 2024. Disponível em: https://piaui.folha.uol.com.br/grupo-hacker-reivindicou-ataque-ao-governo-federal/. Acesso em: 2 dez. 2024.

MAGALHÃES, P. **Requisitos e recomendações para o desenvolvimento e operação de um SGSI**: Abordagem com ISO 27001/27002: Cibersegurança e Informática Forense. Leira: Instituto Politécnico de Leiria, 2021. Disponível em: https://www.researchgate.net/publication/348663585_Requisitos_e_recomendacoes_para_o_desenvolvimento_e_operacao_de_um_SGSI_-_Abordagem_com_ISO_2700127002. Acesso em: 8 out. 2025.

MAGMA3. **Presente na sua transformação digital**. Santos: Magma 3, [2025]. Disponível em: https://magma3.com.br/. Acesso em: jun. 2025.

MALIK, M. **Seu guia para descarte seguro de SSD**: evitando riscos de recuperação de dados. [S. l.]: Brilliance Security Magazine, 16 fev. 2023. Disponível em: https://brilliancesecuritymagazine.com/guest-contributor/your-guide-to-safe-and-secure-ssd-disposal-avoiding-data-recovery-risks/. Acesso em: 8 out. 2025.

MARINHO, G. H. A.; PARANAGUÁ, G. N. de M.; PIVA, J. C. Lei Geral de Proteção de Dados no Âmbito Jurídico. **JNT Facit Business and Technology Journal**, v. 2, n. 51, p. 163-172, jun. 2024. Disponível em https://revistas.faculdadefacit.edu.br/index.php/JNT/article/view/2858. Acesso em: 8 out. 2025.

MARQUES, C. S. A. **Concepção da rede logística reversa para a recuperação de "Lixo Eletroeletrônico" (EE - Lixo) com apoio da Lógica Fuzzy**. 2017. 153 f. Dissertação (Doutorado) - Faculdade de Engenharia (FEIS/UNESP), Ilha Solteira, 2017. Disponível em https://repositorio.unesp.br/server/api/core/bitstreams/09e52b20-215a-42a7-b6ce-4d098ab110a5/content. Acesso em: 8 out. 2025.

MARQUES, I. N. da S. **O avanço dos crimes cibernéticos e seus reflexos no âmbito do direito brasileiro**. 2024. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, Escola de Direito, Negócios e Comunicação, Goiânia, 20 maio 2024. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7961. Acesso em: 2 ago. 2025.

MINHA BIBLIOTECA. **UFTM**: “Dashboard” [Internet]. Uberaba: UFTM, [2024]. Disponível em: https://app.minhabiblioteca.com.br/home/dashboard?context=. Acesso em: 2 mar. 2024.

MIRAGEM, B. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, São Paulo, v. 1009, nov. 2019. Disponível em: https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 2 dez. 2024.

MONTEIRO, R. L. **O impacto da Regulação Geral de Proteção de Dados da UE em empresa brasileira**: eficácia extraterritorial e transferência internacional de dados. São Paulo: Baptista Luz Advogados, 2018. E-book. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2018/05/artigo-baptista-luz-impacto-regulatorio-da-gpdeu-v2.0.pdf. Acesso em: 2 jun. 2025.

MOREIRA, M. N. Como proteger seus dados ao descartar equipamentos eletrônicos? **SERPRO - Notícias**, Brasília, 11 jan. 2023. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2023/como-proteger-seus-dados-ao-descartar-equipamentos-eletronicos. Acesso em: set. 2024.

MOTA, J. A.; GONÇALVES, M. G.; SANTOS, E. B. A.; AKABANE, G. K.; SANTOS, J. Comportamento do usuário no descarte de lixo eletrônico na zona sul da cidade de São Paulo. *In*: ENCONTRO INTERNACIONAL SOBRE GESTÃO EMPRESARIAL E MEIO AMBIENTE, São Paulo, 2016. Disponível em: http://engemausp.submissao.com.br/18/anais/arquivos/90.pdf. Acesso em: set. 2024.

MUNCINELLI, G.; VECCHIA, A. C. D.; LIMA, E. P. de; MUNCINELLI, A. D. LGPD Canvas. **Revista Perspectiva PDM**, [*S. l.*], 2020, p. 12-21. Disponível em: https://lgpdcanvas.com.br/wordpress/wp-content/uploads/2020/06/2-LGPD-Canvas-Mundo-PM-Ed92_artigo_01.pdf. Acesso em: 8 out. 2025.

OLIVEIRA, V. M. **Norma NBR/IEC 27037**: 2013. Porto Alegre: Oliveira Perito, 2021. Disponível em: https://oliveiraperito.com.br/2021/07/20/norma-nbr-iso-iec-270372013/. Acesso em: set. 2024.

PASCHOAL, C. R. S.; PASCHOAL, D. F. da S.; ABREU, P. A. **Ferramentas digitais gratuitas online**: um olhar sobre as suas funcionalidades no ensino. Brazilian Journal of Development, [*S. l.*], v. 7, n. 10, p. 96544-96562, 2021. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/37217. Acesso em: 8 out. 2025.

PAULA, J. S. de; ROLAND, C. E. de F. Computação em nuvem: os desafios das empresas ao migrar para a nuvem. **Revista Eletrônica de Computação Aplicada (RECA)**, Franca, v. 5, n. 2, 2024. Disponível em: http://periodicos.unifacef.com.br/reca/article/view/2996. Acesso em: ago. 2025.

PEDROZO, W. G. **Tuning de índices em sistemas gerenciadores de banco de dados relacionais, utilizando sistemas classificadores**. 2019. Tese (Doutorado em Informática do Programa de Pós-Graduação em Informática) - Pontifícia Universidade Católica do Paraná, Curitiba, 2019. Disponível em:

https://www.ppgia.pucpr.br/pt/arquivos/doutorado/teses/2019/Wendel_goes_2019.pdf. Acesso em: 8 out. 2025.

PINHEIRO, P. P.; SLEIMAN, C.; ROCHA, H.; LOTUFO, L.; BISSOLI, L.; SÊMOLA, M.; TUPINAMBÁ, M. S; SIQUEIRA, R. **Segurança digital**: proteção de dados nas empresas. São Paulo: Atlas, 2020. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788597026405/epubcfi/6/12[%3Bvnd.vst.idref%3Dfm01]!/4/4. Acesso em: 8 out. 2025.

REPKO, A. F. **Interdisciplinary research**: process and theory. 4. ed. Thousand Oaks: Sage Publications, 2020. Disponível em: https://books.google.com.br/books/about/Interdisciplinary_Research.html?id=b_C9DwAAQBAJ&redir_esc=y. Acesso em: 8 out. 2025.

RODRIGUES, G.A.P. **Análise Abrangente de Vazamentos de Dados: Riscos, Conformidade e Estratégias de Prevenção**. 2024. 69p. Dissertação (Mestrado profissional do Departamento de Engenharia Elétrica) - Universidade de Brasília, Brasília, DF, 2024. Disponível em: https://ppee.unb.br/wp-content/uploads/2024/11/Dissertacao_na_versao_final-3.pdf . Acesso em: 8 out. 2025.

SÁ, M. D. de. **Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas**: Aplicações mobile do governo. 2019. Trabalho de Conclusão de Curso (Especialista em Informática) - Universidade Federal de Minas Gerais, Brasília, 2019. Disponível em: https://repositorio.ufmg.br/bitstream/1843/32040/1/MarceloDiasDeSa.pdf. Acesso em: 2 fev. 2025.

SÃO BENTO, M. A. T.; CARNEIRO, E. S. Contribuições das cooperativas de reciclagem no ciclo da logística reversa: uma revisão de literatura. **Cadernos Macambira**, [*S. l.*], v. 9, n. 1, p. 46-67, 2024. DOI: 10.59033/cm.v9i1.1011. Disponível em: https://revista.lapprudes.net/CM/article/view/1011. Acesso em: 8 out. 2025.

SCHAUN, F. da S.; CRACO, T.; BIEGELMEYER, U. H.; FIDELIS, A. C. F.; FERNANDES, A. M.; CAMARGO, M. E. Responsabilidade compartilhada: o papel do consumidor no descarte de resíduos sólidos pós-consumo. **Journal on Innovation and Sustainability (RISUS)**, São Paulo, v. 14, n. 2, p. 106-127, abr./maio 2023. Disponível em: http://dx.doi.org/10.23925/2179-3565.2023v14i2p106-127. Acesso em: jul. 2024.

SCHNEIDER, J.; LAUTNER, I.; MOUSSA, D.; WOLF, J.; SCHELER, N.; FREILING, F.; HAASNOOT, J.; HENSELER, H.; MALIK, S.; MORGENSTERN, H.; WESTMAN, M. In search of lost data: A study of flash sanitization practices. **Proceedings of the Digital Forensics Research Conference Europe (DFRWS EU)**, p. 1-11, 2021. Disponível em: https://dfrws.org/wp-content/uploads/2021/03/In-Search-of-Lost-Data-A-Study-of-Flash-Sanitization-Practices.pdf. Acesso em: 8 out. 2025.

SCHWAITZER, L. S. LGPD e acervos históricos: impactos e perspectivas. **Archeion Online**, João Pessoa, v. 8, n. 2, p. 36-51, 28 dez. 2020. Disponível em: https://pbcib.com/index.php/pbcib/article/view/58517. Acesso em: 8 out. 2025.

SILVA, A. F. U. da. **Fluxogramas**: uma nova linguagem para trabalhar divisibilidade no Ensino Básico. 2020. Dissertação (Mestrado Profissional em Matemática em Rede Nacional,

Instituto de Geociências e Ciências Exata) – Universidade Estadual Paulista “Júlio de Mesquita Filho”, Rio Claro, 2020. Disponível em: https://repositorio.unesp.br/handle/11449/202257. Acesso em: fev. 2025.

SILVA, R C da; NOVAIS, T G. A Lei Geral de Proteção de Dados e sua aplicação no combate aos crimes cibernéticos: desafios e perspectivas. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [*S. l.*], v. 10, n. 4, 2024. Disponível em: https://periodicorease.pro.br/rease/article/view/12254. Acesso em: 8 out. 2025.

SINGH, S. **The code book**: the science of secrecy from ancient Egypt to quantum cryptography. New York: Anchor Books, 2022. Disponível em https://pt.scribd.com/document/709951246/O-Livro-dos-Codigos-Simon-Singh. Acesso em: 8 out. 2025.

SNIA. STORAGE NETWORKING INDUSTRY ASSOCIATION. Storage Security: Data Protection. **Technical White Paper**, [*S. l.*], mar. 8, 2018. Disponível em: https://www.snia.org/sites/default/files/security/SNIA-Data-Protection-TechWhitepaper.pdf. Acesso em: 8 out. 2025.

SNOWDEN, E. **Edward Snowden**: what we know about the source behind the NSA files leak. [*S. l.*]: The Guardian, 11 jun. 2013. Disponível em: https://www.theguardian.com/world/2013/jun/11/edward-snowden-what-we-know-nsa. Acesso em: 8 out. 2025.

SOUSA, D. da S.; GONÇALVES, G. D. Análise do Uso de Comunicação Dispositivo a Dispositivo para Transferência de Dados Compartilhados em Serviços de Armazenamento Pessoal em Nuvem. **Revista de Sistemas e Computação - RSC**, [*S. l.*], v. 10, n. 3, p. 275-284, set./dez. 2020. Disponível em: https://revistas.unifacs.br/index.php/rsc/article/view/6895/4241. Acesso em: 8 out. 2025.

SOUSA, R. S.; LOOS, M. J. Aplicação do Ciclo PDCA e ferramentas de gestão de qualidade na redução de custos e perdas em uma distribuidora de Hortfrut. **Journal of Perspectives in Management – JPM**, Caruaru, v. 4, p. 68-83, 2020. Disponível em: https://www.researchgate.net/publication/352670622_Aplicacao_do_Ciclo_PDCA_e_Ferramentas_da_Qualidade_na_reducao_de_Custos_e_Perdas_em_uma_Distribuidora_de_Hortifruti. Acesso em: 15 out. 2025.

SUDYANA, D.; PRAYUDI, Y.; SUGIANTORO, B. Analysis and evaluation digital forensic investigation framework using ISO 27037: 2012. **International Journal of Cyber-Security and Digital Forensics (IJCSDF)**, [*S. l.*], v. 8, n. 1, p. 1-14, 2019. The Society of Digital Information and Wireless Communications (SDIWC). Disponível em: https://www.researchgate.net/profile/Didik-Sudyana/publication/328281191_Analysis_and_Evaluation_Digital_Forensic_Investigation_Framework_using_ISO_270372012/links/5bc42dad299bf1004c5f47c4/Analysis-and-Evaluation-Digital-Forensic-Investigation-Framework-using-ISO-270372012.pdf?__cf_chl_tk=SLmXatPCd.KMTuSxBMo4Ph6qPcQdK0SH2tR0lJaBXzY-1741370700-1.0.1.1-6_xDppqeQ2K8RnnrjO.GmlVJm9qnveNQ8_4z6q1Q1tc. Acesso em: 8 out. 2025.

SUSNJARA, S.; SMALLEY, I. **O que é armazenamento de dados?**: Think. São Paulo: IBM Brasil, 15 jul. 2024. Disponível em: https://www.ibm.com/br-pt/think/topics/data-storage. Acesso em: 8 out. 2025.

TANAKA, B. M.; GOMES, L. de S. **Gerenciamento de informações**: a importância da gestão da informação e o backup para as empresas. 2019. Trabalho de Conclusão de Curso (Graduação) – Escola Técnica Estadual Prof. Armando José Farinazzo Centro Paula Souza, Fernandópolis, 2019. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/19540. Acesso em: 8 out. 2025.

TAPIA, J. A. R.; VALDÉS, S. R.; GUTIÉRREZ, C. E. E. A qualidade da informação em um sistema de gestão de segurança (ISMS) através de um software baseado no padrão ISO 27001 para instituições de educação. **RILCO DS: Revista de Desarrollo sustentable, Negocios, Emprendimiento y Educación**, v. 3, n. 26, 2021. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=8547078. Acesso em: 8 out. 2025.

TEFFÉ, C. S. de; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro, v. 9, n. 1, p. 1-38, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510. Acesso em: 8 out. 2025.

TEIXEIRA, T.; GUERREIRO, R. M. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: Comentada Artigo por Artigo. São Paulo: Saraiva, 2022. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555599015/epubcfi/6/18[%3Bvnd.vst.idref%3Dpart02.xhtml]!/4/2/2/1:0[%2CPar. Acesso em: 8 out. 2025.

TOTVS, Equipe. **Cidadania digital**: o que é, elementos, desafios e mais! [*S. l.*]: TOTVS, 17 maio de 2023. Disponível em: https://www.totvs.com/blog/gestao-para-assinatura-de-documentos/cidadania-digital/. Acesso em: 8 out. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados – GDPR. **Diário Oficial da União Europeia**, [*S. l.*], L 119, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 8 out. 2025.

UNITAR – UNITED NATIONS INSTITUTE FOR TRAINING AND RESEARCH. **Global E-waste Statistics Partnership**. [*S. l.*]: Unitar, 2024. Disponível em: https://globalewaste.org/. Acesso em: 8 out. 2025.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL. Comitê de Segurança da Informação. **Resolução CSI nº 1, de 14 de maio de 2025**. Porto Alegre: UFRGS, 2025. Disponível em: https://www.ufrgs.br/csi/docs/UFRGS-PoliticaGestaoAtivosTI.pdf. Acesso em: 15 out. 2025.

VAKULOV, A. **Revisando sua estratégia de backup em 2023**. [*S. l.*]: Cloud Security Alliance, 2023. Disponível em: https://cloudsecurityalliance.org/blog/2023/01/13/revising-your-backup-strategy-in-2023. Acesso em: 8 out. 2025.

VASCONCELOS, K. **Os benefícios e riscos da LGPD**. [*S. l.*]: Serviço Federal de Processamento de Dados (Serpro), 2020. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/beneficios-riscos-lgpd-empresas. Acesso em: 15 out. 2025.

WEBER, F. K.; SCHMIDT, F. E. O princípio da publicidade nos atos da administração pública: uma análise sobre a LAI e a LGPD em um possível conflito de normas. **Revista Foco**, [*S. l.*], v. 16, n. 6, p. e 2295, 2023. DOI: https://doi.org/10.54751/revistafoco.v16n6-112. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/2295. Acesso em: 8 out. 2025.

XAVIER, L. H.; VALENTE, A. F.; RECKZIEGEL, L. E.; ALEXANDRE, L.; GOMES, C. F.M.; CONTADOR, L. (org.). **Guia de desmontagem de equipamentos eletroeletrônicos**. 2. ed. Rio de Janeiro: CETEM/MCTI, 2025. Disponível em: http://mineralis.cetem.gov.br/handle/cetem/2918. Acesso em: 8 out. 2025.

APÊNDICE A - Manual de Boas Práticas

Manual de Boas Práticas

Descarte seguro e sustentável de ativos contendo dispositivos de armazenamento de dados

Márcio Giordani Ribeiro da Silva Martins
Geoffroy Roger Pointer Malpass
Ana Claudia Granato Malpass

Márcio Giordani Ribeiro da Silva Martins

Geoffroy Roger Pointer Malpass

Ana Claudia Granato Malpass

Manual de Boas Práticas

Descarte seguro e sustentável de ativos contendo dispositivos de armazenamento de dados

Uberaba, 2025

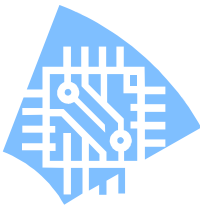
Área de concentração: Gestão Ambiental e Segurança da Informação.

Linha de pesquisa: Sustentabilidade na Gestão de Ativos de TI

Tema: Gestão Segura e Sustentável do Descarte de Ativos Contendo Dispositivos de Armazenamento de Dados, em conformidade com a LGPD, a PNRS e as Normas ISO/IEC 27000.

Orientadores: Prof. Dr. Geoffroy Roger Pointer Malpass;
Profa. Dra. Ana Claudia Granato Malpass.

Ilustrações: Canva; Bizage Modeller



PROPOSTA APLICADA

O “*Manual de Boas Práticas: descarte seguro e sustentavel de ativos contendo dispositivos de armazenamento de dados*” tem por objetivo oferecer orientações práticas e tecnicamente fundamentais para subsidiar a pdronização de processos institucionais relacionados ao descarte desses ativos. Sua proposta não se restringe a um setor ou instituição específicos, sendo aplicável a organizações públicas e privadas que lidam com dispositivos de armazenamento de dados e desejam assegurar a conformidade com a legislação vigente.

Este material foi desenvolvido como produto técnico da Dissertação apresentada ao Programa de Mestrado Profissional em Inovação e Tecnologias da Universidade Federal do Triângulo Mineiro (UFTM), como requisito parcial para obtenção do título de Mestre em Inovação e Tecnologias. A construção do material funtamenta-se em diretrizes legais e normativas, com destaque para a Lei Geral de Proteção de Dados Pessoais (LGPD), a Política Nacional de Resíduos Sólidos (PNRS) e as normas da família ISO/IEC 27000, voltadas para a segurança da informação e à gestão de riscos.

Destinado ao público em geral – especialmente, profissionais, gestores e instituições que ainda não dispõem de processos formalizados para o descarte de ativos de tecnologia da informação – o manual busca contribuir para a construção de uma cultura organizacional pautada na responsabilidade ambiental, na proteção de dados e na sustentabilidade.

Aprovado pela banca avaliadora da UFTM e estrutura conforme os critérios técnicos e científicos exigidos pelo programa de pós-graduação, o manual encontra-se em conformidade com as normas legais brasileiras. Sua elaboração visa ampliar o acesso ao conhecimento e incentivar a adoção de práticas seguras e responsáveis no ciclo de vida dos ativos digitais.

Espera-se, com isso, fomentar a disseminação de boa práticas, reduzindo riscos operacionais e legais decorrentes do descarte inadequado de equipamento e promover de forma integrada, a govenança de dados, a sustentabilidade ambiental e a inovação institucional.

