Guia de Elaboração do Processo de Gestão de Dados

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 1.0
Brasília, maio de 2024

GUIA DE ELABORAÇÃO DO PROCESSO DE GESTÃO DE DADOS

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE

Julierme Rodrigues da Silva

Coordenador-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Adriano de Andrade Moura

Bruno Pierre Rodrigues de Sousa

Leonard Keyzo Yamaoka Batista

Rafael da Silva Ribeiro

Raphael César Estevão

Rogério Vinicius Matos Rocha

Equipe Revisora

Adriano de Andrade Moura

Julierme Rodrigues da Silva
Rodrigo Duran Lima
Rogério Vinicius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
14/05/2024	1.0	Primeira versão do Guia de Elaboração do Processo de Gestão de Dados	Equipe Técnica de Elaboração

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS

O **presente Guia**, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na elaboração do Processo de Gestão de Dados, em atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve 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 dos dados que estão sob sua custódia. Adicionalmente, a Elaboração de um Processo de Gestão de Dados visa atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do *Center for Internet Security* (CIS), da *International Organization for Standardization* (ISO), do *National Institute of Standards and Technology* (NIST) e de Autoridades de Proteção de Dados. Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;
b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
c) não é coautora das publicações internacionais abordadas;

d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente guia; e

e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referências Bibliográficas” deste documento.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, à ABNT, às autoridades de proteção de dados referenciadas, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração **deste documento**.

Este Guia será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas **neste documento**.

INTRODUÇÃO

Este Guia tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a elaborar seu Processo de Gestão de Dados no âmbito institucional.

O Controle 3 do Guia do Framework de Privacidade e Segurança da Informação, estabelece que:

Controle 3: Proteção de Dados – *Utilizar processos e ferramentas para identificar, classificar, manusear, reter e descartar dados.*

O presente Guia serve como um modelo prático a ser utilizado para auxiliar na adoção de medidas do Controle 3 do Guia do Framework de Privacidade e Segurança da Informação[1] v1, e respectivas evoluções desta versão (1.1, 1.2 etc.), elaborado e publicado pela SGD. As medidas do Controle 3 que estão contempladas por este Guia são: 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13 e 3.14.

A Gestão de Dados, bem como seus respectivos responsáveis, encontra, cada vez mais, requisitos complexos e restritivos a serem cumpridos para se ter, assim, um efetivo manuseio de dados ao longo de seu ciclo de vida. Uma implementação ampla e inclusiva de um **Processo de Gestão de Dados** é necessária para aumentar a confiança de todas as partes integrantes do ciclo de vida dos dados da instituição.

Diante da pluralidade dos órgãos da Administração Pública Federal, estabelecer um modelo único para a elaboração do Processo de Gestão de Dados torna-se extremamente complexo. Desta forma, cabe aos responsáveis pela gestão de dados do órgão adaptar as orientações contidas neste documento às necessidades da sua instituição.

As orientações relativas à elaboração do **Processo de Gestão de Dados** foram estruturadas em seis seções:

- Seção 1 destaca o Processo de Gestão de Dados;
- Seção 2 trata sobre o Tratamento de Dados;

[1] <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf> Acessado em 08/04/2024

- Seção 3 trata sobre o Inventário de Dados;
- Seção 4 trata sobre a Classificação dos Dados;
- Seção 5 trata sobre Proteção de Dados;
- Seção 6 trata sobre Descarte de Dados.

1. PROCESSO DE GESTÃO DE DADOS

Dados institucionais ou organizacionais referem-se a qualquer representação, estruturada ou não, de fatos ou ideias que possam ser utilizados no intuito de obter *insights* valiosos para a tomada de decisão, otimizar processos, mitigar riscos, cumprir com requisitos legais e promover a inovação.

Existe uma série de tipos de dados que são importantes para o negócio de uma instituição e que devem ser geridos, uma vez que devem ser vistos como ativos críticos para o sucesso das atividades operacionais e administrativas do negócio, e não como meios temporários para alcançar resultados, ou mesmo como subprodutos de processos de negócio. Estes dados incluem, mas não se limitam a:

- Dados Financeiros, como dados de folha de pagamento, impostos, dados bancários, cartão de crédito etc.;
- Informações de identificação pessoal (PII) e dados de recursos humanos, incluindo números de segurança social (SSNs), informações de saúde, endereços residenciais, datas de nascimento etc.;
- Segredos comerciais, pesquisas, tecnologias patenteadas, outras formas de propriedade intelectual etc.;
- Dados usados para dar suporte a aplicativos voltados para o cliente;
- Metadados (por exemplo, tamanho do arquivo, tipo de arquivo, dados de dados, fonte);
- Informação relativa à gestão de sistemas de informação (ex. diagramas de rede).

A gestão de dados é fundamental para qualquer instituição que lida com informações. Essa prática consiste no desenvolvimento, execução e supervisão de planos, políticas, programas, processos, procedimentos, práticas e tecnologias que entregam, controlam, protegem e aumentam o valor dos ativos de dados e informações ao longo de seus ciclos de vida, garantindo assim a qualidade, segurança e integridade das informações, bem como a sua disponibilidade para análises e tomadas de decisão.

A prática da gestão de dados tem um amplo escopo, abrangendo fatores como:

- Criar, classificar, acessar e atualizar uma diversidade de dados;

- Armazenar dados de várias formas (nuvens, servidores locais etc.);
- Garantir a privacidade e a segurança de dados;
- Compartilhar dados em uma variedade de aplicativos, análises avançadas e algoritmos;
- Arquivar e descartar dados de acordo com os cronogramas de retenção e requisitos de conformidade.

Ao adotar uma abordagem eficaz de gestão de dados, os órgãos podem obter *insights* valiosos, permitindo assim a tomada de decisões baseada em dados. Desta maneira, uma estratégia formal de gestão de dados auxiliará o órgão a obter valor de seus dados.

O Processo de Gestão de Dados refere-se especificamente à sequência de etapas ou atividades bem definidas e organizadas que uma instituição segue para gerenciar seus dados de maneira sistemática e consistente. Este processo pode incluir, a depender da abordagem adotada ou das necessidades específicas da instituição, a identificação de fontes ou levantamento (inventário) de dados, bem como, a classificação, a proteção e o descarte de dados. Além disso, o processo de gestão de dados pode incluir outras etapas, tais como: padronização de formatos, estabelecimento de políticas de uso de dados, implementação de tecnologias de gestão, monitoramento da qualidade e revisão contínua das práticas de gestão de dados para melhoria contínua.

No cenário atual, não é uma tarefa difícil certificar-se de que os dados institucionais não se limitam a estarem apenas dentro da estrutura institucional. São diversos os exemplos de dados custodiados na nuvem, em dispositivos portáteis do usuário final, compartilhados com parceiros ou com serviços on-line em qualquer lugar do mundo.

A proteção de dados tem recebido cada vez mais destaque no cenário global e as instituições estão aprendendo que o respeito à gestão e o uso apropriados de dados são fundamentais, não se restringindo apenas ao simples controle criptográfico. Os dados devem ser geridos de maneira adequada em todo o seu ciclo de vida incorporando as melhores práticas de proteção de dados.

Nas próximas seções deste documento, serão discutidas as etapas do processo de gestão indispensáveis à proteção de dados.

2. TRATAMENTO DE DADOS

O termo "tratamento de dados", considerando-se a definição de dados em seu sentido amplo no contexto institucional, refere-se ao conjunto de operações realizadas sobre os dados ao longo do seu ciclo de vida, tais como a coleta inicial ou produção de dados, seu processamento, análise, interpretação, comunicação e, eventual, descarte final destes dados. No Brasil, restringindo-se ao escopo de dados pessoais, a Lei Geral de Proteção de Dados Pessoais, (LGPD, Lei n° 13.709/2018), que dispõe sobre o tratamento de dados pessoais por pessoa natural ou jurídica de direito público ou privado, define o termo "tratamento" em seu art. 5º, inciso X.

> *"Art. 5º...*
>
> *X - tratamento: 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;*
>
> *...".*

Apesar da abrangência da LGPD no cenário atual do país, regulamentando o tratamento do específico conjunto de dados pessoais, existe uma gama de dados tratados pelas instituições, tais como dados fiscais, financeiros e segredos comerciais e industriais, que vão além do escopo delimitado pelos dados pessoais e que são regulamentados por diversos normativos vigentes coexistentes à LGPD. São exemplos destes normativos, a Lei de Acesso à Informação, LAI (Lei nº 12.527 de 18 de novembro de 2011), que dispõe sobre os procedimentos a serem observados no acesso a informações mantidas sob custódia da administração pública, a Lei de Sigilo Fiscal (Lei 5.172, de 25 de outubro de 1966), que dispõe sobre o sistema tributário nacional e institui normas gerais de direito tributário, e portarias da Receita Federal e do Ministério da Fazenda, a Lei nº 10.180, de 6 de fevereiro de 2001, que organiza e disciplina os sistemas de controle interno, a Lei de Propriedade Intelectual de Software (Lei nº 9.609, de 19 de fevereiro de 1998) e a Lei de Segredo Industrial (Lei nº 9.279, de 14 de maio de 1996).

Portanto, é importante que as instituições observem os normativos vigentes e adotem as melhores práticas de gestão de dados, de privacidade e de segurança da informação ao lidar com qualquer tipo de dado, seja ele pessoal ou não. Isso inclui a

implementação de controles de privacidade e segurança da informação adequados, além de implementar políticas de gestão de dados a fim de garantir que os dados sejam coletados, armazenados, utilizados e eliminados de maneira ética e segura, obedecendo sempre a legislação vigente.