Lista de Ilustrações

Lista de Quadros

Lista de Abreviaturas e Siglas

ADF	Atestado de Destinação Final
ANPD	Autoridade Nacional de Proteção de Dados
BPMN	*Business Process Model and Notation*
CD	*Compact Disc*
CTF/APP	Cadastro Técnico Federal de Atividades Potencialmente Poluidoras e Utilizadoras de Recursos Ambientais
DAS	*Direct-Attached Storage*
DPO	*Data Protection Officer*
DVD	*Digital Versatile Disc*
DVR	*Digital Video Recorder*
GDPR	*General Data Protection Regulation*
GSI	Gestão de Segurança da Informação
GDPR	*General Data Protection Regulation*
GSI	Gestão de Segurança da Informação
HDD	Hard Disk Drive
IEC	*International Electrotechnical Commission*
IoT	Internet of Trings
ISA	*International Federation of the National Standardizing Associations*
Iscsi	Intert Small Computer System Interface
ISO	International Organization for Standardizations
LAN	Local Area *Network*
LGPD	Lei Geral de Proteção de Dados
LUN	*Logical Unit Number*
NAS	Network Attached Storage
PDCA	*Plan* (Planejar)*, Do* (Executar), *Check* (Verificar), *Act* (Agir*)*
PNRS	Política Nacional de Resíduos Sólidos
PEVs	Pontos de Entrega Voluntária
RCB	*Registered Certification Body*
ROM	*Read-Only Memory*
RPO	*Recovery Point Objective*
RTO	*Recovery Time Objective*
SAN	*Storage Area Network*
SATA	*Serial Advanced Technology Attachment*
SGSI	Sistema de Gestão de Segurança da Informação
SI	Segurança de Informação
SSD	Solid State Drive
TI	Tecnologia da Informação
UFTM	Universidade Federal do Triângulo Mineiro
UNSCC	*United Nations Standards Coordinating Committee*
USB	*Universal Serial Bus*
VLAN	*Virtual Local Area Network*

Apresentação

A elaboração deste **Manual de Boas Práticas para o Descarte Seguro de Ativos de Armazenamento de Dados** seguiu um caminho baseado em pesquisa bibliográfica, análise documental e estudo da legislação vigente. O processo partiu da identificação da necessidade de orientar o descarte responsável de ativos de armazenamento de dados, unindo aspectos de segurança da informação e sustentabilidade ambiental.

Para isso, foram consultadas normas nacionais e internacionais, como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010) e o Decreto nº 10.240/2020, além de referenciais técnicos como a família de normas ISO/IEC 27000. Também foram utilizados estudos acadêmicos e relatórios oficiais que tratam da logística reversa e da economia circular.

O conteúdo foi organizado em seções que apresentam definições, orientações práticas e recomendações aplicáveis a instituições públicas, privadas e à sociedade em geral.

Por fim, os fluxogramas de **Procedimentos de Armazenamento, *Backup*, Descarte, Sanitização e Ciclo PDCA** apesentados foram elaborados e, posteriormente, validados por três profissionais de áreas distintas — Tecnologia da Informação, Direito e Meio Ambiente. Essa revisão multidisciplinar assegurou que as orientações propostas fossem tecnicamente consistentes, juridicamente adequadas e ambientalmente responsáveis, reforçando a aplicabilidade do manual no contexto organizacional.

Márcio Giordani Ribeiro da Silva Martins
http://lattes.cnpq.br/5994033881338905
Setembro, 2025

Sumário

1

Introdução

O presente Manual de Boas Práticas para o Descarte Seguro e Sustentável de Ativos de Tecnologia da Informação tem como finalidade orientar profissionais, instituições públicas e privadas, bem como a sociedade em geral, sobre os procedimentos necessários para o descarte correto de equipamentos que contenham dispositivos de armazenamento de dados.

Seu conteúdo está fundamentado na legislação brasileira vigente, especialmente na Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) —, na Lei nº 12.305/2010 — que institui a Política Nacional de Resíduos Sólidos (PNRS) —, e nas diretrizes técnicas das normas da família ISO/IEC 27000, que tratam da segurança da informação.

A proposta do manual é apresentar, de forma clara e estruturada, as boas práticas relacionadas ao ciclo de vida dos dados e dos equipamentos que os armazenam, contemplando etapas como: armazenamento seguro, realização de backup, sanitização de dados e descarte ambientalmente adequado dos ativos de Tecnologia da Informação (TI).

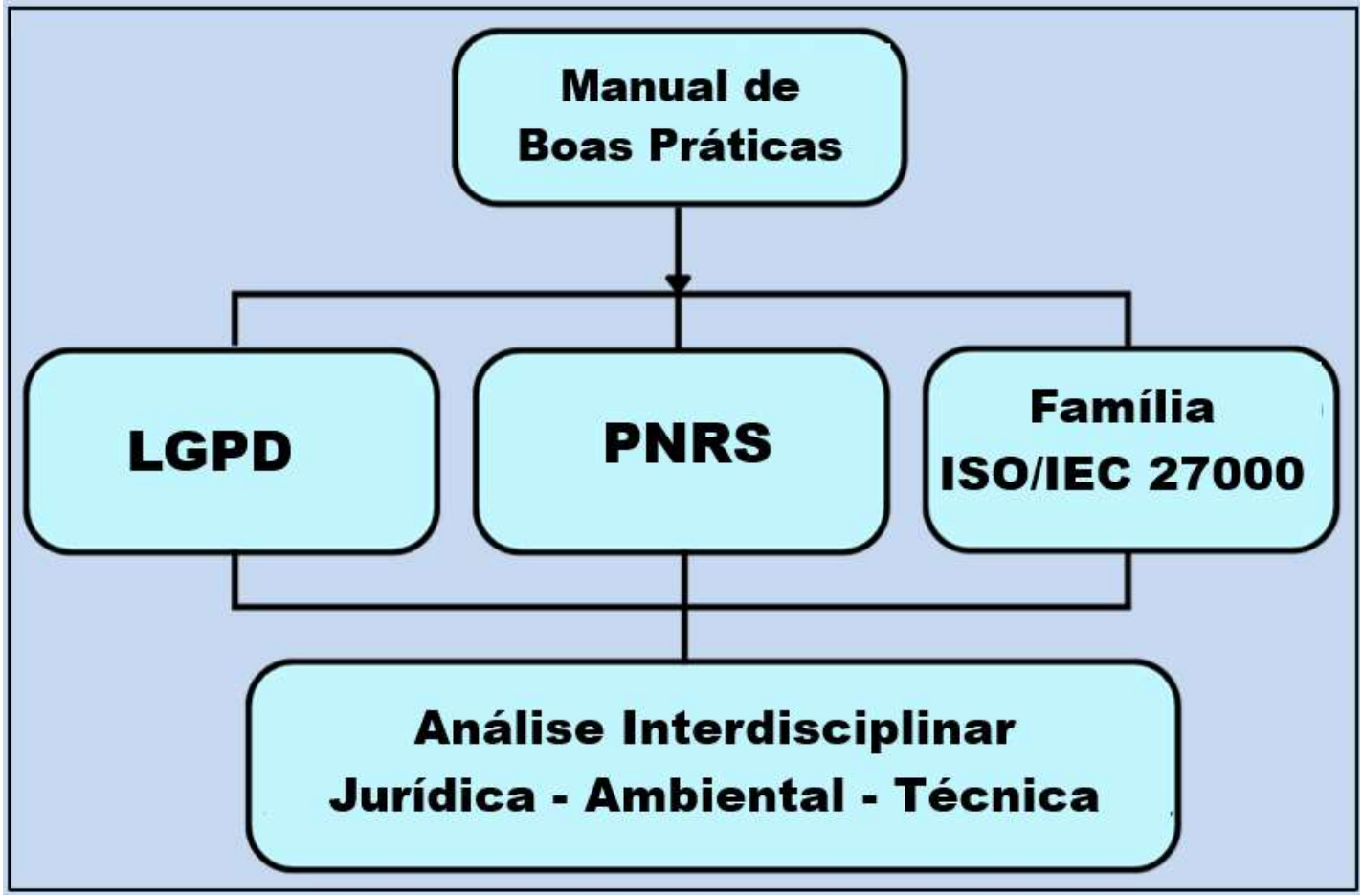
Adotando uma abordagem prática e interdisciplinar, este manual se propõe a ser um guia acessível e aplicável, que contribua para a proteção da privacidade, a mitigação de riscos legais e o compromisso com a sustentabilidade ambiental. Sua utilização visa promover a padronização de processos, o fortalecimento da governança de dados e o cumprimento das responsabilidades socioambientais e legais das organizações.

A construção do Manual de Boas Práticas objetiva:

- ✓ **Orientar** organizações e indivíduos quanto à adoção de procedimentos padronizados para a eliminação segura de dados e o descarte responsável de equipamentos de TI;
- ✓ **Prevenir riscos** associados a vazamentos de informações, garantindo a conformidade com a legislação de proteção de dados e normas internacionais de segurança da informação;
- ✓ **Fomentar a conscientização socioambiental**, incentivando práticas sustentáveis que minimizem impactos negativos ao meio ambiente, por meio da destinação correta de resíduos eletrônicos;
- ✓ **Apoiar a governança corporativa**, fornecendo subsídios para que empresas e instituições públicas aprimorem seus processos de gestão de ativos tecnológicos e de dados;
- ✓ **Promover a cultura de segurança e responsabilidade digital**, fortalecendo a confiança de clientes, parceiros e sociedade em geral nas práticas de gestão e descarte de informações.

Os principais aspectos considerados no Manual de Boas Práticas estão relacionados as três normativas: LGPD, PNRS e Família ISO/IEC 27000, com ênfase no descarte de ativos contendo informações pessoais e corporativas. A Figura 1, a seguir, possibilita uma visão da estrutura do referido manual.

Figura 1: Estrutura do Manual de Boas Práticas



Fonte: Proposta do Manual de Boas Práticas (2025).

Pode-se considerar que, o Manual de Boas Práticas apresentado foi resultado da pesquisa bibliográfica, dos conceitos aplicados nos fluxogramas e da validação dos três consultores técnicos responsáveis, que atuaram de forma interdisciplinar. Suas contribuições possibilitaram o alinhamento com a LGPD, garantindo a proteção de dados pessoais; a observância dos princípios da PNRS, assegurando o correto gerenciamento de resíduos e a responsabilidade compartilhada; e a incorporação das boas práticas técnicas estabelecidas pela família ISO/IEC 27000, reforçando os mecanismos de segurança da informação. Essa convergência jurídica, ambiental e técnica consolidou a base de sustentação do Manual de Boas Práticas, assegurando rigor normativo, viabilidade operacional e compromisso socioambiental.

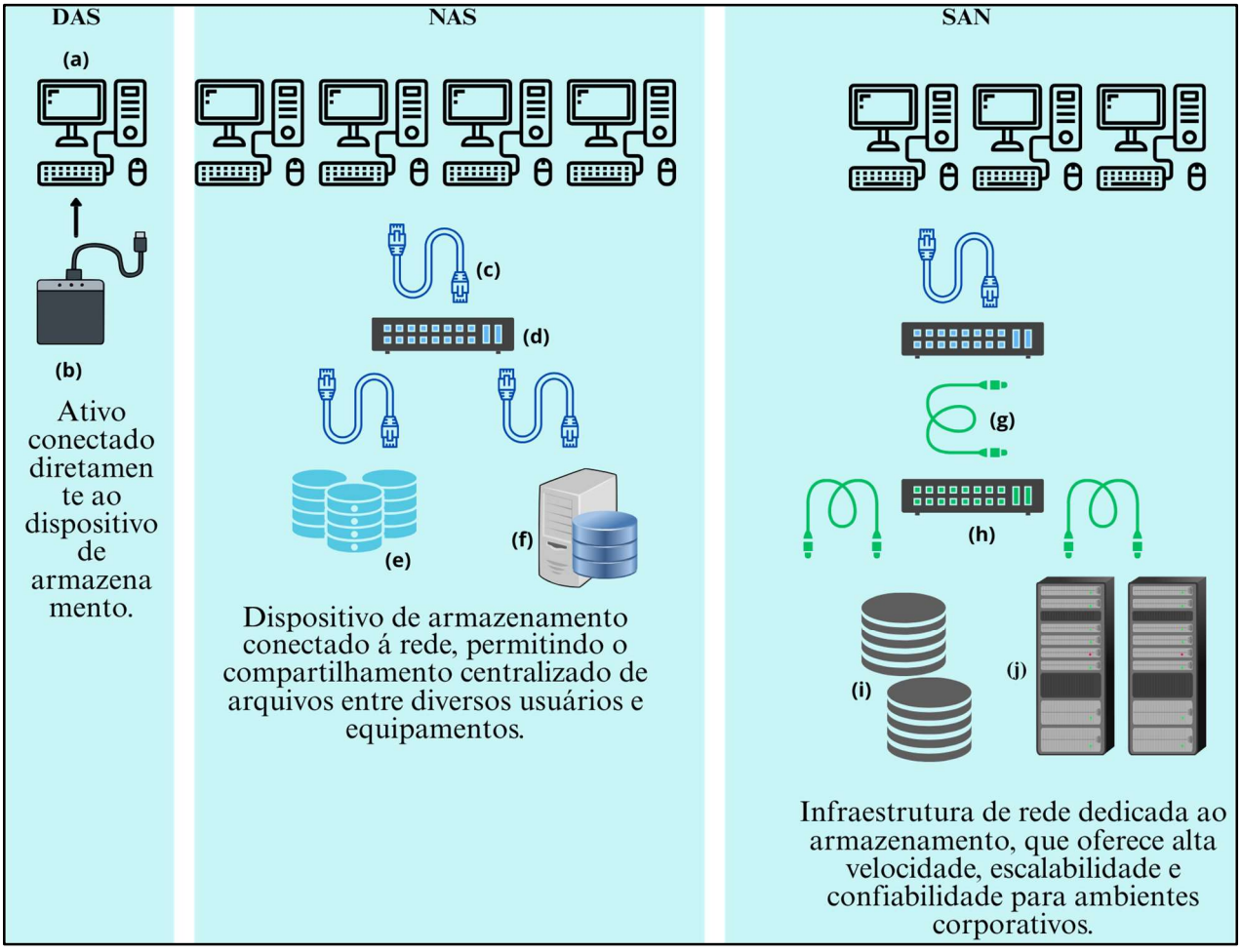
2

Gestão de Armazenamento e *Backups*

O armazenamento, pode ser realizado de duas formas: por meio de conexão direta (*Direct-Attached Storage* – DAS) ou através da conexão em rede, que inclui soluções como o *Network Attached Storage* (NAS) e *o Storage Area Network* (SAN).

Essas modalidades de armazenamento estão representadas na Figura 2 e detalhadas no Quando 1, que ilustram os elementos principais e a interação entre usuários, dispositivos de armazenamento e infraestrutura de rede em cada modelo. Essa forma esquemática evidencia como o armazenamento direto é conectado localmente aos usuários, enquanto os modelos em rede (NAS e SAN) dependem de dispositivos de comunicação específicos para o acesso seguro e eficiente aos dados, apresentadas de forma esquemática.

Figura 2: Demonstrativo DAS, NAS e SAN



Fonte: Elaboração própria, 2025.

Quadro 1: Legenda Técnica dos Componentes DAS, NAS e SAN

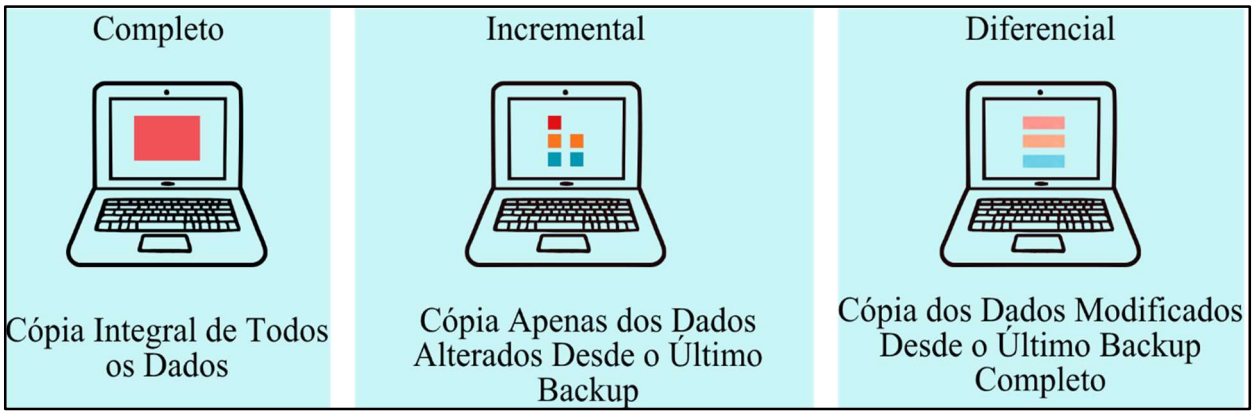
Elemento	Legenda Técnica
(a)	Estações ou servidores clientes - acessam diretamente os dados em dispositivos conectados fisicamente à máquina, sem intermediação de rede. De acordo com a ISO/IEC 27040, esse modelo exige atenção a controles de acesso físico restrito e sanitização de mídias, dado que a perda ou o roubo do hardware pode comprometer a confidencialidade da informação.
(b)	Dispositivo de armazenamento - Unidade de disco local ou periférico (ex.: HD interno, SSD, ou dispositivo externo ligado por *Universal Serial Bus* (USB) e *Serial Advanced Technology Attachment* (SATA). Trata-se do elemento central no DAS, e sua segurança está relacionada à proteção contra manipulação não autorizada, bem como à adoção de mecanismos de criptografia e descarte seguro, conforme orienta a norma ISO/IEC 27040.
(c)	Cabos de Rede - Conexões físicas (*Ethernet* ou similares) que permitem a comunicação entre os usuários e equipamentos (Amaral, 2012). A norma ISO/IEC 27040 sugere o uso de canais criptografados e segmentação lógica da rede para reduzir riscos de interceptação de tráfego e acesso não autorizado.
(d)	*Switch* NAS- Dispositivo de rede comum responsável por gerenciar a comunicação entre múltiplos clientes e dispositivos (computadores, impressoras, IoT, dispositivos de armazenamento) (Amaral, 2012). Esse componente deve ser configurado com monitoramento de tráfego, prevenindo ataques internos e externos (ISO/IEC 27040).
(e)	Armazenamento: Dispositivo de armazenamento em rede (NAS), como unidades de disco configuradas para operação compartilhada de arquivos entre usuários (ISO/IEC 27040).
(f)	Servidor dedicado: executa o serviço de NAS, gerenciando requisições de acesso a arquivos.
(g)	Cabos de rede: Cabos (ex: *Fibre Channel*, *Internet Small Computer System Interface* **(**iSCSI) que compõem a infraestrutura física de uma SAN, interligando servidores e dispositivos de armazenamento via rede dedicada (Amaral, 2012).
(h)	*Switch* SAN: Elemento de comutação especializado (*switch* FC ou iSCSI) que gerencia o tráfego em alta velocidade entre servidores e dispositivos de armazenamento em SAN.
(i)	*Arrays* de discos conectados à SAN, apresentados como armazenamento local aos servidores através de virtualização ou mapeamento de volumes (*Logical Unit Number* **-** LUNs)
(j)	Servidores corporativos: acessam volumes de armazenamento através da SAN, com alta performance, confiabilidade e escalabilidade, conforme orientado para ambientes corporativos na ISO/IEC 27040

Fonte: Elaboração própria, 2025.

Quando a realização de backups é fundamental para garantir a continuidade das operações e a preservação das informações em caso de falhas, exclusões acidentais, ataques ou incidentes de segurança. Para isso, recomenda-se seguir a regra 3-2-1: manter três cópias dos dados, em dois tipos diferentes de mídias, sendo uma delas em local externo ao ambiente principal. As cópias devem ser armazenadas em locais seguros, com acesso restrito, proteção contra danos físicos e lógicos, e testes periódicos de recuperação para assegurar sua eficácia.