3. INVENTÁRIO DE DADOS

Um inventário de dados consiste num documento primordial que registra todas as informações básicas sobre um conjunto de dados mantido e gerenciado por uma instituição. Dentre essas informações registradas em um inventário, pode-se destacar, como exemplo, o curador deste conjunto de dados, quais as categorias dos dados e onde estão localizados, bem como o fluxo e a frequência de atualização destes dados e o formato dos arquivos armazenados neste conjunto de dados, entre outros detalhes relevantes para instituição[2,3]. Esses detalhes sobre um conjunto de dados são conhecidos como “metadados”.

Os metadados são informações sobre dados. Um conjunto completo de metadados descreve todos os aspectos dos dados em questão, incluindo quem, o quê, onde, quando, como e por que de um conjunto de dados, juntamente com qualquer tratamento que tenha ocorrido. Os metadados são considerados um componente essencial de qualquer bom conjunto de dados[4]. A gestão eficaz dos metadados é essencial para garantir a qualidade dos dados, melhorar a governança e permitir a tomada de decisões baseada em dados.

Existem diversas razões pelas quais um inventário de dados é considerado um ativo fundamental para uma instituição[5], esses benefícios variam de acordo com as necessidades e desafios específicos de cada instituição. São exemplos desses benefícios:

- **Colaboração da equipe**: Quando a equipe precisa de informações de outro departamento, eles usam o inventário para saber o que existe e a quem solicitá-las. Isso permite a colaboração em relatórios e projetos analíticos.
- **Segurança**: criar e gerenciar um inventário de dados reduz riscos e incertezas criando uma lista de verificação para requisitos de segurança, proteção de dados e conformidade legal. Em alguns casos, o inventário pode chamar a atenção para dados que a instituição não deveria mais manter.
- **Abertura de dados ao público**: Ter um inventário completo também é importante para determinar quais conjuntos de dados serão divulgados

[2] Johns Hopkins University
[3] https://atlan.com/data-inventory-vs-data-catalog/
[4] U.S. National Park Service’s Data Management Guidelines for Inventory and Monitoring Networks
[5] Johns Hopkins University

publicamente. O inventário de dados pode ser usado para priorizar a liberação de dados.

- **Qualidade dos dados**: Um inventário de dados auxilia aos proprietários dos dados na avaliação da qualidade dos seus dados, trazendo as classificações de qualidade para um local central onde a instituição pode priorizar esforços para melhorar a qualidade dos dados.
- **Gerenciamento de desempenho**: os conjuntos de dados no inventário podem conter pontos de dados individuais que podem servir como métricas para gerenciamento de desempenho. Ter os conjuntos de dados listados de forma organizada facilita as conversas sobre a seleção de métricas.
- **Identificação de dados ausentes**: Com uma visão completa dos dados existentes, uma instituição pode identificar quais dados não existem, mas que seriam úteis para tarefas específicas.
- **Centralização e coordenação**: Um inventário é o primeiro passo para considerar soluções para gerenciamento e armazenamento de dados.

Além disso, um inventário pode ser útil no cumprimento de diversos requisitos legais e na priorização do trabalho em vários projetos de dados.

A seguir, um exemplo de alguns itens que podem constar em um inventário de dados:

- **Identificador** – pode ser um nome de arquivo ou outro identificador exclusivo.
- **Tipo de dados** – financeiro, fiscais, dados pessoais ou outro tipo de dados.
- **Proprietário ou curador dos dados** – indivíduo ou unidade de negócios responsável pelos dados.
- **Classificação/rótulo de dados** – as instituições devem, no mínimo, capturar a sensibilidade dos dados usando categorias sensíveis ou não sensíveis. Se forem capazes, as instituições podem classificar ainda mais os dados usando a área temática (por exemplo, dados pessoais).
- **Localização dos dados** – onde os dados são armazenados.
- **Retenção de dados** – prazo necessário para retenção de dados para requisitos legais, regulatórios ou comerciais.

- **Fluxo de dados** – uma descrição ou representação visual de, no mínimo, como os dados fluem para fora da organização.

Com o objetivo de agilizar e simplificar a pesquisa e descoberta dos dados mais relevantes em uma instituição, é vantajoso adotar um catálogo de dados. Esse recurso consolida de forma organizada e centralizada todas as informações sobre as bases de dados sob a custódia da instituição, possibilitando às partes interessadas localizarem e compreenderem, de forma rápida e facilitada, os dados necessários e apropriados para qualquer finalidade analítica, a partir de sua descrição e caracterização técnica e negocial.

A Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), por meio da Diretoria de Infraestrutura de Dados (DEDAD), lidera uma iniciativa conhecida como Catálogo de Base de Dados (CBD).