Existem três tipos principais de backup, como mostra a Figura 3.

Figura 3: Tipos de Backup: Completo, Incremental e Diferencial



Fonte: Elaboração própria, 2025.

Além dos backups, é essencial implementar controles de autenticação, autorização e criptografia, aplicando sempre o princípio do menor privilégio, para garantir a confidencialidade e a integridade das informações.

3

Legislações aplicadas

Este Manual de Boas Práticas fundamenta-se na convergência de três pilares legais e normativos que regem o descarte seguro e sustentável de ativos de TI: a LGPD, a PNRS e a família de normas ISO/IEC 27000.

Esses instrumentos atuam de maneira complementar, oferecendo respaldo jurídico e técnico para as ações propostas neste manual, de modo a garantir tanto a proteção de dados pessoais quanto à preservação ambiental e a segurança da informação.

LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

Estabelece os princípios e regras para o tratamento de dados pessoais, impondo obrigações às organizações quanto à coleta, ao armazenamento, ao uso e ao descarte de informações sensíveis. Seu cumprimento visa à proteção da privacidade, à transparência nos processos e à responsabilização das instituições.

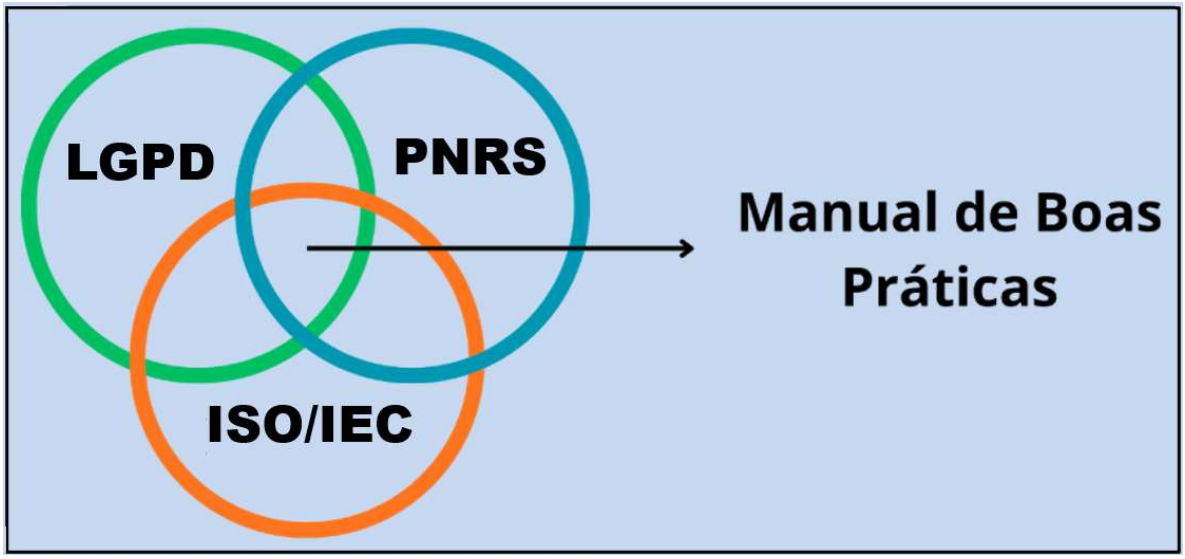
PNRS – Política Nacional de Res íduos Sólidos (Lei nº 12.305/2010)

Regulamenta a gestão e o gerenciamento de resíduos sólidos, incluindo os resíduos eletrônicos provenientes de equipamentos de TI. A PNRS orienta sobre a logística reversa, a destinação ambientalmente adequada e a responsabilidade compartilhada entre fabricantes, consumidores, usuários e o poder público.

Normas da Família ISO/IEC 27000

Conjunto de normas internacionais que definem princípios e controles para a gestão da segurança da informação. São aplicadas em processos que envolvem a proteção de dados, desde o armazenamento até a eliminação definitiva dos dispositivos, promovendo conformidade, integridade e disponibilidade da informação.

Figura 4: Pilares legais e normativos do descarte seguro e sustentável de ativos de Tecnologia da Informação



Fonte: Elaboração própria, 2025.

Relevância para este Manual

A integração dessas três referências fortalece a proposta do manual, ao oferecer diretrizes claras, confiáveis e legalmente respaldadas. As práticas recomendadas aqui foram estruturadas para atender às exigências normativas em vigor no Brasil, garantindo que instituições públicas e privadas possam adotar procedimentos eficazes, seguros e sustentáveis no descarte de ativos contendo dados.

3.1 Lei Geral de Proteção de Dados (LGPD)

A **LGPD (Lei nº 13.709/2018)** foi inspirada no *General Data Protection Regulation* (GDPR) — o Regulamento Geral sobre a Proteção de Dados da União Europeia — e estruturada com base em sessenta e cinco artigos, que juntos asseguram a proteção dos dados pessoais e da privacidade dos cidadãos, alinhando-se às melhores práticas globais. Tendo forte inspiração na GDPR, a lei traz, como grande diferencial para a sociedade brasileira a garantia de que o indivíduo possui direito sobre seus dados e que aquele que efetua o tratamento de dados possui uma série de obrigações perante o seu titular.

No contexto brasileiro, a construção normativa que culminou na LGPD teve início com a promulgação da Lei de Acesso à Informação (LAI), Lei nº 12.527, de 18 de novembro de 2011. Essa legislação regulamenta o direito constitucional de acesso a informações públicas, previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal (CF). A LAI promove a transparência da administração pública, permitindo que cidadãos acessem dados sobre o uso de recursos governamentais, salvo quando classificados como sigilosos (Weber; Schmidt, 2023), sendo, portanto, uma base inicial relevante para as discussões posteriores sobre proteção de dados no país.

A LGPD estabelece diretrizes obrigatórias para a coleta, o tratamento, o armazenamento e o descarte de dados pessoais no Brasil. Seu propósito é assegurar a **privacidade, a segurança da informação e a proteção** dos direitos fundamentais dos titulares de dados. A não conformidade pode gerar **sanções administrativas**, como advertências, multas de até 2% do faturamento da empresa (limitadas a R$ 50 milhões por infração), bloqueio ou eliminação dos dados, entre outras penalidades legais.

PRINCÍPIOS APLICÁVEIS AO TRATAMENTO DE DADOS:

- **Finalidade legítima e específica:** os dados só podem ser coletados e usados para objetivos claramente definidos.
- **Necessidade:** deve-se restringir o tratamento apenas às informações estritamente indispensáveis.
- **Transparência:** os titulares devem ser informados de forma clara sobre como seus dados são utilizados.

DIREITOS DOS TITULARES

- **Acesso e correção:** consultar e atualizar seus dados pessoais.
- **Eliminação:** solicitar a exclusão dos dados após o término da finalidade ou a qualquer momento, salvo obrigações legais.
- **Informação:** ser notificado sobre o compartilhamento e a forma de uso de suas informações.

OBRIGAÇÕES DAS ORGANIZAÇÕES

1. **Mapeamento do tratamento de dados**
   - Registrar quais dados são coletados, a finalidade, os métodos de tratamento e os destinatários.
   - Definir prazos de retenção e processos de descarte seguro.
2. **Controles técnicos e administrativos**
   - Proteger contra acessos não autorizados, perdas ou vazamentos de dados.
   - Implementar medidas alinhadas às melhores práticas de segurança da informação.
   - Garantir a confidencialidade, integridade e disponibilidade dos dados.
3. **Retenção e descarte**
   - Estabelecer prazos compatíveis com a finalidade e a legislação aplicável.
   - Eliminar dados de forma segura ao fim do período de uso.
   - No caso de suportes físicos, observar a **Política Nacional de Resíduos Sólidos (PNRS)**, assegurando o descarte ambientalmente adequado.
   - Formalizar o processo de exclusão em relatórios que permitam **rastreabilidade e auditoria**.

ELIMINAÇÃO SEGURA DOS DADOS

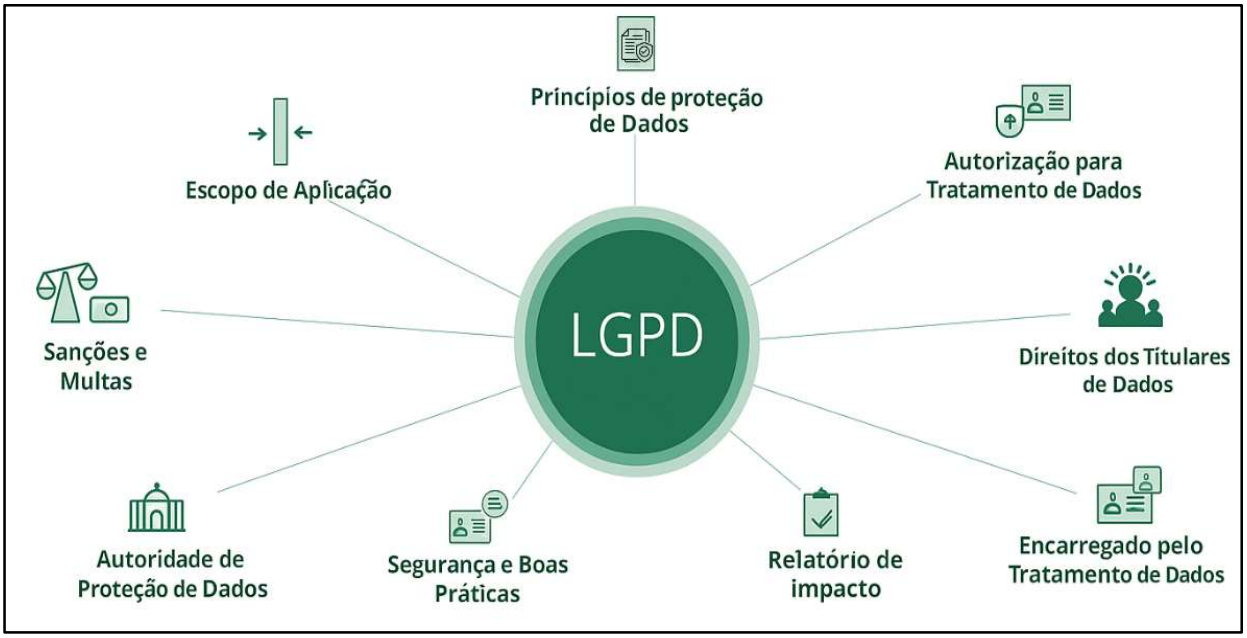
- A LGPD não detalha procedimentos de descarte, o que cria riscos de vazamentos.
- Cabe às organizações desenvolver políticas internas para assegurar exclusão definitiva e segura.
- Controladores e operadores podem ser responsabilizados civilmente, inclusive de forma solidária, quando atuarem em desacordo com a legislação.

CENÁRIO ATUAL NO BRASIL

- Apesar do reconhecimento da importância da LGPD, pesquisas apontam que apenas 15% das empresas iniciaram adequação correta, revelando um grande desafio de cultura organizacional.
- Cabe às organizações desenvolver políticas internas para assegurar exclusão definitiva e segura.
- Empresas enfrentam barreiras como falta de investimentos, ausência de profissionais qualificados (ex.: *Data Protection Officer* - DPO) e políticas internas pouco eficazes.

Em se tratando dos principais pontos da lei, Sá (2019) destaca que a LGPD, é um marco regulatório fundamental para a governança de dados no Brasil e explica em nove pontos que classifica como principais, que são destacados na Figura 5.

Figura 5: Principais pontos da LGPD



Fonte: Adaptado de Sá (2019).

1. **Princípios de Proteção de Dados (Art. 6º):** orientam o tratamento, destacando finalidade, necessidade, adequação, segurança, transparência e responsabilização.
2. **Bases Legais (Art. 7º):** autorizam o tratamento de dados, como consentimento do titular, cumprimento de obrigações legais, execução de políticas públicas, entre outras hipóteses legítimas.
3. **Direitos dos Titulares (Art. 18):** garantem acesso, correção, portabilidade e exclusão de dados, assegurando maior controle aos cidadãos.
4. **Encarregado de Dados – DPO (Art. 5º e 41):** profissional responsável pela comunicação entre controlador, titulares e a Autoridade Nacional de Proteção de Dados (ANPD).
5. **Relatório de Impacto (Art. 38):** documento que avalia riscos, descrevendo dados tratados, finalidade e medidas de segurança adotadas.
6. **Segurança e Boas Práticas (Arts. 46 a 49):** exigem medidas técnicas e administrativas para prevenir acessos não autorizados, vazamentos ou uso inadequado.
7. **Autoridade Nacional de Proteção de Dados – ANPD (Arts. 55-A a 55-K):** órgão que regulamenta, orienta, fiscaliza e aplica sanções relacionadas à LGPD.
8. **Sanções (Art. 52):** variam de advertências e multas até a suspensão ou proibição total do tratamento de dados.
9. **Escopo de Aplicação (Art. 3º):** abrange qualquer operação de tratamento realizada no Brasil ou voltada a indivíduos localizados no país, independentemente da sede ou do meio utilizado.

3.2 Política Nacional de Resíduos Sólidos

A **Política Nacional de Resíduos Sólidos (PNRS) - Lei n. 12.305/2010 -** representa um marco regulatório fundamental para a gestão e o descarte de resíduos no Brasil, estabelecendo diretrizes que vão desde a geração até o descarte final, cujo objetivo é minimizar os impactos ambientais e promover a sustentabilidade. Entre suas metas, destacam-se o incentivo à reutilização, reciclagem e o descarte correto de rejeitos, visando minimizar os danos causados ao meio ambiente.

RESÍDUOS ELETRÔNICOS (*E-LIXO*)

- São equipamentos eletroeletrônicos descartados, com composição complexa e volume crescente.
- Representam um desafio para a gestão ambiental sustentável, devido ao risco ambiental e à presença de dados pessoais armazenados.

RESPONSABILIDADE COMPARTILHADA (ART. 33, PNRS)

- O gerenciamento de resíduos é responsabilidade de **geradores, fabricantes, importadores, distribuidores e comerciantes**.
- Inclui rastreabilidade de ativos em todo o ciclo de vida.
- A responsabilidade persiste mesmo após o uso pelo consumidor.

HIERARQUIA DE GESTÃO DE RESÍDUOS (ART. 9º, PNRS)

- Prioridades:

não geração → redução → reutilização → reciclagem → tratamento → disposição final adequada.

PROTEÇÃO DE DADOS NO CICLO DE VIDA DOS PRODUTOS

- Controladores, operadores e fornecedores devem garantir privacidade desde o desenvolvimento até o descarte.
- A **ISO/IEC 27040** prevê controles de eliminação e sanitização segura de dispositivos de armazenamento.
- Visa reduzir riscos de vazamentos e acessos indevidos.

RESPONSABILIDADE SOLIDÁRIA

- Fabricantes e assistências técnicas podem ser responsabilizados por eventuais vazamentos de dados.

LOGÍSTICA REVERSA E PEVS

- Fabricantes, importadores, distribuidores e comerciantes devem disponibilizar **Pontos de Entrega Voluntária (PEVs)**.
- Consumidores descartam resíduos nesses pontos, que devem ser destinados a recicladoras homologadas.

Conforme ilustrado na Figura 6, é possível observar diferentes modelos de Pontos de Entrega Voluntária (PEVs), estruturas geralmente confeccionadas em metal ou plástico de alta resistência, utilizadas para o descarte adequado de resíduos eletrônicos por parte dos consumidores. Esses pontos visam facilitar a logística reversa e promover práticas ambientalmente corretas, conforme preconizado pela PNRS.

Figura 6: Ponto de descarte de resíduos eletrônicos

Fonte: Jucon (2019).

ORIENTAÇÕES PARA O DESCARTE SUSTENTÁVEL DE ATIVOS DE ARMAZENAMENTO DE DADOS

O descarte de equipamentos eletroeletrônicos que armazenam dados deve seguir princípios de responsabilidade socioambiental e de proteção da informação, conforme previsto pela legislação brasileira e pelas normas internacionais de segurança.

Etapas recomendadas:

- Consumo consciente: avaliar a real necessidade de substituição de equipamentos antes do descarte (Almeida, 2023).
- Descarte adequado: utilizar pontos de coleta autorizados e programas oficiais de reciclagem, conforme PNRS (Brasil, 2010).
- Coleta e triagem: garantir que os dispositivos sejam encaminhados a operadores licenciados para separação dos componentes.
- Reciclagem e destinação final: assegurar que materiais aproveitáveis retornem ao ciclo produtivo, em conformidade com os princípios da Economia Circular (Almeida, 2023).

Exemplos de Dispositivos sujeitos à logística reversa (Decreto nº 10.240/2020):
Câmeras digitais; Celulares; Laptops, netbooks e notebooks; Pen drives, cartões de memória, HDD, SSD, CDs, DVDs, disquetes; gravadores de vídeo digital (DVR); Impressoras; Tablets.

Cuidados com dados pessoais:

- Antes do descarte, **remover todas as informações** armazenadas em discos rígidos, cartões de memória ou similares, conforme o art. 31, II, do Decreto nº 10.240/2020.
- Adotar métodos seguros de **sanitização de dados**, conforme recomendações da **ISO/IEC 27040**.
- Consumidores devem estar cientes de que, uma vez descartado o equipamento, ocorre a **transferência imediata da propriedade** do bem para os responsáveis pelo sistema e a irreversibilidade dos dados nele contidos (art. 32, Brasil, 2020).
- Em caso de uso indevido ou acesso não autorizado a informações, deve-se formalizar denúncia às autoridades competentes (art. 31, § 2º, Brasil, 2020).

Benefícios da conformidade:

- Redução da extração de recursos naturais;
- Reaproveitamento de materiais como insumos para novas tecnologias;
- Preservação ambiental e fortalecimento da justiça social;
- Maior segurança no tratamento de informações sensíveis.

3.3 Família ISO/IEC 27000

A **Organização Internacional de Normalização (ISO)** foi criada em 1947, a partir da fusão entre a *International Federation of the National Standardizing Associations (ISA)* e o *United Nations Standards Coordinating Committee (UNSCC)*. Com sede em Genebra, Suíça, reúne representantes de organismos nacionais de normalização de mais de 160 países. Seu objetivo principal é desenvolver normas técnicas internacionais que promovam **padronização, qualidade e segurança** em produtos, serviços e sistemas (Oliveira, 2021).

No Brasil, a **Associação Brasileira de Normas Técnicas (ABNT)**, fundada em 1940, é a entidade responsável por adotar, traduzir e difundir as normas ISO. Reconhecida como o **Foro Nacional de Normalização**, a ABNT representa oficialmente o país junto à ISO e adapta as normas internacionais à realidade nacional, garantindo que os padrões globais possam ser aplicados ao contexto brasileiro (Lavos, 2023).

As normas ISO possuem caráter **voluntário**, já que são elaboradas por uma organização internacional não governamental e não possuem força de lei. Contudo, sua adoção é amplamente estratégica, pois oferecem diretrizes reconhecidas mundialmente que aumentam a eficiência, reduzem riscos e fortalecem a conformidade de processos em diferentes setores (Tapia; Valdés; Gutiérrez, 2021).

IMPORTÂNCIA PARA AS BOAS PRÁTICAS

A adoção da família **ISO/IEC 27000** representa um passo fundamental para organizações que desejam alinhar sua gestão de segurança da informação a padrões internacionalmente reconhecidos. Ao aplicar essas normas, a instituição:

- Garante maior **confiança e transparência** junto à sociedade e parceiros;
- Aumenta sua **resiliência operacional**, evitando interrupções críticas;
- Atende a exigências legais relacionadas à **LGPD** e a políticas públicas como a **PNRS**;
- Reforça práticas de **proteção de dados** e de **descarte seguro** de ativos e equipamentos.