O CBD[6] consiste em uma base centralizada de informações a respeito de bases de dados custodiadas pela administração pública federal e tem o objetivo de classificar, organizar e disponibilizar, de maneira simples e em canais centralizados e descentralizados, informações (descrições e características) sobre os ativos de dados da administração pública federal por meio de metadados.

Dessa forma, é possível encontrar rapidamente informações, acessar os metadados e iniciar a preparação e análise dos dados com eficiência, além de qualificar e agilizar a análise das informações institucionais de grande diversidade de bases de dados. Isso porque transforma detalhes técnicos em ativos negociais significativos e de fácil localização.

É de extrema relevância que as instituições públicas estejam alinhadas a iniciativa do CBD a fim de que as informações sobre os dados em posse do governo se tornem úteis para todos.

3.1. INVENTÁRIO DE DADOS PESSOAIS

O Inventário de Dados Pessoais – IDP, definido na LGPD em seu art. 37, consiste no registro das operações de tratamento dos dados pessoais realizados pelo órgão. Ele proporciona uma espécie de "fotografia" do atual cenário do tratamento de dados pessoais do serviço/processo de negócio.

[6] https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/catalogo-de-bases-de-dados

De uma forma geral, esse registro mantido pelo IDP envolve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão como:

- atores envolvidos (agentes de tratamento e o encarregado);
- finalidade (o que a instituição faz com o dado pessoal);
- hipótese (arts. 7º e 11 da LGPD);
- previsão legal;
- dados pessoais tratados pela instituição;
- categoria dos titulares dos dados pessoais;
- tempo de retenção dos dados pessoais;
- instituições com as quais os dados pessoais são compartilhados;
- transferência internacional de dados (art. 33 LGPD); e
- medidas de segurança atualmente adotadas.

É importante deixar documentado todo o fluxo de dados para que o titular tenha pleno conhecimento das finalidades, quais dados estão sendo tratados e a fase que o órgão atua.

Além de representar um documento importante no processo de gestão de dados pessoais, o IDP serve de subsídio para a avaliação de impacto à proteção de dados pessoais com vistas a verificar a conformidade do órgão no que se refere ao preconizado pela LGPD.

Fique Atento!
A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Inventário de Dados Pessoais, que incentiva a adoção de registros das operações de tratamento de dados pessoais e suas respectivas avaliações, sob a ótica dos princípios da LGPD e contém importantes instruções para que os órgãos e seus colaboradores possam elaborar um inventário de dados pessoais.
Disponível em: Guia de Elaboração de Inventário de Dados Pessoais

4. CLASSIFICAÇÃO DE DADOS

Conforme ABNT NBR 16167:2020, a classificação de dados pode ser definida como: a ação de definir o nível de relevância do dado, a fim de assegurar que o dado receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a organização. Dessa forma, durante a classificação de dados, recomenda-se que sejam considerados o valor do dado, os requisitos legais, a sensibilidade, a criticidade, o ciclo de vida e o prazo de retenção do dado, a necessidade de compartilhamento e restrição, a análise de riscos e os impactos para o negócio.

No decorrer do processo de classificação, é recomendado que todos os dados recebam um rótulo de classificação com base no nível de impacto para com o órgão. O rótulo deve seguir com o dado durante todo o tratamento, da coleta até o seu, eventual, descarte.

Pode ocorrer o processo de reclassificação do dado, nos casos de:

- identificação de um dado incorretamente classificado;
- mudanças no contexto de valor dos dados;
- atendimentos de requisitos legais;
- mudanças em processos internos do órgão;
- vencimento do prazo de temporalidade da classificação de um determinado dado ou se for atingido o fim do tratamento do dado.

Os esquemas de classificação, assim como os rótulos recebidos pelos dados, podem ser propostos de várias maneiras, não existindo uma ideia mais correta que outra, tudo irá depender da realidade e necessidade do órgão no tratamento dos dados. Vale ressaltar que a criação de esquemas de classificação muito complexos, utilizando diversos níveis, poderá engessar o processo e o fluxo de tratamento do dado, por meio da aplicação de controles desnecessários. Em contrapartida, poucos níveis podem gerar uma falsa sensação de segurança, devido ao relaxamento na classificação ou mesmo à perda de recursos por gestão além do necessário.

É importante ressaltar que devem ser observadas, no decorrer do processo de elaboração de um esquema de classificação de dados, legislações que dispõem sobre restrição de acesso, sobretudo as disposições previstas na Lei nº 12.527, de 18 de novembro

de 2011 (Lei de Acesso à Informação - LAI), e no Decreto nº 7.724, de 16 de maio de 2012, bem como orientações ou normas complementares editadas por órgãos competentes.