Assim, a integração da família **ISO/IEC 27000** ao dia a dia institucional fortalece a governança, promove a cultura de prevenção e assegura que os processos de tratamento e descarte de informações sejam conduzidos de forma segura, auditável e sustentável.

FAMÍLIA ISO/IEC 27000

Entre as normas ISO, destaca-se a família ISO/IEC 27000, voltada à Gestão de Segurança da Informação (GSI). Esse conjunto de normas orienta a criação de um Sistema de Gestão de Segurança da Informação (SGSI), fornecendo princípios e requisitos para estabelecer, implementar, manter e melhorar continuamente controles de segurança. O objetivo é proteger os ativos informacionais críticos, reduzir riscos e assegurar a continuidade dos serviços (Rodrigues, 2024). Para que um SGSI funcione de forma eficaz, é essencial o comprometimento da alta gestão e a participação de todos os setores da organização. Isso inclui a definição de responsabilidades, papéis, políticas, controles e processos que assegurem a integridade, confidencialidade e disponibilidade da informação.

No contexto da Segurança da Informação (SI), a família de normas ISO/IEC 27000 estabelece diretrizes para a implementação, auditoria e aprimoramento contínuo de SGSI (Lavos, 2023). A certificação baseada nessas normas não se limita a um procedimento formal, mas representa um diferencial competitivo, pois confere reconhecimento internacional às organizações e fortalece sua credibilidade perante clientes, fornecedores, colaboradores e parceiros (Barreto et al., 2018). Além disso, sua adoção proporciona um processo sistemático de identificação, tratamento e correção de vulnerabilidades, reduzindo riscos e aumentando a resiliência operacional.

Quadro 2: Lista da série ISO/IEC 27000 e funções principais

Norma ISO/IEC	Função Principal
27000	Termos e definições para Sistemas de Gestão de Segurança da Informação (SGSI).
27001	Requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI.
27002	Diretrizes para implementação de controles de segurança da informação.
27003	Guia para implementar um SGSI.
27004	Medição e monitoramento da eficácia do SGSI.
27005	Gestão de riscos de segurança da informação.
27006	Requisitos para órgãos que auditam e certificam SGSI.
27007	Diretrizes para auditoria de SGSI.
27008	Avaliação de controles implementados no SGSI.
27014	Diretrizes para governança de segurança da informação.
27017	Controles de segurança para serviços de nuvem.
27018	Proteção de dados pessoais em nuvens públicas.
27031	Planejamento da continuidade dos negócios em segurança da informação.
27032	Segurança cibernética e proteção contra ameaças na internet.
27033	Proteção de comunicações entre redes (dividida em várias partes).
27034	Segurança de aplicativos desenvolvidos internamente ou adquiridos/operados por 3ºs.
27035	Gestão de incidentes de segurança da informação.
27037	Preservação, coleta, manuseio e descarte de evidências digitais, incluindo equipamentos de armazenamento de dados.
27039	Implementação e gestão de sistemas de detecção e prevenção de intrusão.
27040	Técnicas de segurança para proteção de ambientes de armazenamento de dados.
27701	Gestão da privacidade e dados pessoais (expansão da ISO/IEC 27001).

Fonte: ISO/IEC

ISO/IEC 27001

A ISO/IEC 27001 é a norma central dessa família. Ela estabelece os requisitos para que uma organização possa ser certificada em segurança da informação. O processo de certificação é conduzido por um Registered Certification Body (RCB), que realiza auditorias documentais e presenciais para verificar se os controles estão corretamente aplicados.

- A certificação tem validade de três anos;
- Exige auditorias anuais de monitoramento;
- Caso sejam identificadas não conformidades graves, o certificado pode ser suspenso até que os ajustes necessários sejam realizados (Magalhães, 2021).

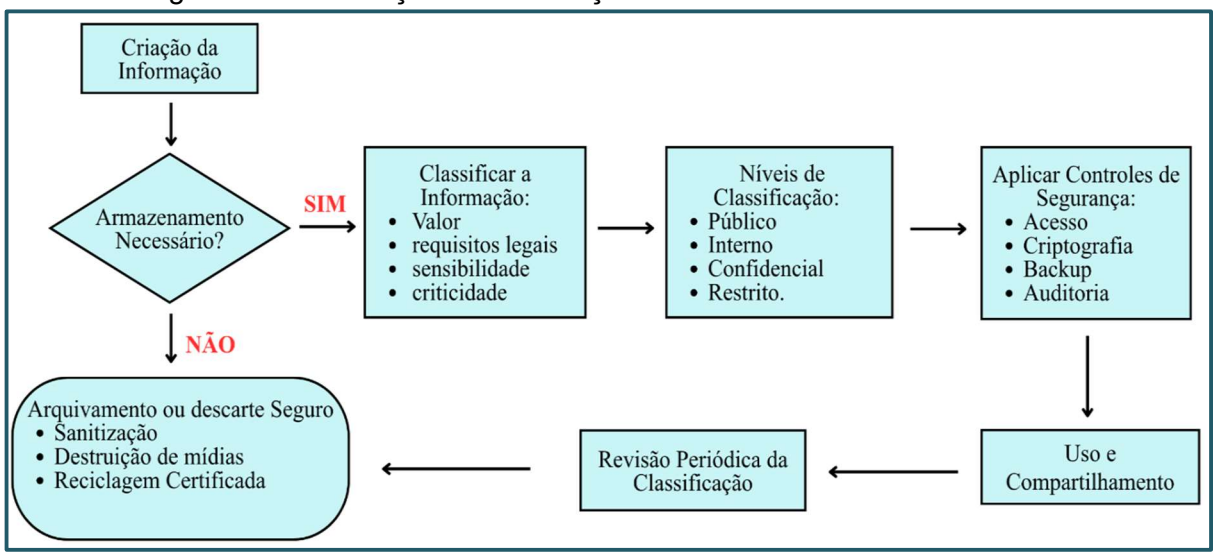
ISO/IEC 27002

A ISO/IEC 27002 complementa a ISO/IEC 27001, fornecendo diretrizes e boas práticas para a devida implementação dos controles da segurança da informação.

- Define objetivos de controle e medidas a serem aplicadas;
- Orienta sobre classificação, armazenamento, transferência e descarte seguro da informação

A Figura 7 ilustra visualmente esse processo normativo, destacando a necessidade de um procedimento estruturado antes do armazenamento de dados pessoais. A representação gráfica adota uma lógica sequencial, com base nos princípios da norma ISO/IEC 27002.

Figura 7: Classificação da Informação conforme a ISO/IEC 27002



Fonte: Elaboração Própria, 2025.

ISO/IEC 27037

A ISO/IEC 27037 fornece diretrizes para a identificação, aquisição, coleta e preservação de evidências digitais.

- Orienta sobre os procedimentos adequados para a coleta e preservação forense;
- Estabelece responsabilidades de peritos e organizações durante o processo de manuseio;
- Apoia investigações forenses conforme normas legais e técnicas;
- Estabelece princípios para garantir a integridade e autenticidade das evidências.

ISO/IEC 27040

A norma ISO/IEC 27040 estabelece princípios, requisitos e controles para a proteção das informações em ambientes de armazenamento físico e em nuvem.

- Aborda riscos relacionados a dispositivos de armazenamento de dados e ao ciclo de vida da informação;
- Fornece recomendações sobre criptografia, sanitização, descarte e destruição de mídias;
- Reforça a importância de políticas de backup, redundância e continuidade dos negócios.

ISO/IEC 27701

A norma ISO/IEC 27701 recomenda requisitos adicionais para o tratamento de dados pessoais.

- Apoia organizações nacionais e internacionais na legislação de proteção de dados;
- Fornece controles específicos para controladores e operadores de dados pessoais.
- Facilita a conformidade com legislações como a LGPD e a GDPR.

4

Fluxogramas

O fluxograma é uma técnica gráfica de representação sequencial de atividades, que permite visualizar, de forma ordenada e lógica, as etapas envolvidas na execução de um processo (Cruz, 2013). Utiliza símbolos padronizados para descrever operações, pontos de decisão, promovendo uma melhor compreensão do fluxo de trabalho e facilitando sua análise (Cury, 2015).

Os fluxogramas os quais este Manual de Boas Práticas tem como elementos chaves, na prática do descarte de ativos com armazenamento de dados, foram desenvolvidos com o uso do *software* gratuito *Bizagi Modeler* (versão 4.2.0.003). Este foi escolhido por sua interface intuitiva, facilidade de uso e compartilhamento com a notação *Business Process Model and Notation* (BPMN) – padrão amplamente utilizado para representar graficamente processos de negócios e operacionais.

São elementos estruturais fundamentais para o entendimento dos fluxogramas elaborados:

1. Início – Representa o ponto de partida de um processo, indicando onde as ações começam a ser executadas.

2. Tarefa – Corresponde a uma ação ou atividade específica que faz parte da sequência de etapas do processo.

3. Objeto de Dados – Simboliza materiais de apoio como documentos, planilhas, relatórios ou formulários utilizados no fluxo.

4.Decisão – Indica a necessidade de escolher entre alternativas, definindo qual caminho o processo seguirá.

5. Raia – Utilizada para separar e identificar responsáveis, departamentos ou áreas envolvidas em determinadas etapas do processo.

6. Fim – Demonstra o encerramento do processo, ou seja, o ponto em que o fluxo chega à sua conclusão.

7. Fluxo de sequência – Indica a ordem cronológica em que as etapas do processo devem ser executadas.

FLUXOGRAMAS DO CICLO DE VIDA DOS ATIVOS DE ARMAZENAMENTO

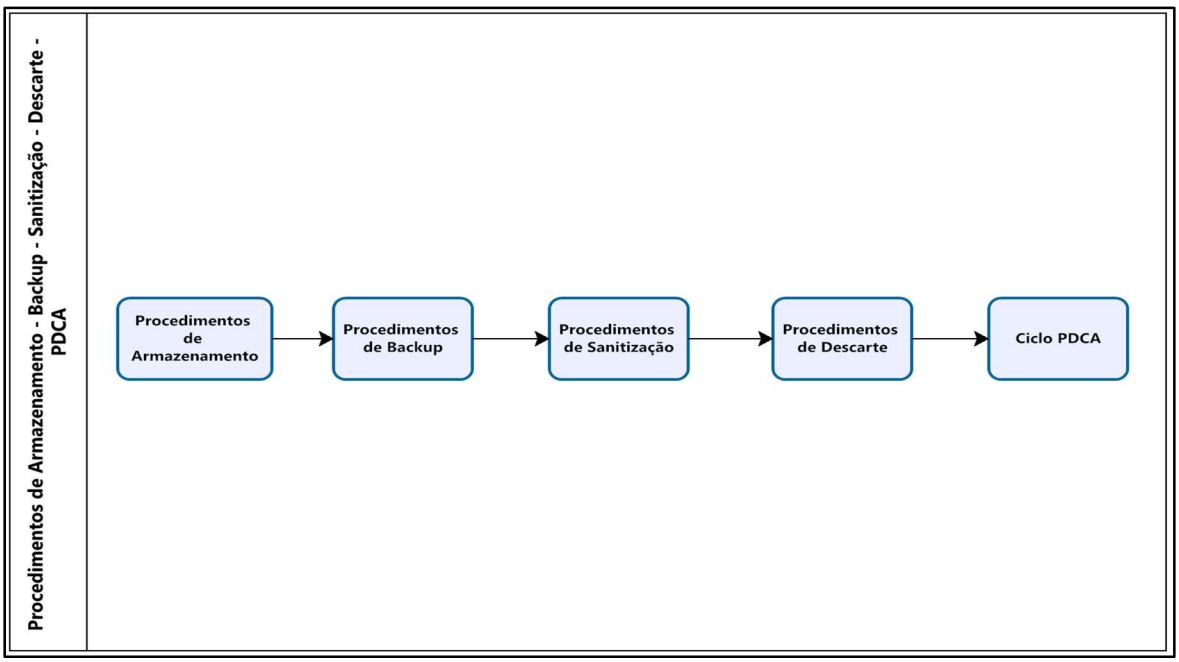
Os fluxogramas apresentados nesta seção representam, de forma clara e sequencial, as etapas essenciais para a gestão de dados em todo o seu ciclo de vida. Foram estruturados com base em normas da família ISO/IEC 27000, LGPD e PNRS, permitindo a padronização de procedimentos e a melhoria contínua da gestão da informação.

As etapas contemplam:

1. Armazenamento – definição do local, meio e controles adequados para guardar dados com segurança.
2. Backup – criação e teste periódico de cópias de segurança para garantir a continuidade das operações.
3. Sanitização – remoção segura de informações de mídias, evitando acesso indevido.
4. Descarte – eliminação definitiva dos ativos, seguindo critérios de segurança e sustentabilidade.
5. Gestão contínua (PDCA) – monitoramento, auditoria e revisão dos processos, visando à conformidade legal e à redução de riscos.

O fluxograma final, Figura 8, consolida essas práticas em um modelo integrado, mas flexível, que pode ser aplicado de forma parcial ou completa, conforme a realidade de cada organização. Dessa forma, a ferramenta apoia o cumprimento das exigências legais, o fortalecimento da segurança da informação e a promoção da cidadania digital responsável.

Figura 8: Procedimentos de descarte de Ativos: Armazenamento - *Backup* – Sanitização – Descarte – PDCA



Fonte: Elaboração própria, 2025.

4.1 **Armazenamento de Dados**

O armazenamento de dados corresponde ao processo de guardar informações digitais em dispositivos físicos ou virtuais, de modo que possam ser recuperadas, utilizadas e gerenciadas quando necessário. Esses dados podem ser pessoais, corporativos ou institucionais, variando desde simples arquivos de texto até bases de dados complexas, registros financeiros, imagens, vídeos e sistemas inteiros.

Os dispositivos de armazenamento podem ser classificados em diferentes tipos:

1. Armazenamento interno: presente em computadores, notebooks, tablets e celulares, geralmente por meio de discos rígidos (HDD) ou unidades de estado sólido (SSD).
2. Armazenamento externo ou portátil: dispositivos como pen drives, cartões de memória, CDs, DVDs e HDs externos, que permitem transportar dados entre diferentes equipamentos.
3. Armazenamento em rede ou em nuvem: sistemas conectados, como servidores, storages e plataformas online, que permitem o acesso remoto às informações.

Do ponto de vista da segurança da informação, esses ativos são considerados críticos, pois contêm dados que, se não forem devidamente tratados no momento do descarte, podem gerar riscos como:

- Vazamentos de informações sensíveis (pessoais, corporativas ou estratégicas);
- Fraudes e acessos não autorizados;
- Descumprimento de legislações como a LGPD.

Portanto, compreender o que são dispositivos de armazenamento e a relevância das informações neles contidas é essencial para adotar práticas corretas de eliminação, reciclagem e destinação final, garantindo ao mesmo tempo a proteção de dados e a preservação ambiental.

Os procedimentos de armazenamento seguro de dados pessoais demandam atenção especial, uma vez que se relacionam diretamente à proteção de direitos fundamentais. A LGPD, ao estabelecer marcos regulatórios para o tratamento de informações, fortalece garantias constitucionais como a privacidade, a liberdade de expressão, a dignidade da pessoa humana e o direito à informação, configurando-se como um instrumento essencial para a cidadania digital.

Nesse sentido, a proteção de dados pessoais transcende aspectos técnicos, estando ancorada em valores constitucionais e legais que delimitam o uso das informações e asseguram ao indivíduo sua autonomia e segurança no contexto da sociedade da informação (Miragem, 2019).

A proteção de dados pessoais está diretamente relacionada à preservação de direitos fundamentais como: **Privacidade**; **Liberdade de expressão**; **Dignidade da pessoa humana**; **Acesso à informação**. Esses direitos formam a base da **cidadania digital**, definindo limites para o uso das informações pessoais por organizações públicas e privadas. A Figura 9 apresenta esses princípios constitucionais e legais de forma visual, destacando sua integração à prática de gestão de dados.

Figura 9: Direitos fundamentais relacionados à proteção de dados pessoais

Fonte: Adaptado de Sá (2019).

Pode-se considerar, portanto que o armazenamento de dados pessoais deve ser realizado de forma segura, pois envolve a proteção de um direito fundamental. A **LGPD** estabelece que a utilização de informações pessoais deve ocorrer dentro de marcos legais e éticos, assegurando tanto a privacidade dos indivíduos quanto o desenvolvimento econômico sustentável.

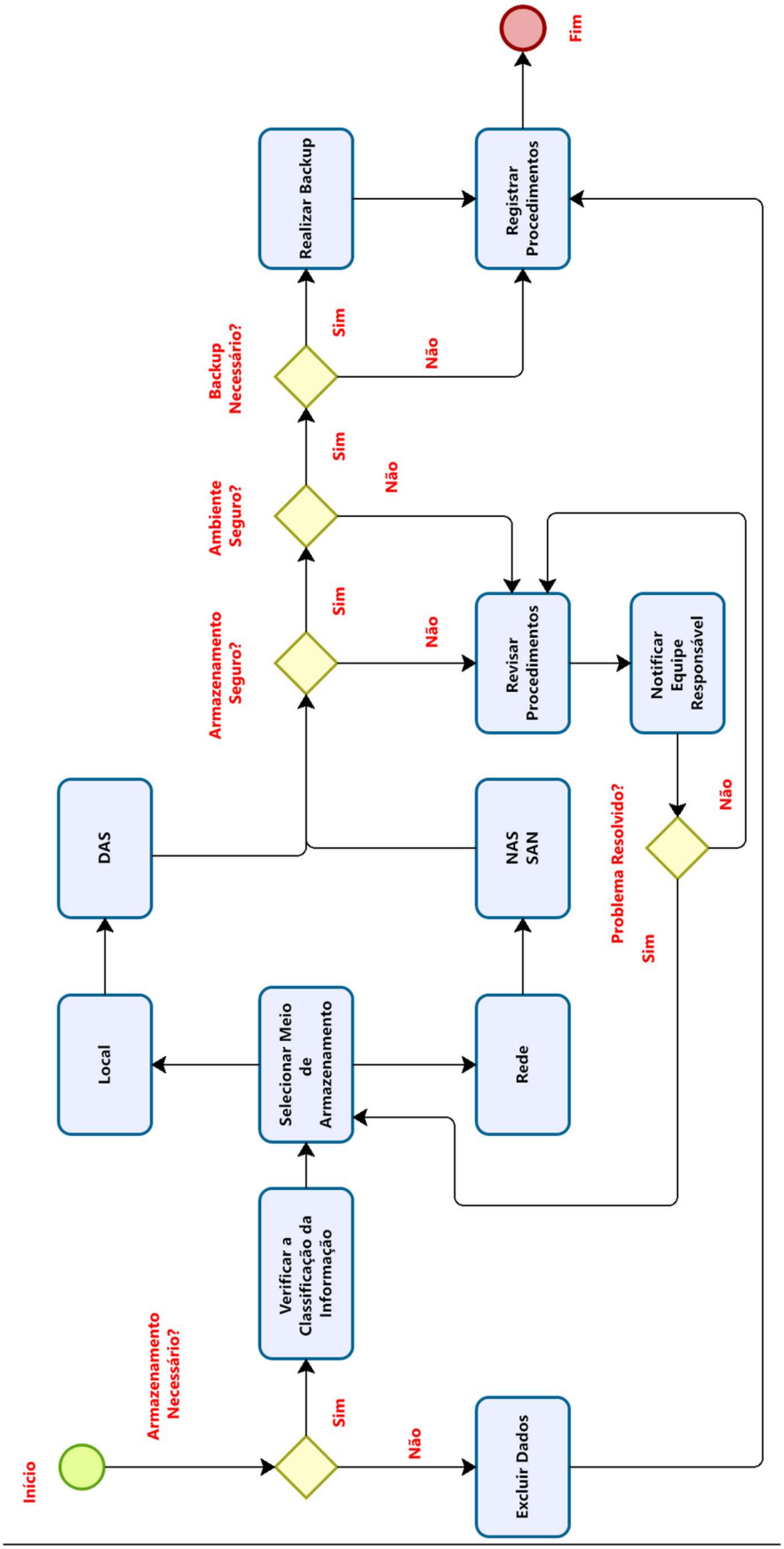
BOAS PRÁTICAS PARA A PROTEÇÃO DE DADOS PESSOAIS

- Definir ambientes seguros para o armazenamento (servidores, nuvem ou mídias físicas com controles adequados);
- Restringir o acesso apenas a pessoas autorizadas;
- Monitorar continuamente o uso e a integridade dos dados armazenados;
- Adotar políticas claras de retenção e descarte, respeitando prazos legais e finalidades específicas.

PARA ISSO, DEVE-SE REALIZAR:

- **Classificação da informação**: estabelecer critérios para identificar níveis de sensibilidade dos dados e definir controles de acesso proporcionais.
- **Medidas técnicas de segurança**: aplicar ferramentas e protocolos de proteção (criptografia, backups, controle de acessos, monitoramento de incidentes).
- **Medidas organizacionais**: implementar políticas internas claras, com responsabilidades definidas sobre o tratamento de dados.
- **Capacitação contínua**: promover treinamentos regulares para colaboradores, reforçando a importância da proteção de dados e das responsabilidades legais.
- **Prevenção de vulnerabilidades**: revisar periodicamente sistemas, procedimentos e contratos, garantindo conformidade com a LGPD e normas internacionais (ex.: ISO/IEC 27002).
- **Gestão de riscos**: manter processos de avaliação contínua para antecipar falhas, reduzir riscos de vazamento e aumentar a confiança nas operações.

Figura 10: Fluxograma de Procedimentos de Armazenamento de Dados



Procedimentos de Armazenamento de Dados.

Fonte: Elaboração própria, 2025.

FLUXOGRAMA - ETAPAS DO PROCEDIMENTO DE ARMAZENAMENTO DE DADOS:

1. **Verificação da necessidade de armazenamento**
    - Avaliar se o dado realmente precisa ser armazenado, em conformidade com o princípio da minimização previsto na LGPD.
    - O armazenamento desnecessário eleva riscos, custos e consumo de recursos (ISO/IEC 27040).
    - Verificar a classificação da informação, conforme abordagens da LGPD e LAI.

2. **Avaliação do local e do meio de armazenamento**
    - Considerar fatores como capacidade, custos, infraestrutura disponível e frequência de acesso.
    - Escolher entre armazenamento local (DAS) ou em rede (NAS ou SAN), conforme a criticidade da informação e a finalidade do tratamento.
    - Seguir critérios da ISO/IEC 27002, ISO/IEC 27040 e ISO/IEC 27701.

3. **Implantação de controles de segurança**
    - Implementar controles físicos e lógicos: autenticação, criptografia, registros de acesso e monitoramento contínuo.
    - Adotar políticas administrativas de gestão de acesso e auditoria periódica, conforme ISO/IEC 27001 e ISO/IEC 27002.

4. **Gestão de cópias de segurança (backup)**
    - Realizar backups de acordo com a criticidade das informações.
    - Garantir continuidade dos negócios e disponibilidade da informação, conforme diretrizes da ISO/IEC 27001 e art. 46 da LGPD.

5. **Verificação e revisão periódica do ambiente**
    - Conduzir auditorias internas, relatórios de conformidade e testes de segurança.
    - Caso sejam identificadas falhas, revisar critérios, controles e registros adotados.
    - Aplicar planos de ação corretiva e indicadores de eficácia, garantindo melhoria contínua (ISO/IEC 27001).

4.2 Procedimentos de *Backup*

O procedimento de *backup* é uma etapa indispensável da governança em segurança da informação, pois garante a continuidade dos serviços, preserva a integridade dos dados e previne perdas em incidentes tecnológicos.

A prática mais recomendada é a estratégia 3-2-1, que consiste em:

- Manter três cópias atualizadas dos dados;
- Utilizar dois tipos diferentes de mídia (ex.: servidor local e nuvem);
- Armazenar uma cópia em local externo ao ambiente principal.

Essa prática está diretamente alinhada ao art. 46 da LGPD, que exige a adoção de medidas técnicas e administrativas para proteger dados pessoais contra acessos não autorizados, destruição, perda, alteração ou difusão indevida.

A Figura 11 comunica, de forma visual, os principais requisitos para a realização de *backups* em ambientes organizacionais: segurança (representada pelo escudo e cadeado), automação (ícone do *notebook* com sincronização), redundância (armazenamento local e em nuvem) e gestão eficiente (engrenagens). Na elaboração da imagem foi planejado que cada elemento visual carregasse um significado técnico e simbólico.

Figura 11: Procedimentos de *backup* em ativos contendo dados

Fonte: Elaboração própria, 2025.

AQUITETURA DO FLUXOGRAMA DE BACKUP - AÇÕES SEQUENCIAIS

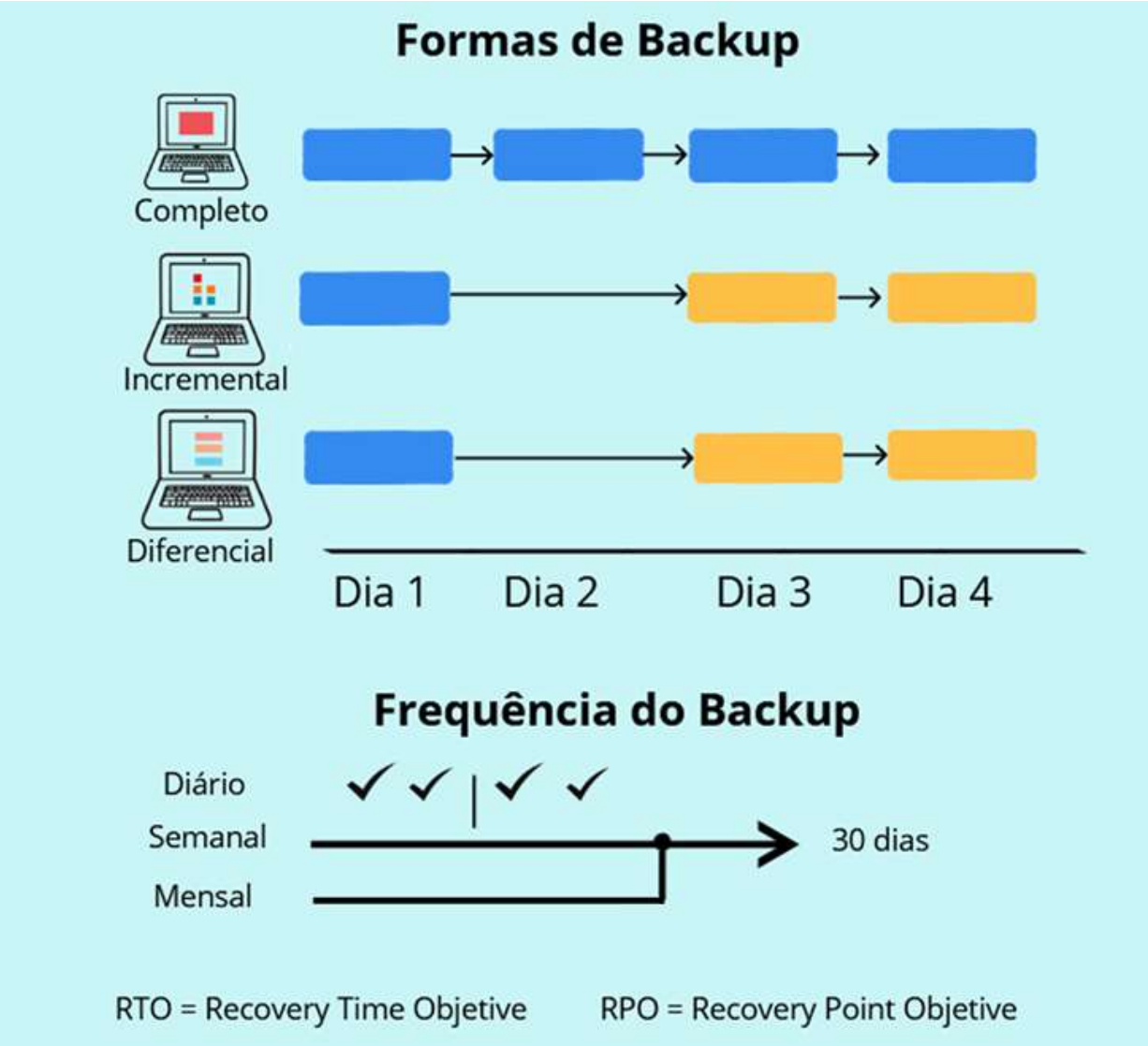
- **Seleção dos dados** → Definição das informações que realmente necessitam ser preservadas, conforme o princípio da minimização de dados (LGPD, art. 6º, III).
- **Necessidade de backup** → Verificação se a cópia é justificada; evita redundância e custos desnecessários.
- **Criticidade das informações** → Classificação da sensibilidade e importância dos dados, conforme recomenda a ISO/IEC 27002.
- **Arquitetura de backup** → Escolha entre Local, DAS, NAS/SAN, considerando escalabilidade, tempo de recuperação, custos e riscos, conforme ISO/IEC 27040.

Figura 12: Ações sequências de Backup de Dados

Fonte: Elaboração própria, 2025.

- **Forma de backup** → Definição entre Completo, Incremental ou Diferencial, levando em conta RTO (Recovery Time Objective), RPO (Recovery Point Objective) e a natureza das informações (Figura 13).
- **Frequência do backup** → Intervalo em que serão feitas as cópias, alinhado ao RPO e às exigências de continuidade de negócios.

Figura 13: Formas e Frequência de Backup – Exemplo prático



Fonte: Elaboração própria, 2025.

- **Execução (manual ou automática)** → Decisão entre backup manual (dependente de operador, indicado para situações específicas) ou automático (recomendado pela ISO/IEC 27002 por reduzir falhas humanas).

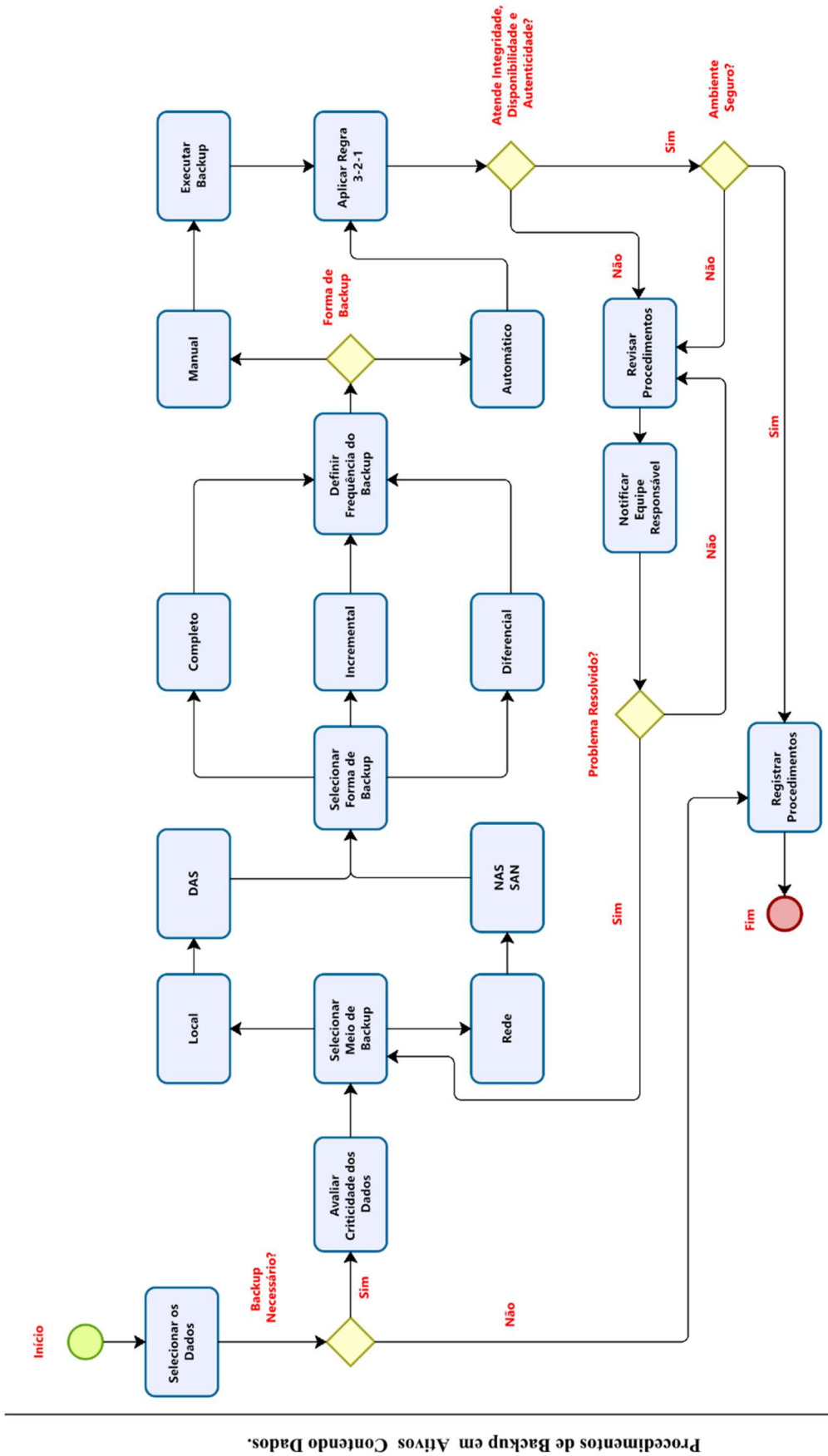
- **Regras de backup (3-2-1)** → Boas práticas de resiliência: 1 cópia de produção, 2 cópias em mídias distintas e 1 cópia externa.

Figura 14: Estratégia de Backup – 3-2-1

Fonte: Elaboração própria, 2025.

- **Verificação de integridade e autenticidade** → Testes para assegurar que os backups podem ser restaurados corretamente, em conformidade com a LGPD (princípios de segurança e prevenção).
- **Registro do procedimento** → Formalização do processo, com informações sobre data, responsáveis e resultados, garantindo rastreabilidade, auditoria e responsabilização.

Figura 15: Fluxograma de Procedimentos de *Backup* em Ativos Contendo dados



Procedimentos de Backup em Ativos Contendo Dados.

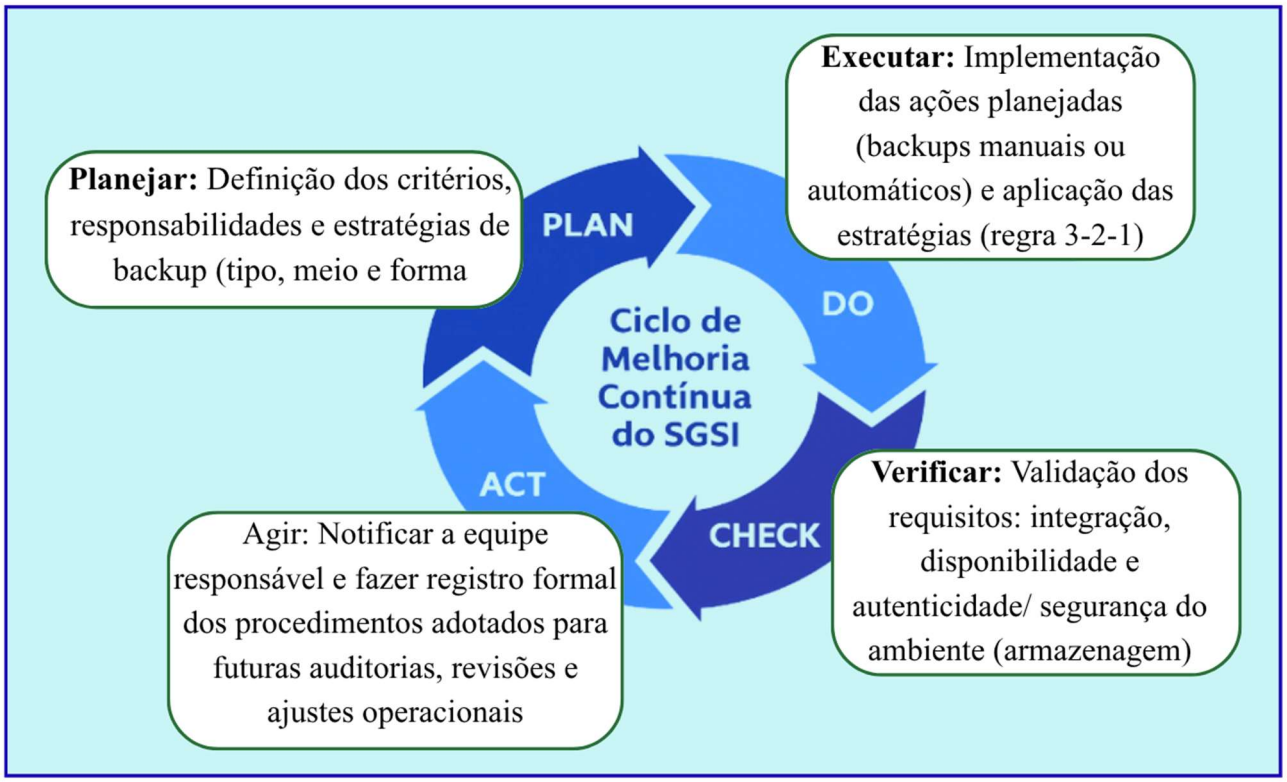
Fonte: Elaboração própria, 2025.

FLUXOGRAMA DE PROCEDIMENTOS DE BACKUP EM ATIVOS CONTENDO DADOS

1. **Selecionar os dados**
    - Explicar que a etapa inicial deve estar em conformidade com o princípio da **minimização de dados** (LGPD, art. 6º, III). Apenas informações realmente necessárias devem ser consideradas para backup, reduzindo riscos e custos.
2. **Avaliar a necessidade de backup**
    - Esclarecer que essa decisão deve considerar fatores como a **criticidade dos dados**, o valor estratégico para o negócio e os requisitos de **continuidade operacional**.
3. **Analisar criticidade das informações**
    - Relacionar com a **ISO/IEC 27002**, que prevê controles proporcionais ao nível de sensibilidade da informação. Dados pessoais, estratégicos ou confidenciais requerem maior robustez.
4. **Selecionar a arquitetura de backup (Local, DAS, NAS/SAN)**
    - Fundamentar na **ISO/IEC 27040**, trata da arquitetura de armazenamento e backup seguro.
    - Explicar quando cada tipo é mais indicado (ex.: Local → baixo custo e simplicidade; NAS/SAN → maior escalabilidade e resiliência).
5. **Definir a forma de backup (Completo, Incremental, Diferencial)**
    - Detalhar as diferenças técnicas de cada modelo.
    - Relacionar com critérios de **RTO e RPO** no plano de continuidade de negócios.
6. **Estabelecer a frequência do backup**
    - Relacionar à **dinâmica das atualizações**, criticidade dos sistemas e exigências regulatórias.
    - Destacar que uma periodicidade inadequada pode gerar **não conformidade** com a LGPD (perda ou exposição de dados pessoais).
7. **Definir o tipo de execução (Manual ou Automática)**
    - Explicar que a **ISO/IEC 27002** recomenda a automação para reduzir falhas humanas.
    - Justificar quando o backup manual ainda é necessário e como documentá-lo corretamente.
8. **Aplicar regras de backup (ex.: 1-2-3)**
    - Inserir a regra 1 cópia de produção + 2 cópias de segurança em diferentes mídias + 1 cópia externa/*off-line*.
    - Relacionar isso à resiliência contra desastres, falhas técnicas e ataques (ex.: ramsonwares).
9. **Verificar integridade e autenticidade dos dados**
    - Explicar a importância da checagem, garantindo que os backups possam ser restaurados sem corromper dados.
    - Relacionar com o princípio da **segurança e prevenção** da LGPD.
10. **Registrar o procedimento realizado**
    - Mostrar que o registro assegura **rastreabilidade**, **auditoria** e **responsabilização**, princípios centrais da LGPD e da ISO/IEC 27001.
11. **Encerramento do processo**
    - O ciclo só se encerra quando há comprovação de integridade e documentação completa.