No âmbito federal, encontra-se a Norma Complementar nº 20/IN01/DSIC/GSIPR, publicada pelo Gabinete de Segurança Institucional da Presidência da República – GSIPR. Nesta Norma Complementar, em seu Anexo A, é apresentado um quadro exemplificativo contendo os seguintes tipos de informação:

- **Ostensiva**, descrita como transparência ativa ou passiva;
- **Sigilosa (classificada em grau de sigilo)**, descrita como reservada, secreta ou ultrassecreta;
- **Sigilosa Protegida por Legislação Específica**,
  - decorrentes de direitos de personalidade (sigilo fiscal, bancário, comercial, empresarial e bancário);
  - decorrentes de procedimento administrativo disciplinar em curso (sigilo de inquérito policial, segredo de justiça em processo civil ou penal); e
  - decorrentes de informação de natureza patrimonial (segredo industrial, direito autoral e propriedade intelectual e industrial); e
- **Pessoal**, prevista no art. 31da LAI e LGPD.

Neste sentido, uma proposta **exemplificativa** de esquema de classificação de dados conteria os seguintes níveis de classificação:[7]

- **Pública**, com acesso irrestrito e visível a todos os usuários, inclusive pelo público externo;
- **Restrita**, quando se tratar de informação sigilosa não classificada em grau de sigilo, protegidas por demais hipóteses legais de restrição de acesso; e
- **Sigilosa classificada em grau de sigilo**, nos termos do art. 23 da Lei nº 12.527/2011, subdividida nos graus **ultrassecreto**, **secreto** ou **reservado**.

Observação: O esquema de classificação apresentado anteriormente tem caráter meramente EXEMPLIFICATIVO! Cabe ao órgão considerar, como base, a realidade própria do negócio institucional na elaboração de seu esquema de classificação.

[7] <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acessado em 08/04/2024

5. PROTEÇÃO DE DADOS

Esta etapa do processo de gestão de dados tem por objetivo observar os princípios da privacidade (desvinculação, transparência e intervenção)[8] e da segurança da informação (confidencialidade, integridade e disponibilidade) durante o ciclo de vida do tratamento dos dados aos quais o órgão tem acesso. É importante que o órgão garanta que os dados estejam protegidos por meio de controles e medidas apropriadas, e que elas sejam determinadas de acordo com a sensibilidade dos dados, requisitos legais, regulatórios e de negócios.

Existe uma gama extraordinária de *frameworks* (compostos, geralmente, por normas e guias) sobre privacidade e segurança da informação utilizados globalmente por instituições no intuito de estabelecer práticas robustas na proteção de dados importantes e sensíveis dentro de contextos institucionais. As diretrizes e orientações contidas nestes documentos variam desde os mais abrangentes, com controles e medidas aplicáveis em qualquer negócio, até os mais específicos, que consideram detalhes de normas vigentes em um determinado país, cada um com seu foco, dependendo do tipo de dado e da área de aplicação, ambos os casos necessitam de uma adaptação para a realidade de quem os adota. Além de proteger dados institucionais, a adoção destes *frameworks* auxilia no cumprimento com regulamentações legais.

Alguns dos principais frameworks de boas práticas em proteção de dados, são:

- Normas ABNT NBR (16167);
- ISO/IEC 27000 *family standards (27001, 27002, 27701 etc.);*
- CIS *Critical Security Controls* v8[9];
- NIST *Cybersecurity Framework* (CSF);
- ISO/IEC 29000 *family standards (29100, 29134, 29151, 29184 etc.);*
- CIS *Controls Privacy Guide*[10];
- NIST *Privacy Framework.*

[8] https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_privacidade_concepcao.pdf
[9] https://www.cisecurity.org/controls
[10] https://www.cisecurity.org/insights/white-papers/cis-controls-v8-privacy-companion-guide

No âmbito da Administração Pública Federal, algumas das principais normas de conformidade legal são:

- LAI – Lei de Acesso à Informação (Lei 12.527/2011);
- LGPD – Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018);
- Publicações da ANPD (Autoridade Nacional de Proteção de Dados)[11];
- Normativos do GSI/PR (Gabinete de Segurança Institucional da Presidência da República)[12];
- Política Nacional de Segurança da Informação (PNSI)[13].

Além disso, o Guia do Framework de Privacidade e Segurança da Informação, elaborado pela Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos, consolida diversas obrigações, diretrizes e recomendações contidas nestas normas e boas práticas com o objetivo de fomentar a privacidade e a segurança da informação nas instituições públicas. Essa consolidação surge no sentido de auxiliar na identificação, no acompanhamento e no preenchimento das lacunas de privacidade e segurança da informação para se alcançar a conformidade legal relacionada ao tema.

Durante todas as fases do ciclo de vida do tratamento de dados, é essencial seguir diretrizes específicas para assegurar a proteção dos dados. Dentre essas fases, pode-se destacar, como exemplo, a coleta, a retenção (armazenamento), o processamento e o compartilhamento de dados. A seguir, algumas diretrizes exemplificativas são destacadas em cada uma dessas fases.

5.1. COLETA DE DADOS

A coleta de dados é um processo de reunir dados de diversas fontes que servirão de insumos para planejar estratégias e agregar valor ao negócio da organização por meio de análises, pesquisas ou tomada de decisões. Estes dados podem ser gerados por pessoas, processos ou sistemas. A coleta pode ser realizada por meio de várias técnicas, incluindo:

- **Questionários e Pesquisas**: ferramentas comuns para coletar informações diretamente de pessoas, seja em formato digital ou papel;

[11] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes
[12] https://www.gov.br/gsi/pt-br/ssic/legislacao
[13] https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm

- **Observações**: notando e registrando comportamentos ou eventos em situações controladas ou naturais;
- **Entrevistas**: conversas estruturadas ou semiestruturadas para obter informações detalhadas de participantes;
- **Sensores e dispositivos eletrônicos**: uso de tecnologias para coletar dados automaticamente, como sensores meteorológicos ou dispositivos de rastreamento de atividades;
- **Registros administrativos e dados históricos**: aproveitamento de dados já existentes armazenados por organizações ou governos.

É crucial que este processo seja realizado de forma ética e em conformidade com as normas legais vigentes, a depender do tipo e nível de classificação dos dados. Um exemplo é a coleta de dados pessoais que deve observar as determinações específicas estabelecidas pela LGPD e as diretrizes constantes nas publicações da ANPD. A anonimização e pseudonimização são princípios de privacidade e proteção de dados que podem ser adotados na coleta de dados pessoais, por exemplo, bem como a implementação de criptografia na fonte com o objetivo de resguardar o princípio da confidencialidade e integridade dos dados na segurança da informação.

A ANPD, por exemplo, em seu Guia Orientativo sobre Cookies e Proteção de Dados Pessoais, apresenta diretrizes que auxiliam o órgão na coleta e classificação de cookies de acordo com os princípios estabelecidos pela LGPD.

5.2. RETENÇÃO DE DADOS

A retenção de dados refere-se à prática de armazenamento de dados por um determinado período. As organizações fazem isso por diversas razões, incluindo conformidade com requisitos legais, necessidades de auditoria, operações de negócios e para análise futura, entre outros. Por isso, a unidade responsável deve desenvolver e manter um plano ou política de retenção de dados que defina como e por quanto tempo os dados devam ser mantidos antes de serem eliminados ou arquivados.

Todos os dados e documentos devem ser preservados pelo período apropriado, conforme determinado pelos requisitos legais, tais como a LAI, LGPD e demais regulamentos que versarem sobre o assunto, bem como as normas de boas práticas.

É importante ressaltar que, quando se trata da retenção de dados em geral, os órgãos devem observar, ao menos, os prazos mínimos e máximos estipulados para retenção, bem como organizar o armazenamento dos dados de forma segmentada, levando em consideração a sensibilidade dos dados.

Quando se tratar de dados pessoais, deve-se ter um cuidado especial durante sua retenção, tais cuidados podem ser identificados na LGPD, regulamentos expedidos pela ANPD (Autoridade Nacional de Proteção de Dados) e em normas específicas de boas práticas, tais como ABNT, ISO/IEC, NIST e CIS, desde que as orientações não sejam contrárias ao que se estabelece na LGPD e em publicações da ANPD. Alguns exemplos de diretrizes incluem, mas não se limitam a:

- reter dados pessoais apenas pelo período autorizado para cumprir a(s) finalidade(s) identificada(s) ou conforme exigido pela lei e excluir os dados pessoais imediatamente quando o período de retenção expirar;
- quando for necessário reter dados pessoais por mais tempo do que o necessário para fins específicos, implementar medidas como a desidentificação para proteger os dados pessoais;
- definir períodos de retenção de dados pessoais limitados no tempo e adequados à finalidade do processamento;
- confirmar se o sistema de informação consegue detectar a expiração do período de retenção;
- desenvolver uma funcionalidade automatizada que exclua dados pessoais quando seu período de retenção expirar. Esta exclusão deverá ocorrer imediatamente ou assim que possível;
- escolher ferramentas (incluindo exclusão parcial, *hashing*, *hashing* de chave e índice) necessárias para a proteção de dados pessoais se esses dados não puderem ser desidentificados.

É importante que os dados sejam armazenados em locais seguros, com controles de acesso e registros passíveis de identificação.

5.3. PROCESSAMENTO DE DADOS

O processamento de dados refere-se ao conjunto de operações, por meio de procedimentos manuais ou automatizados, para transformar dados brutos em informações úteis e significativas que possam ser utilizadas no intuito de obter insights valiosos para a tomada de decisão, de otimizar processos, de mitigar riscos, de cumprir com requisitos legais e de promover a inovação dentro de uma organização.