Ao final do processo de *backup* de dados, representado pelas etapas “Notificar Equipe Responsável” e “Registrar Procedimentos” (Figura 16), estabelece-se uma ligação direta com o ciclo de melhoria contínua do SGSI, baseado na metodologia PDCA (Plan–Do–Check–Act), conforme a ISO/IEC 27001. Esse ciclo garante ajustes constantes nos procedimentos por meio de auditorias internas, revisões periódicas e evolução tecnológica.

Figura 16: PDCA - Ciclo de Melhoria contínua do SGSI do Fluxograma



Fonte: Elaboração Própria, 2025.

As estratégias de backup eficazes vão além da tecnologia, exigindo políticas institucionais claras, capacitação das equipes, controle de acessos, testes de restauração e revisões contínuas. Falhas em backups, frequentemente decorrentes de procedimentos não padronizados ou ausência de treinamentos, são apontadas como causas significativas de exposição indevida de dados pessoais.

Do ponto de vista técnico, é fundamental atenção em backups locais e na sanitização adequada das mídias após o descarte, evitando o uso indevido de informações sensíveis.

Dessa forma, o fluxograma elaborado traduz os requisitos da LGPD e das normas ISO/IEC 27001 e 27701, promovendo uma lógica processual coerente, preventiva e auditável, garantindo backups eficientes, juridicamente seguros e tecnicamente robustos, assegurando a proteção dos titulares de dados e a continuidade institucional.

4.3 Procedimentos de Sanitização

Os procedimentos de sanitização de ativos que armazenam dados pessoais e sensíveis são essenciais para garantir a eliminação segura dessas informações ao final de seu ciclo de vida. A necessidade de adotar medidas eficazes nesse processo decorre das obrigações legais impostas aos agentes de tratamento, que devem prevenir o acesso indevido ou a recuperação indevida dos dados, mesmo após o descarte de mídias e equipamentos (Brasil, 2018).

CONSIDERAÇÕES SOBRE SANITIZAÇÃO DE DADOS PARA O USUÁRIO

1. **O que é sanitização de dados**

- A sanitização não se resume à simples exclusão de informações. Trata-se de um **processo técnico, jurídico e ambiental**, que garante a remoção completa e segura de dados de ativos digitais antes de seu descarte ou reutilização.

2. **Importância legal**

- Cumpre a **LGPD**, prevenindo riscos de exposição indevida de dados pessoais.
- Reduz a possibilidade de **sanções legais e danos à reputação** da organização.
- Exige **políticas claras, documentadas e atualizadas**, garantindo a proteção dos direitos dos titulares de dados.

3. **Segurança da informação**

- Integra os **controles técnicos essenciais** para proteger ativos de informação.
- Deve seguir o **ciclo PDCA** (Planejar, Executar, Verificar, Agir), promovendo melhoria contínua.
- Inclui **atualização tecnológica, monitoramento e capacitação das equipes** para evitar vulnerabilidades e incidentes.

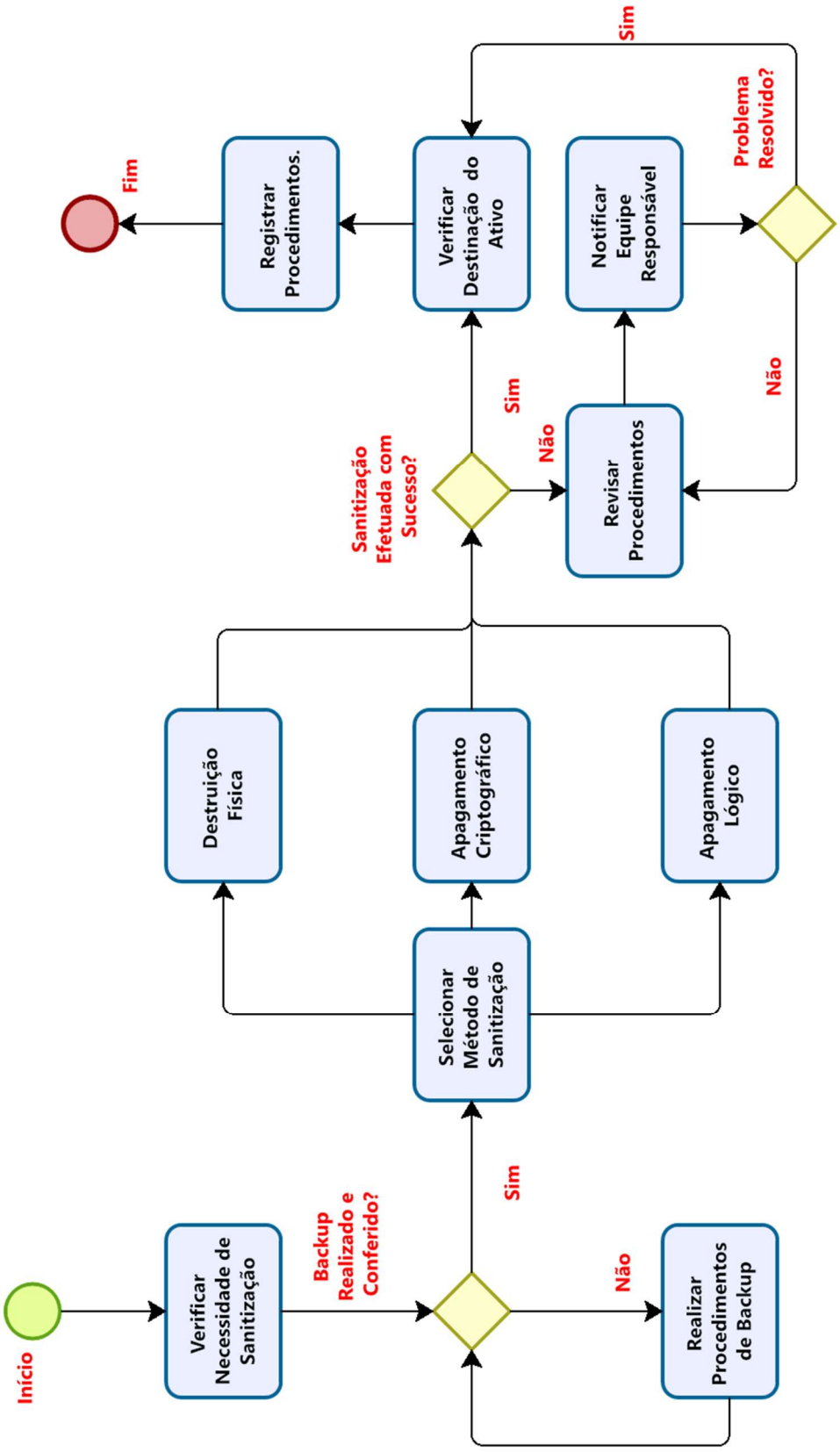
4. **Sustentabilidade ambiental**

- A sanitização adequada é pré-requisito para **reciclagem ou destinação correta de dispositivos eletrônicos**.
- Evita impactos ambientais do descarte inadequado, promovendo **logística reversa e responsabilidade compartilhada**.

5. **Benefícios de seguir o fluxograma**

- **Conformidade legal** com LGPD e normas relacionadas.
- **Segurança e integridade das informações**.
- **Sustentabilidade ambiental** no manejo de dispositivos eletrônicos.
- **Melhoria contínua** dos processos, garantindo eficácia, eficiência e adaptação a novas demandas.
- **Fortalecimento da confiança** de titulares de dados e *stakeholders.*

Figura 17: Fluxograma de Procedimentos de Sanitização em Ativos Contendo Dados



Fonte: Elaboração própria, 2025.

ETAPAS DO PROCEDIMENTO DE SANITIZAÇÃO DE DADOS

1. **Verificar necessidade de sanitização**
   - Avaliação se realmente há necessidade de exclusão dos dados do ativo.
   - Deve considerar requisitos legais, operacionais e técnicos.

2. **Backup realizado e conferido?**
   - Checagem da existência de cópia de segurança atualizada e válida.
   - Caso **não haja *backup***, deve-se interromper o processo e executar backup antes de continuar.

3. **Selecionar método de sanitização**
   - Escolha baseada no tipo de mídia, criticidade e sensibilidade da informação.
   - Métodos disponíveis:
     - ✓ **Destruição física** → indicada para mídias obsoletas, danificadas ou descartadas definitivamente.
     - ✓ **Apagamento criptográfico** → inutilização das chaves criptográficas, recomendado para dispositivos previamente criptografados.
     - ✓ **Apagamento lógico** → sobrescrita por software especializado, apropriado para mídias que serão reutilizadas.

4. **Sanitização efetuada com sucesso?**
   - Verificação da efetividade do processo.
   - Caso negativo, revisar e reaplicar o procedimento, optando por métodos mais rigorosos se necessário.

5. **Verificar destinação do ativo**
   - Definição sobre reutilização, descarte ou reencaminhamento do ativo.
   - Deve estar em conformidade com a política institucional de gestão de ativos.

6. **Registrar procedimentos**
   - Documentar todas as etapas: data, método utilizado, responsável técnico e resultado.
   - Garante rastreabilidade, auditoria e conformidade com a LGPD e normas ISO/IEC.

4.4 Procedimento de descarte

No procedimento de descarte de ativos de armazenamento de dados é fundamental compreender os aspectos legais, técnicos e ambientais que envolvem o descarte de ativos contendo dados. Tal procedimento exige condutas seguras e responsáveis, considerando a proteção das informações, a conformidade com a legislação vigente e os princípios da sustentabilidade.

A Figura 18 esquematiza o disposto no Decreto nº 10.240/2020, que estabelece que confere ao consumidor a responsabilidade de remover previamente todos os dados pessoais e informações privadas dos equipamentos (1), como forma de garantir a proteção da privacidade e prevenir eventuais violações. Cumprida essa exigência, o decreto isenta as empresas e entidades gestoras da responsabilidade por dados remanescentes, transferindo ao consumidor os riscos decorrentes de eventual omissão (2). O decreto reforça o dever legal dos comerciantes de informar o consumidor, no momento da entrega do equipamento, sobre a obrigatoriedade da exclusão dos dados (3). Por fim, destaca-se à perda tácita, imediata e irrevogável da propriedade dos bens descartados (4), o que implica na irrecuperabilidade dos dados neles contidos e na inexistência de qualquer direito à indenização, mesmo que os dispositivos venham a ser reutilizados por terceiros (Brasil, 2020).

Figura 18: Obrigações legais dos consumidores no descarte de produtos eletrônicos

Fonte: Elaboração própria, 2025.

A Figura 19, de forma integrada, ilustra as principais diretrizes legais, técnicas e ambientais que devem orientar o descarte responsável de ativos contendo dados. Ela reforça a necessidade de remoção prévia de informações pessoais, a irreversibilidade da perda da propriedade no ato do descarte e a importância de avaliar alternativas como reuso e manutenção antes da destinação final, conforme exigem a LGPD, o Decreto nº 10.240/2020 e a PNRS.

Figuras 19: Diretrizes para o descarte responsável de ativos com dados

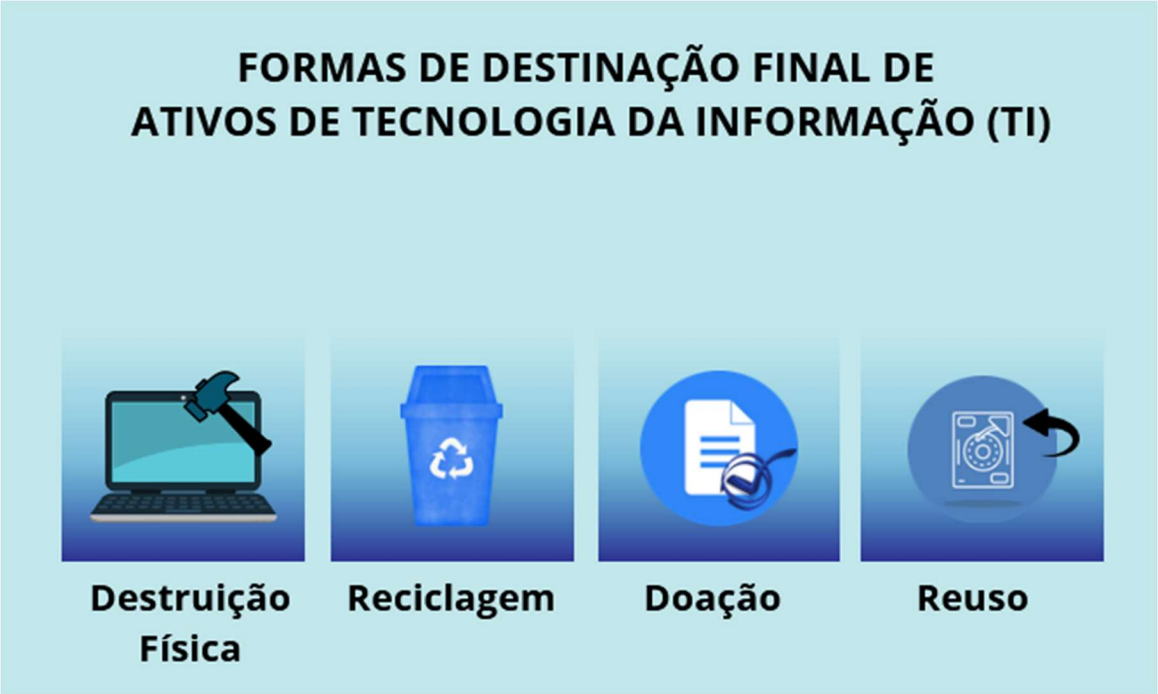
Fonte: Elaboração própria, 2025.

1. a remoção prévia dos dados é obrigatória;
2. o consumidor perde automaticamente a propriedade sobre o bem no ato do descarte;
3. empresas e entidades gestoras não respondem por dados não excluídos; e
4. eventuais usos indevidos podem ser denunciados às autoridades, sem previsão de indenização. Portanto, antes de encaminhar qualquer dispositivo para descarte, devem ser esgotadas todas as possibilidades de reaproveitamento, em consonância com os princípios da ecoeficiência e do desenvolvimento sustentável (Brasil, 2010).

FORMAS DE DESTINAÇÃO FINAL DE ATIVOS DE TI

As formas de destinação final de ativos de TI, Figura 20, devem seguir critérios que garantam a segurança da informação, a conformidade legal e a sustentabilidade ambiental. A destruição física deve ser realizada por meio de ferramentas seguras, como trituradores, prensas ou degaussing, com emissão de certificado de destruição. A reciclagem exige que os ativos sejam encaminhados para empresas licenciadas e certificadas (ISO 14001), após a sanitização completa dos dados. A doação de equipamentos deve ser registrada formalmente, garantindo a irrecuperabilidade das informações. Já o reuso pode ocorrer internamente, com controle de acesso e rastreabilidade, ou externamente, somente após a execução de sanitização segura, assegurando a proteção dos dados e a responsabilidade institucional.

Figura 20: Destinação final de ativos de tecnologia da informação



Fonte: Elaboração própria, 2025.

Independente da forma de destinação final adotada, o procedimento de descarte de ativos de TI deve ser concluído com o registro detalhado de todas as etapas executadas. Esse registro garante rastreabilidade, governança e conformidade com os princípios de transparência e prestação de contas, conforme o artigo 37 da LGPD e as recomendações da ISO/IEC 27002. Ele deve contemplar desde a verificação do backup e da sanitização dos dados até a documentação da destinação final, assegurando que todo o processo seja realizado de maneira segura, ética e ambientalmente responsável.

Embora a PNRS não especifique diretamente a necessidade de certificações como ISO 14001 ou ISO/IEC 27001, nem detalhe os procedimentos para emissão do Atestado de Destinação Final (ADF), ela estabelece diretrizes gerais para a gestão ambiental e a responsabilidade compartilhada pelo ciclo de vida dos produtos. Além disso, determina que as empresas elaborem e implementem Planos de Gerenciamento de Resíduos Sólidos (PGRS), conforme o artigo 33 da lei, promovendo práticas de gestão ambiental adequadas.

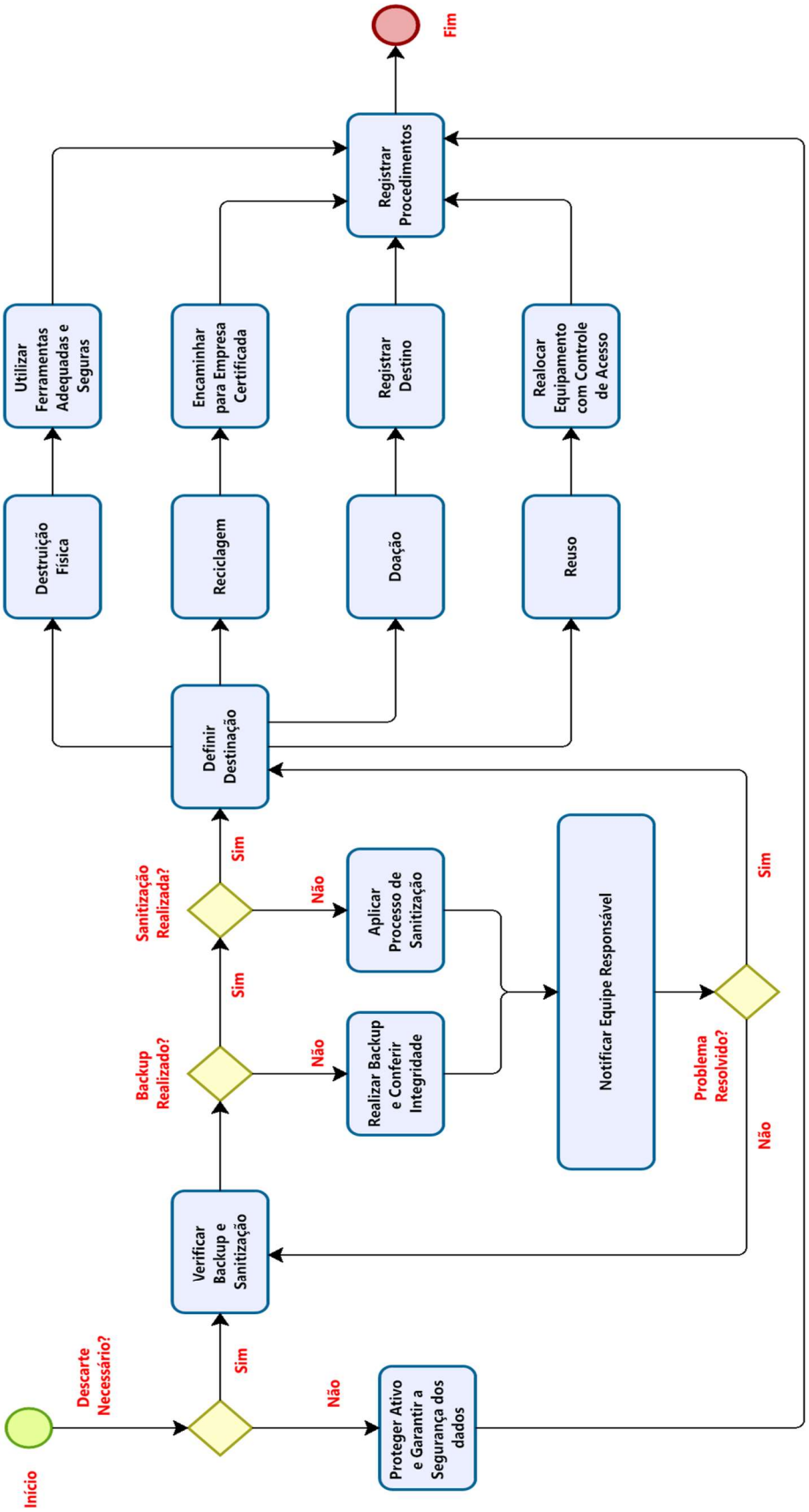
A emissão do ADF é regulamentada pelo Sistema Nacional de Informações sobre a Gestão dos Resíduos Sólidos (SINIR), conforme o Decreto nº 10.936/2022. Esse sistema exige que as empresas responsáveis pela destinação final de resíduos estejam licenciadas e cadastradas no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras e Utilizadoras de Recursos Ambientais (CTF/APP), conforme a Instrução Normativa Ibama nº 01/2013.

Portanto, para assegurar plena conformidade legal e ambiental, a empresa responsável pela destinação de resíduos deve: Possuir licenciamento ambiental válido; estar cadastrada no CTF/APP; apresentar certificações como ISO 14001 e ISO/IEC 27001; emitir o ADF por meio do SINIR, garantindo transparência e rastreabilidade de todo o processo (Figura 21).

Figura 21: Encaminhamento de dispositivos para empresas certificadas

Fonte: Elaboração própria, 2025.

Figura 22: Fluxograma de Procedimentos de Descarte em Ativos contendo dados



Procedimentos de Descarte em Ativos Contendo Dados.

Fonte: Elaboração própria, 2025.

ETAPAS DO PROCEDIMENTO DE DESCARTE EM ATIVOS CONTENDO DADOS

1. **Verificar necessidade de descarte**
    - Avaliar se o descarte é realmente necessário, considerando a obsolescência tecnológica, falhas irreparáveis ou término do ciclo de vida.
    - Caso **não seja necessário**, aplicar controles de segurança (ISO/IEC 27002) e manter o ativo protegido, registrando formalmente a decisão.
2. **Proteger ativo e garantir segurança dos dados**
    - Se o descarte não for autorizado ou for adiado, implementar controles para mitigar riscos de acesso indevido, perda de integridade ou uso inadequado.
    - Atender à LGPD (art. 6º, VII e VIII) e registrar os procedimentos adotados.
3. **Backup e verificação de integridade**
    - Confirmar se existe cópia de segurança válida e íntegra dos dados armazenados.
    - Se **não houver backup**, deve-se realizá-lo antes de prosseguir.
4. **Sanitização dos dados**
    - Confirmar se os dados foram removidos de forma definitiva.
    - Caso negativo, aplicar método adequado de sanitização (apagamento lógico, criptográfico ou destruição física), conforme ISO/IEC 27040.
    - Se falhar, notificar a equipe responsável para reaplicar o processo.
5. **Definição da destinação do ativo**
    - Escolher a forma de descarte mais adequada, considerando conformidade legal, segurança da informação e sustentabilidade (destruição física; reciclagem; Doação; reuso).
6. **Registro das decisões e procedimentos**
    - Documentar todas as etapas realizadas: data, responsável técnico, método de sanitização, destino do ativo.
    - Atender à LGPD (art. 37) e às recomendações da ISO/IEC 27037 e ISO/IEC 27002 sobre rastreabilidade e governança da informação.
    - Esse registro assegura transparência, prestação de contas e conformidade legal, técnica e ambiental.
7. **Encerramento do ciclo**
    - O processo somente é considerado finalizado quando todas as etapas foram concluídas e registradas.
    - Garante-se, assim, a conformidade com a LGPD, a PNRS e as normas ISO/IEC, assegurando um descarte seguro, ético e sustentável.

4.5 Ciclo PDCA

O gerenciamento eficaz da segurança da informação exige não apenas a implementação de controles técnicos, mas também a adoção de metodologias de gestão que assegurem a melhoria contínua dos processos organizacionais. Nesse contexto, modelos consagrados de gestão da qualidade passaram a ser incorporados ao SGSI, oferecendo um arcabouço estruturado para planejamento, execução, monitoramento e correção das práticas adotadas. Entre esses modelos destaca-se o ciclo PDCA, amplamente reconhecido por sua capacidade de sistematizar a busca por resultados consistentes, favorecer a integração entre áreas e fortalecer a cultura de prevenção e conformidade.

PDCA é uma sigla em inglês que representa um ciclo composto por quatro fases interligadas, utilizadas na gestão de processos com foco na melhoria contínua. As etapas são: ***P**lan* (planejar), ***D**o* (executar), ***C**heck* (verificar) e ***A**ct* (agir), explicadas na Figura 23, na configuração aplicada ao SGSI. Essa metodologia utilizada na gestão de qualidade por empresas que buscam a eficácia nos processos, promovendo integração entre diferentes áreas organizacionais e consolidando práticas sustentáveis e seguras (Magalhães, 2021).

Figura 23: Ciclo PDCA aplicado ao Sistema de Gestão da Segurança da Informação

Fonte: Adaptado de Magalhães (2021)

A metodologia PDCA, portanto, é utilizada nas organizações com o objetivo de alinhar as estratégias empresariais à melhoria dos resultados, promovendo, ao mesmo tempo, o aperfeiçoamento contínuo dos processos. Ela também é conhecida como Ciclo da Qualidade, por auxiliar na identificação e resolução de problemas internos, com base em uma abordagem estruturada que envolve ruptura e controle. Sua aplicação se concentra em quatro etapas principais: identificação das causas dos problemas e planejamento das ações corretivas (*Plan*), implementações das ações (*Do*), verificação dos resultados (C*heck*) e padronização das soluções adotadas (*Act*).

No contexto do descarte e gestão de ativos de TI, aplicar o PDCA permite estruturar processos de forma sistemática, segura e auditável, garantindo conformidade legal, eficiência operacional e proteção das informações. Neste contexto, considerando os quatro fluxogramas a Figura 24 demonstra o processo cíclico do descarte na lógica PDCA.

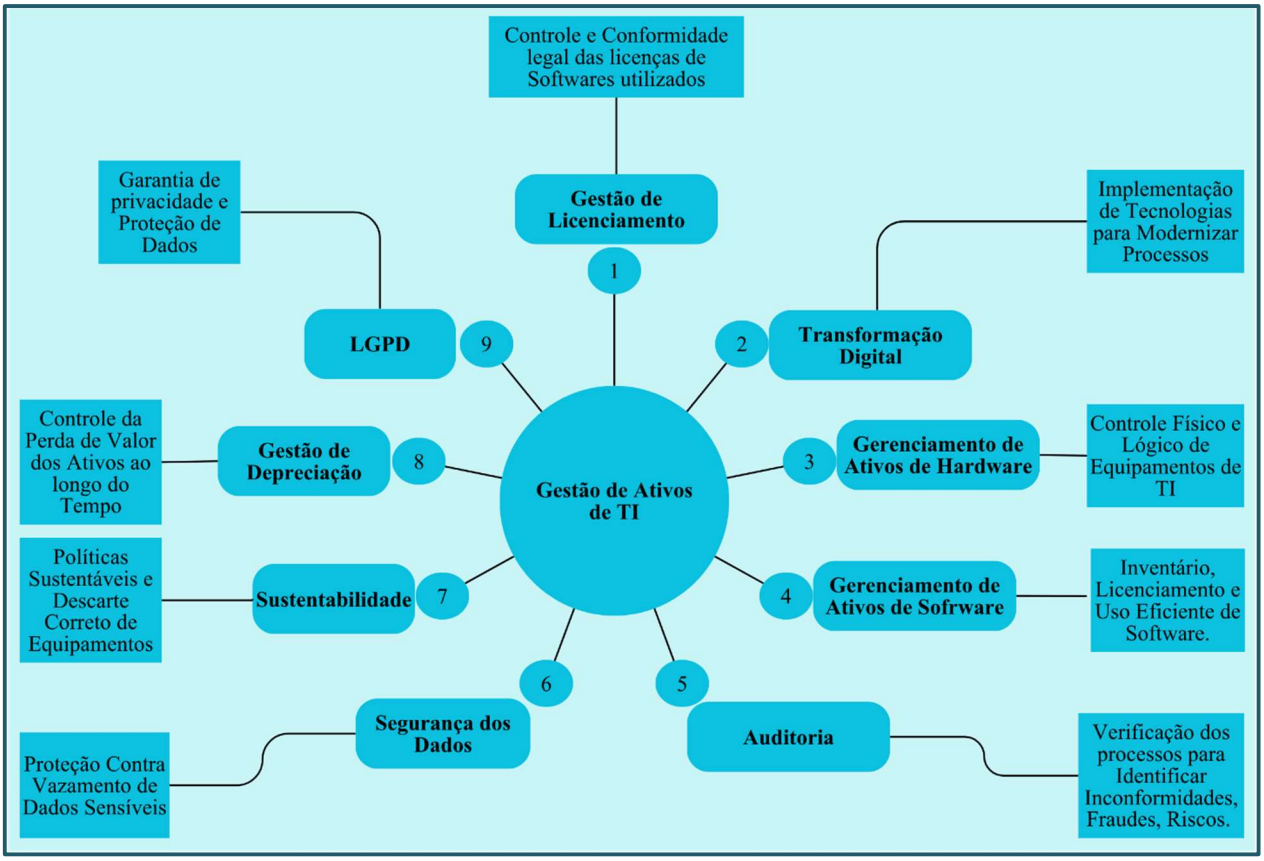
Figura 24: Sequência dos Procedimentos na lógica PDCA do ciclo de vida dos ativos

Fonte: Elaboração própria, 2025.

A aplicação do ciclo PDCA no gerenciamento do descarte de ativos de TI assegura que cada etapa do processo seja planejada, executada, verificada e corrigida de forma contínua, garantindo segurança, conformidade legal e sustentabilidade institucional.

Antes de detalhar os fluxogramas elaborados, é importante apresentar uma visão conceitual da Gestão de Ativos de TI, destacando os principais eixos que orientam as boas práticas identificadas. A Figura 25 apresenta um mapa conceitual que integra aspectos técnicos, jurídicos e ambientais, mostrando as ferramentas que podem ser aplicadas para gerir os ativos de TI de forma eficiente, segura e sustentável.

Figura 25: Ferramentas Aplicadas na Gestão de Ativos de TI



Fonte: Adaptado de Magma (2025).

A solução desenvolvida pela empresa Magma contempla **nove ferramentas integradas**, cada uma contribuindo para diferentes dimensões da gestão de ativos: legal, operacional, ambiental e de segurança da informação.

DESCRIÇÃO DAS FERRAMENTAS REPRESENTADAS:

1. **Gestão de Licenciamento** – Controle e conformidade legal de softwares, prevenindo uso indevido e assegurando contratos com fornecedores, conforme ISO/IEC 27002.

2. **Transformação Digital** – Modernização de processos internos por meio de digitalização, automação e integração, garantindo eficiência e segurança da informação (ISO/IEC 27001).

3. **Gerenciamento de Ativos de Hardware** – Inventário, rastreabilidade e monitoramento físico e lógico dos equipamentos, garantindo disponibilidade e descarte ambiental adequado (ISO/IEC 27002 e PNRS).

4. **Gerenciamento de Ativos de Software** – Controle de inventário e licenciamento, evitando redundâncias e promovendo conformidade interna e legal.

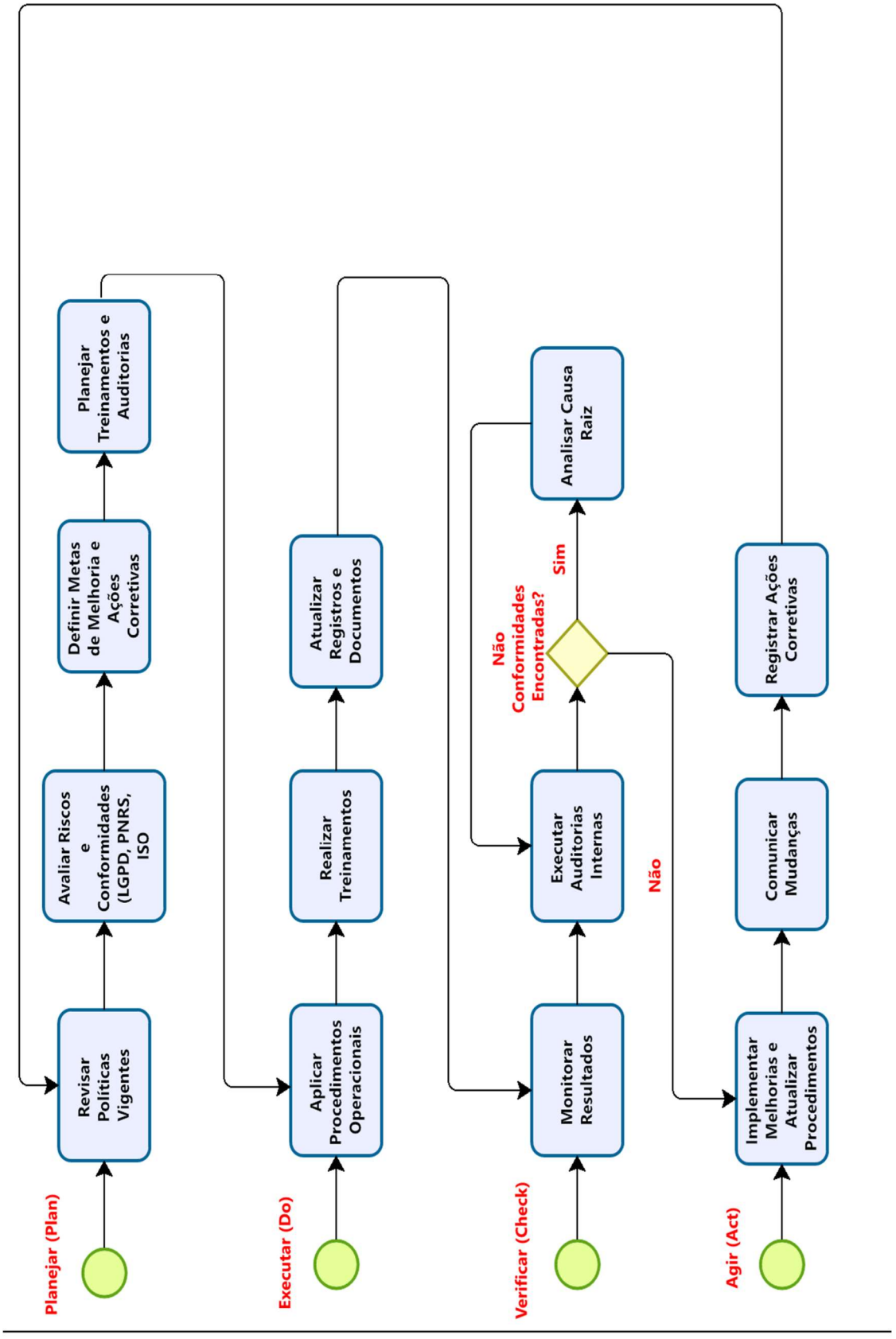
5. **Auditoria** – Verificação sistemática de processos para identificar inconformidades e oportunidades de melhoria, assegurando processos auditáveis e seguros (ISO/IEC 27001/27006).

6. **Segurança de Dados** – Proteção da confidencialidade, integridade e disponibilidade das informações por meio de criptografia, controle de acesso e monitoramento contínuo, conforme LGPD e ISO/IEC 27001, 27002, 27040.

7. **Sustentabilidade** – Práticas sustentáveis no uso e descarte de ativos, incluindo reuso, reciclagem e logística reversa, em conformidade com a PNRS.

8. **Gestão de Depreciação** – Controle da perda de valor dos ativos, planejamento de substituição de equipamentos e avaliação de custo-benefício, garantindo eficiência operacional e segurança ambiental.
9. **LGPD –** Garantia da privacidade e proteção de dados pessoais, com controle de acesso e medidas técnicas e organizacionais, alinhando-se à ISO/IEC 27701.

Figura 26: Fluxograma PDCA Aplicado à Gestão de Ativos de Informação



Fonte: Elaboração própria, 2025.

FLUXO DO PDCA APLICADO À GESTÃO DE ATIVOS DE INFORMAÇÃO

1. PLANEJAR (PLAN) - Nesta etapa ocorre a preparação estratégica e normativa do processo.

Fluxo de ações:

1. Revisar políticas vigentes – verifique regulamentos internos e externos que tratam da segurança da informação, descarte de ativos e sustentabilidade.
2. Avaliar riscos e conformidades – identifique vulnerabilidades e cheque aderência às legislações (LGPD, PNRS) e normas ISO/IEC (27001, 27002, 27701).
3. Definir metas de melhoria e ações corretivas – estabeleça indicadores claros (tempo médio de descarte, percentual de ativos reaproveitados, etc.) e planeje medidas de correção para riscos identificados.
4. Planejar treinamentos e auditorias – determine conteúdos de capacitação e cronograma de auditorias internas.
5. Ao concluir esta fase, deve haver um plano documentado que oriente as demais etapas.

2. EXECUTAR (DO) - O planejamento se transforma em prática.

Fluxo de ações:

1. Aplicar procedimentos operacionais – siga o roteiro definido: verificar necessidade do descarte → realizar backup → sanitizar ativos → definir destinação (reuso, doação, reciclagem ou descarte final) → registrar cada ação.
2. Realizar treinamentos – execute os treinamentos planejados, garantindo que todos os envolvidos conheçam os procedimentos técnicos, legais e ambientais.
3. Atualizar registros e documentos – formalize os procedimentos realizados, registrando datas, métodos e resultados obtidos.
4. Ao final, toda execução deve estar documentada e rastreável.

3. VERIFICAR (CHECK) - Fase dedicada ao controle e avaliação da execução.

Fluxo de ações:

1. Monitorar resultados – acompanhe indicadores de desempenho (ex.: tempo médio de descarte, falhas em sanitização, quantidade de ativos reaproveitados).
2. Executar auditorias internas – realize auditorias programadas para verificar conformidade com o planejamento, normas e legislações.
3. Analisar causa raiz (se necessário) – caso sejam identificadas não conformidades, investigue a origem do problema antes de propor soluções.
4. Essa etapa garante que falhas sejam identificadas e corrigidas antes de comprometer a integridade do processo.

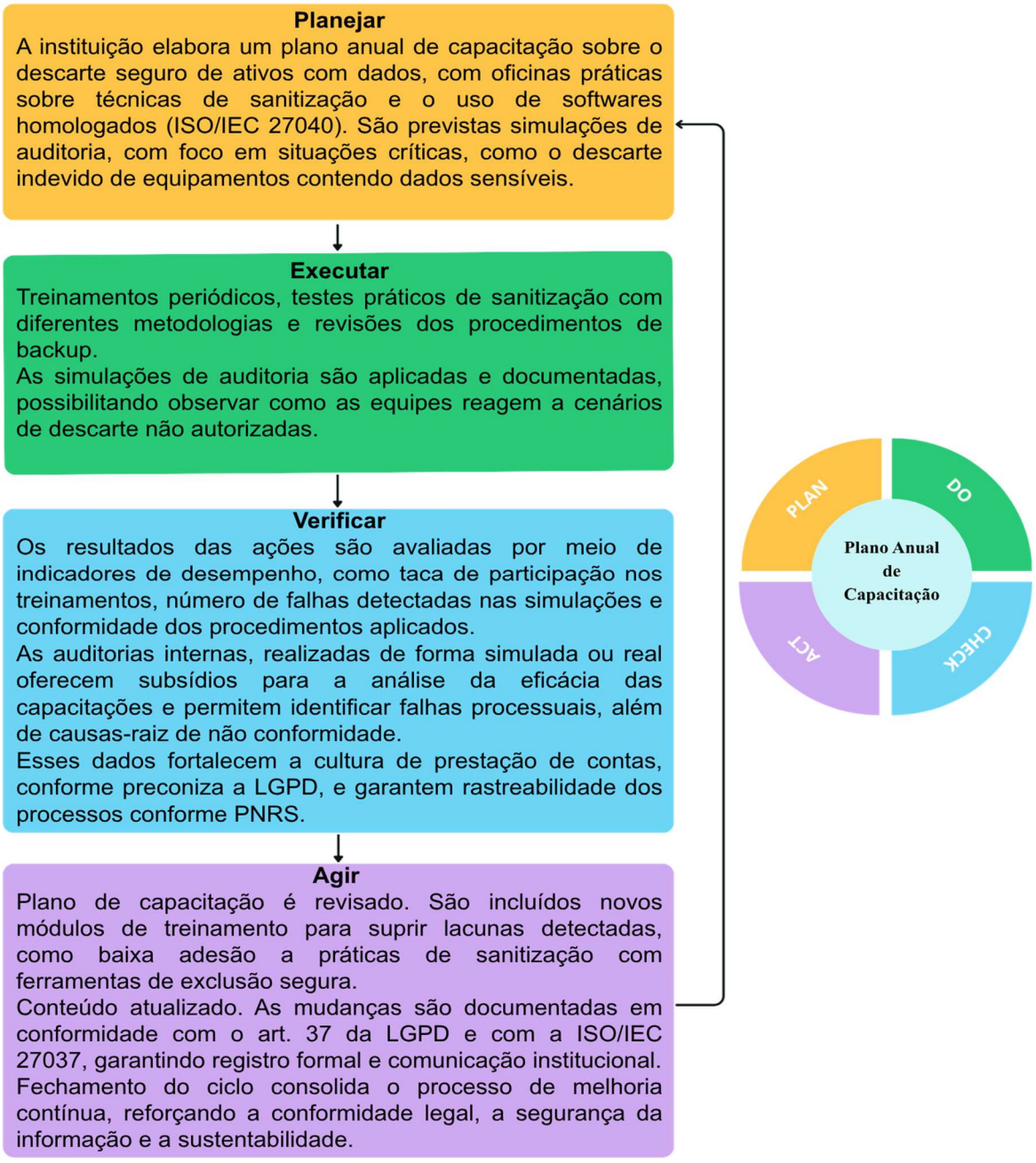
4. AGIR (ACT) - Momento de consolidar melhorias e retroalimentar o sistema.