Etapas típicas no processamento de dados incluem:

- **Validação**: garantir que os dados coletados sejam precisos e relevantes para o contexto em que serão usados;
- **Limpeza**: remover ou corrigir dados que estejam incompletos, incorretos ou irrelevantes, para melhorar a qualidade dos dados;
- **Organização**: estruturar os dados de forma a facilitar a análise e o processamento subsequente, como classificá-los em tabelas, bancos de dados ou outros formatos organizados;
- **Transformação**: modificar os dados para adequá-los a requisitos ou formatos específicos necessários para análises adicionais ou integração com outros sistemas;
- **Armazenamento**: guardar os dados transformados em sistemas, garantindo que sejam acessíveis e seguros;
- **Recuperação**: obter os dados armazenados conforme necessário para análises ou relatórios futuros;
- **Análise**: aplicar técnicas estatísticas e matemáticas para interpretar os dados e extrair padrões ou insights;
- **Relatórios e Visualização**: apresentar os dados processados de maneira compreensível, usando gráficos, tabelas ou relatórios que facilitam a tomada de decisão.

Conforme o tipo e a classificação dos dados, se faz necessário observar normas legais de conformidade específicas durante o processamento. Exemplo disso, são os processamentos realizados sobre dados pessoais que devem observar uma série de diretrizes específicas estabelecidas pela LGPD e em publicações pela ANPD. Além dos

normativos legais nacionais, existem diversas diretrizes constantes em normas de boas práticas, a exemplo da ISO/IEC, CIS e NIST, que orientam sobre o processamento seguro e ético dos dados. Realizar, por exemplo, o processamento de dados de maneira segmentada com base na sensibilidade é uma das melhores práticas adotadas globalmente pelas instituições com níveis de maturidade consideráveis (almejados). Tal segmentação se faz necessária para que não se processe dados sensíveis em ativos institucionais destinados a dados de menor sensibilidade.

5.4. COMPARTILHAMENTO E TRANSFERÊNCIA DE DADOS

O compartilhamento de dados refere-se ao processo pelo qual os dados são disponibilizados, transmitidos, distribuídos, comunicados ou difundidos entre diferentes instituições, sistemas ou indivíduos em atendimento a alguma finalidade, incluindo colaboração em pesquisa, melhorias nos serviços, integração de sistemas ou até mesmo para fins de conformidade regulatória. O compartilhamento promove a melhoria da eficiência dentro e entre as instituições.

Este processo deve envolver tecnologias, boas práticas e estruturas legais que facilitem o acesso seguro aos dados pelas partes, sem comprometer a privacidade dos indivíduos e segurança dos dados.

No âmbito da administração pública, a depender do tipo dos dados tratados e seu nível de classificação, normas legais específicas de conformidade devem ser observadas durante a realização do compartilhamento de dados entre órgãos públicos e entre o setor público e privado. Um exemplo é o compartilhamento de dados pessoais, que deverá observar principalmente, as disposições contidas no Decreto nº 10.046, de 9 de outubro de 2019 e disposições estabelecidas pela LGPD e em publicações da ANPD, além de outras normas regulamentares que versarem sobre o assunto.

Para orientar as entidades e os órgãos públicos, são abordados pela ANPD, no seu Guia orientativo de Tratamento de Dados Pessoais pelo Poder Público, os principais requisitos a serem considerados nos procedimentos de compartilhamento de dados pessoais pelo Poder Público. É relevante destacar que esses requisitos representam diretrizes gerais, derivadas da LGPD, e podem ser adaptados ou complementados conforme o contexto e as particularidades de cada situação específica.

A transferência internacional de dados, principalmente os pessoais, está sujeita a regulamentações específicas, por isso, o órgão deve documentar a conformidade com estes requisitos, como exemplo, a base legal para transferência.

Também é necessário identificar os países e organizações internacionais para os quais os dados possam ser transferidos, pois essas informações devem estar disponíveis e de acordo com as regulamentações nacionais, principalmente quando se tratar de dados pessoais. Além disso, as identidades de países que estejam em subcontratos também devem ser incluídas.

Fique Atento!
A Autoridade Nacional de Proteção de Dados (ANPD) traz em sua página uma série de publicações relacionadas a Proteção de Dados pessoais, é relevante que o Órgão ou Entidade ao se deparar com essa temática, avalie os documentos publicados por eles.
Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes

As práticas seguras de compartilhamento de dados geralmente incluem medidas como:

- **Acordos de confidencialidade**: para garantir que as partes envolvidas mantenham a confidencialidade das informações compartilhadas;
- **Protocolos de segurança**: proteção de dados durante o transporte e armazenamento, como criptografia e uso de redes seguras;
- **Controle de acesso**: limitar o acesso aos dados apenas aos usuários autorizados que necessitam dessas informações para suas funções;
- **Auditoria**: rastrear quem acessou os dados e o que foi feito com eles.