Fluxo de ações:

1. Implementar melhorias e atualizar procedimentos – revise protocolos à luz das auditorias e resultados obtidos.
2. Comunicar mudanças – compartilhe atualizações com todas as equipes envolvidas, para evitar reincidência de falhas.
3. Registrar ações corretivas – formalize todas as mudanças e correções realizadas, mantendo rastreabilidade e conformidade documental.
4. Essa etapa fecha o ciclo e prepara o reinício do planejamento com aprendizado acumulado e melhorias incorporadas.

Diante do exposto, como exemplo de uma boa prática aplicável ao fluxograma PDCA, pode-se citar a criação de um Plano Anual de Capacitação sobre Descarte Seguro de Ativos de Dados, ilustrado na Figura 27.

Figura 27: Prática da aplicação do fluxograma PDCA – Plano anual de capacitação



Fonte: Elaboração própria, 2025.

Legenda de ações:

- **Plan: planeje oficinas, metas e simulações → base de prevenção.**
- **Do: execute treinamentos, simulados e registros → prática operacional.**
- **Check: monitore indicadores, audite e analise causas → controle e conformidade.**
- **Act: revise planos, inclua melhorias e atualize cronogramas → evolução contínua.**

CICLO PDCA – DESENVOLVIDO

Etapa Plan (Planejar)

Na etapa de planejamento, a instituição deve elaborar o Plano Anual de Gestão de Ativos de Informação, que servirá como guia para todas as ações subsequentes.

O objetivo desta etapa é consolidar uma base sólida de prevenção, definindo estratégias claras para assegurar conformidade normativa e eficiência operacional.

Etapa Do (Executar)

Na etapa de execução, o plano elaborado deve ser colocado em prática por meio de atividades periódicas e registradas.

Esta fase materializa as ações previstas, criando um ambiente organizacional que valoriza a prevenção de incidentes e fortalece a cultura de conformidade.

Etapa Check (Verificar)

A fase de verificação é dedicada ao monitoramento e avaliação dos resultados das ações executadas.

Essa etapa garante a transparência e a prestação de contas, atendendo às exigências da LGPD (accountability e segurança contínua) e da PNRS (controle e rastreabilidade dos processos).

Etapa Act (Agir)

Por fim, a etapa Act consiste em incorporar melhorias ao processo com base nos resultados obtidos.

Essa etapa fecha o ciclo, assegurando a melhoria contínua e preparando o reinício do planejamento em um nível mais elevado de maturidade.

FLUXOGRAMA PDCA

GESTÃO INTEGRADA E DOCUMENTADA DO DESCARTE DE ATIVOS DE DADOS

As modificações nos fluxos de descarte devem ser documentadas de forma clara, em conformidade com o artigo 37 da LGPD e com a ISO/IEC 27037. Essa documentação deve ser comunicada às equipes envolvidas, garantindo que o conhecimento atualizado seja disseminado e aplicado em toda a instituição.

O caráter cíclico do processo assegura o aprimoramento contínuo, fortalece a cultura de prevenção e mantém a aderência aos princípios da LGPD e aos compromissos socioambientais da PNRS.

Com base no fluxograma proposto, recomenda-se que as instituições adotem mecanismos integrados que articulem três eixos fundamentais:

- **Conformidade legal (LGPD);**
- **Segurança técnica (ISO/IEC);**
- **Responsabilidade socioambiental (PNRS).**

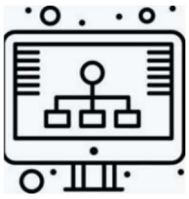
Esse modelo interdisciplinar fortalece a gestão dos dados e dos dispositivos, assegurando a proteção de direitos e promovendo a sustentabilidade institucional.

USO DE UM FLUXOGRAMA BASEADO NO PDCA AJUDA A:

- Visualizar **passo a passo as etapas do processo**;
- Facilitar o **entendimento e a execução correta por parte das equipes**;
- Destacar **pontos críticos de controle**, como backup, sanitização e destinação final;
- Integrar práticas de **melhoria contínua**, possibilitando ajustes e aprimoramentos futuros.

5

Deveres e Responsabilidades



REGISTRO DE ATIVOS

É responsabilidade da instituição manter um registro completo e detalhado de todos os dispositivos e ativos de armazenamento de dados que passam pelo processo de descarte. Esse registro deve incluir informações como:

- Tipo e identificação do dispositivo;
- Método utilizado para a destruição ou sanitização dos dados;
- Data do descarte;
- Nome do responsável pelo procedimento.

O registro garante rastreabilidade, permite auditorias futuras e assegura a conformidade com normas legais e técnicas, como a LGPD e a ISO/IEC 27037.

AUDITORIAS REGULARES

A instituição deve realizar auditorias periódicas para avaliar a conformidade dos procedimentos de descarte. Essas auditorias incluem:

- Verificação da correta execução dos métodos de destruição de dados;
- Conferência dos registros de ativos descartados;
- Identificação de possíveis falhas ou desvios nos processos.

O objetivo das auditorias é assegurar que os procedimentos estão sendo cumpridos integralmente, reforçando a segurança da informação, a responsabilidade socioambiental e a adesão às normas vigentes.

6

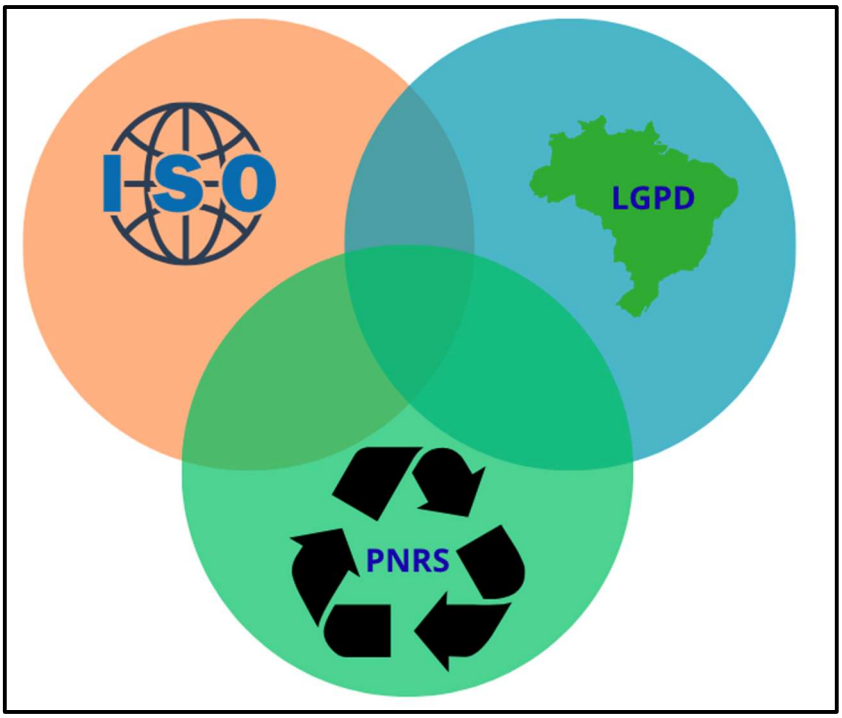
Interligação entre LGPD, PNRS e ISO

A integração entre a Lei Geral de Proteção de Dados (LGPD), a Política Nacional de Resíduos Sólidos (PNRS) e as normas da família ISO/IEC 27000 deve ser entendida como uma prática essencial de governança organizacional. Essa convergência normativa permite que a instituição:

- Promova conformidade legal e técnica de forma sinérgica;
- Evite sobreposição de atividades e desperdício de recursos;
- Reforce a transparência, prevenção, responsabilidade e melhoria contínua;
- Aumente a maturidade de seus sistemas de gestão;
- Fortaleça a reputação institucional ao integrar tecnologia, meio ambiente e governança de dados.

A Figura 28 ilustra a conexão entre proteção de dados, segurança da informação e sustentabilidade ambiental, evidenciando que essas dimensões não são isoladas, mas complementares.

Figura 28: Tríade: Integração legal, ambiental e técnica na gestão de ativos



Fonte: Elaboração própria, 2025.

7

Orientações Finais

1. DESCARTE E TRATAMENTO DE INFORMAÇÕES

No contexto do tratamento e descarte de informações, a integração normativa é especialmente relevante:

- **LGPD (Lei 13.709/2018):** obriga a eliminação segura dos dados pessoais após o término de sua finalidade.
- **ISO/IEC 27001:** define controles técnicos e operacionais para evitar vazamento de informações em mídias, documentos e equipamentos.
- **PNRS (Lei 12.305/2010):** determina critérios de destinação final ambientalmente adequada para resíduos de tecnologia e documentos.

Boa prática:

A destruição de mídias físicas ou digitais deve ocorrer por métodos certificados de sanitização ou destruição física. Em seguida, os resíduos devem ser encaminhados a empresas autorizadas em **logística reversa**, que emitam **certificados de destinação final** e mantenham registros auditáveis.

2. SEGURANÇA DA INFORMAÇÃO COMO SUPORTE

A segurança da informação, conforme a **ISO/IEC 27001**, fornece a base técnico-operacional para o cumprimento da LGPD. Entre os controles recomendados, destacam-se:

- **Autenticação multifator** e **gestão de acessos**;
- **Criptografia de dados** em repouso e em trânsito;
- **Resposta a incidentes** e registros de auditoria;
- **Sanitização de mídias** e monitoramento do ciclo de vida da informação.

Boa prática:

Essas medidas asseguram que os dados pessoais sejam tratados de forma segura até sua eliminação.

3. SUSTENTABILIDADE E RESPONSABILIDADE SOCIOAMBIENTAL

Além dos controles técnicos, recomenda-se adotar práticas sustentáveis, como:

- Digitalização de documentos para reduzir o uso de papel;
- Reutilização responsável de equipamentos de TI;
- Parcerias com fornecedores certificados em reciclagem e logística reversa.

Boa prática:

Essas ações aproximam a instituição dos objetivos da PNRS e reforçam o compromisso ético com a sociedade.

4. BENEFÍCIOS DA INTEGRAÇÃO NORMATIVA

A integração entre LGPD, ISO/IEC e PNRS traz ganhos práticos:

- **Eficiência operacional:** processos otimizados e eliminação de redundâncias;
- **Redução de riscos:** mitigação de falhas legais, ambientais e reputacionais;
- **Documentação e rastreabilidade:** registros claros e auditáveis;
- **Cultura de conformidade:** equipes alinhadas a princípios de governança, segurança e sustentabilidade.

Boa prática:

Esses ganhos asseguram maior integração entre áreas, fortalecem a governança institucional e promovem práticas alinhadas à segurança da informação, à proteção de dados e à sustentabilidade ambiental.

Orientação Final:

As instituições devem adotar **sistemas de gestão integrados**, capazes de monitorar continuamente os processos, documentar as evidências e responder de forma coordenada a incidentes. Esse modelo garante não apenas o cumprimento das exigências legais, mas também promove a sustentabilidade institucional e a confiança social.

8

Referências Bibliográficas

ALMEIDA, N. M. C. de. **Resíduos eletroeletrônicos de computadores e periféricos:** mapeamento e análise da gestão no município de Natal-RN. Orientadora: Luciana Figueiredo Lopes Lucena. 2023. 54 f. Trabalho de Conclusão de Curso (Graduação em Ciências e Tecnologia) - Escola de Ciência e Tecnologia, Universidade Federal do Rio Grande do Norte, Natal, 2023. Disponível em: https://repositorio.ufrn.br/items/1c028948-b501-4e73-9a07-16e2d489a581. Acesso em: jul. 2024.

AMARAL, A. F. F. **Redes de computadores**. Colatina: Instituto Federal do Espírito Santo, 2012. Apoio Ministério da Educação (MEC); Universidade Federal de Santa Catarina (UFSC), e-TEC Brasil. Disponível: https://proedu.rnp.br/bitstream/handle/123456789/710/Rede%20de%20Computadores_COR_CAPA_FICHA_ISBN_20120229.pdf?sequence=3. Acesso em ago. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: set. 2024.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: set. 2024.

BRASIL. Lei n. 12.305, de 2 de agosto de 2010. Institui a Política Nacional de Resíduos Sólidos; altera a Lei n. 9.605, de 12 de fevereiro de 1998; e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, ano 147, n. 147, p. 3-7, 3 ago. 2010. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12305.htm. Acesso em: set. 2024.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: set. 2024.

BRASIL. Decreto nº 9.177, de 19 de outubro de 2017. Regulamenta a Lei nº 12.305, de 2 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos. **Diário Oficial da União**: seção 1, Brasília, DF, 20 out. 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9177.htm. Acesso em: set. 2025.

BRASIL. Decreto nº 10.240, de 12 de fevereiro de 2020. Regulamenta a logística reversa de produtos eletroeletrônicos de uso doméstico e seus componentes. **Diário Oficial da União**, Brasília, DF, 13 fev. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10240.htm. Acesso em: set. 2024.

LAVOS, S. L. **Implementação de um sistema de gestão de segurança de informação (SGSI) baseado na norma ISO/IEC 27001 na EIB, SA.** 2023. 333 f. Projeto (Mestrado em Cibersegurança e Informática Forense) – Instituto Politécnico de Leiria, Escola Superior de Tecnologia e Gestão, Departamento de Engenharia Informática, Leira, 2023. Disponível em: http://hdl.handle.net/10400.8/9598. Acesso em ago. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27000:2018** – Information technology – Security techniques – Information security management systems – Overview and vocabulary. Geneva: ISO/IEC, 2018. Disponível em: https://www.iso.org/standard/73906.html. Acesso em: set. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27001:2022** – Information technology – Security techniques – Information security management systems – Requirements. Geneva: ISO/IEC, 2022. Disponível em: https://www.iso.org/standard/27001. Acesso em: set. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27002:2022** – Information technology – Security techniques – Code of practice for information security controls. Geneva: ISO/IEC, 2022. Disponível em: https://www.iso.org/standard/75652.html. Acesso em: set. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27006:2015** – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems. Geneva: ISO/IEC, 2015. Disponível em: https://www.iso.org/standard/82908.html. Acesso em: set. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27037:2012** – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO/IEC, 2012. Disponível em: https://www.iso.org/standard/44381.html. Acesso em: set. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27040:2015** – Information technology – Security techniques – Storage security. Geneva: ISO/IEC, 2015. Disponível em: https://www.iso.org/standard/80194.html. Acesso em: set. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27701:2019** – Information technology – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. Geneva: ISO/IEC, 2019. Disponível em: https://www.iso.org/standard/71670.html. Acesso em: set. 2025.

JUCON, S. **Saiba como descartar seu lixo eletrônico de forma adequada.** Eco world, [s.d.]. Disponível em: https://ecowords.com.br/saiba-descartar-seu-lixoeletronico-de-forma-adequada/. Acesso em: jun. 2025.

MAGALHÃES, P. **Requisitos e recomendações para o desenvolvimento e operação de um SGSI – Abordagem com ISO 27001/27002. Cibersegurança e Informática Forense**. Instituto Politécnico de Leiria, 2021. Disponível em: https://www.researchgate.net/publication/348663585_Requisitos_e_recomendacoes_para_o_desenvolvimento_e_operacao_de_um_SGSIbordagem_com_ISO_2700127002. Acesso em: ago. 2025.

MAGMA 3. **Presente na sua transformação digital** [Internet]. Magma 3; [s.d.] Disponível em: https://magma3.com.br/. Acesso em: jun. 2025.

MIRAGEM, B. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, São Paulo, v. 1009, nov. 2019. DTR\2019\40668. Disponível em: https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPDe-o-direito-do-consumidor.pdf. Acesso em: dez. 2024.

OLIVEIRA, V. **Norma NBR/IEC 27037:2013**. Porto Alegre, 2021. Disponível em: https://oliveiraperito.com.br/2021/07/20/norma-nbr-iso-iec-270372013/. Acesso em: set. 2024.

RODRIGUES, G.A.P. **Análise Abrangente de Vazamentos de Dados: Riscos, Conformidade e Estratégias de Prevenção**. 2024. Dissertação de mestrado profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 69 p. Disponível em: https://ppee.unb.br/wpcontent/uploads/2024/11/Dissertacao_na_versao_final-3.pdf. Acesso em: mar. 2025.

SÁ, M. D. de. **Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas:** Aplicações mobile do governo. 2019. Trabalho de Conclusão de Curso (Especialista em Informática) - Universidade Federal de Minas Gerais, Brasília, 2019. Disponível em: https://repositorio.ufmg.br/bitstream/1843/32040/1/MarceloDiasDeSa.pdf. Acesso em: fev. 2025.

TAPIA, J. A. R.; VALDÉS, S. R.; GUTIÉRREZ, C. E. E. A qualidade da informação em um sistema de gestão de segurança (ISMS) através de um software baseado no padrão ISO 27001 para instituições de educação. **RILCO DS: Revista de Desarrollo sustentable, Negocios, Emprendimiento y Educación**, v. 3, n. 26, 2021. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=8547078. Acesso em: 8 out. 2025

WEBER, F. K.; SCHMIDT, F. E. O princípio da publicidade nos atos da administração pública: uma análise sobre a LAI e a LGPD em um possível conflito de normas. Revista Foco, [S. l.], v. 16, n. 6, p. e 2295, 2023. DOI: https://doi.org/10.54751/revistafoco.v16n6-112. Publicado em: 16 jun. 2023. Acesso em: ago. 2024.

Este manual, elaborado por Márcio Giordani Ribeiro da Silva Martins no âmbito do Mestrado Profissional em Inovação e Tecnologias da Universidade Federal do Triângulo Mineiro (UFTM), apresenta procedimentos padronizados para o descarte seguro e sustentável de ativos que contenham dados. Orientado pelos Professores Doutores Geoffroy Roger Pointer Malpass e Ana Claudia Granato Malpass, o trabalho inclui fluxogramas baseados em revisão normativa e análise interdisciplinar nas áreas de Tecnologia da Informação, Gestão Ambiental e Direito. Os procedimentos foram descritos de forma generalista, permitindo sua aplicação por diferentes instituições públicas e privadas, independentemente da existência de estruturas formais para o descarte de ativos tecnológicos.