Além disso, o compartilhamento de dados deve ser monitorado por meio de ferramentas de proteção específicas, com recursos para identificar e bloquear o tráfego de dados que esteja em desacordo com as normas da organização e com as leis anteriormente mencionadas. Os dados que forem classificados com níveis mais altos de sensibilidade, somente devem ser transmitidos ou transportados mediante recursos de segurança que garantam a sua proteção e rastreabilidade.

Em conclusão à etapa de Proteção de Dados, seguem alguns exemplos das principais medidas de que devem ser adotadas, minimamente, pelo órgão durante as diversas fases do ciclo de vida do tratamento de dados:

- Configuração de listas de controle de acessos a dados e registro dos acessos aos dados sensíveis:
  - As permissões de acessos podem ser baseadas em diversas características tais como, em identidade, em criticidade dos dados, na necessidade de conhecimento do usuário e em papéis desempenhados ou em perfis institucionais. As configurações de listas de controle de acessos devem abranger sistemas de arquivos, banco de dados e aplicações locais e remotas;
  - Os registros de acessos aos dados sensíveis devem incluir, principalmente, o autor de modificações e exclusão destes dados;
- Criptografia de dados em dispositivos de usuário final e mídias removíveis:
  - A maioria dos sistemas operacionais contém aplicações nativas para criptografar dados armazenados nos discos dos dispositivos de usuário final e em mídias removíveis;
- Criptografia de dados sensíveis em repouso e em trânsito:
  - A criptografia de dados em repouso pode incluir servidores, aplicações e bancos de dados que contenham dados sensíveis.
  - Exemplos de implementações para criptografia de dados sensíveis em trânsito podem incluir os seguintes protocolos: *Transport Layer Security (TLS)* e *Open Secure Shell (OpenSSH)*; e
- Implantação de solução de prevenção contra perda de dados:
  - As ferramentas de prevenção de perda de dados podem se classificar em:
    - Baseada em *host:* monitoram a atividade em laptops, servidores, dispositivos móveis e outros dispositivos que acessam a rede;
    - Baseada em rede: concentra-se em como os dados se movimentam, entram e saem de uma rede; e

- Baseada em nuvem: concentra-se nos dados armazenados e acessados pelos serviços de nuvem.

6. DESCARTE DE DADOS

A etapa de descarte de dados refere-se ao processo de eliminação segura e irreversível de dados confidenciais e sensíveis necessários ao negócio de uma organização. Estes dados podem estar armazenados em dispositivos eletrônicos como computadores, servidores, discos rígidos, unidades USB, mídias digitais, como CD's e DVD's, e outros meios de armazenamento. Esse processo é essencial para manter a confidencialidade dos dados e a privacidade dos indivíduos, evitando que dados sensíveis ou confidenciais sejam acessados por pessoas não autorizadas após o término de seu uso legítimo.

Existem diversos documentos contendo boas práticas para a execução do processo de descarte seguro de dados. Alguns exemplos dessas boas práticas, são:

- ABNT NBR 16167:2020;
- ISO/IEC 27000 *family standards (27001, 27002, 27018, 27701 etc.);*
- CIS *Critical Security Controls*;
- NIST *Cybersecurity Framework* (CSF).

O descarte de dados reduz o uso dos recursos de armazenamento e manutenção de dados (armazenamento físico ou em nuvem, tempo da equipe para manter os dados de forma adequada) e mitiga o impacto de um incidente de violação de dados, uma vez que uma quantidade menor de dados estará disponível nos ativos da organização.

O método de descarte deve ser adequado ao grau de sensibilidade dos dados, de maneira que aqueles que forem classificados como altamente sensíveis ou com severas restrições de acesso sejam destruídos de forma a torná-las completamente irreversíveis.

O órgão deve proporcionar aos colaboradores capacitação e conscientização sobre os procedimentos de descarte de dados. Além disso, deve-se garantir que todos os colaboradores estejam devidamente informados sobre os procedimentos de descarte de dados. Isto deve ser conseguido por meio da manutenção da documentação a respeito dos procedimentos no descarte de dados, disponibilizando-a aos colaboradores e garantindo que estes saibam onde encontrá-la.

A variedade de meios de armazenamento de dados utilizados por um órgão exigirá diferentes métodos de descarte. Alguns fatores devem ser considerados ao escolher uma técnica de descarte, a natureza e a abrangência do dado a ser descartado, se existe ou não

um metadado associado ao dado, se o dado é pessoal e as características físicas da mídia na qual o dado é armazenado. Abaixo podemos citar alguns meios de armazenamento e formas de destruição de dados trazidas pelo *Center for Internet Security* (CIS)[14]:

- Relatórios, correspondência e outros meios de comunicação impressos:
    1. Trituração;
    2. Incineração ou queima;
    3. Corte em tiras;
    4. Perfuração;
    5. Pulverização;
    6. Reciclagem; entre outros.
- Mídias portáteis (por exemplo, unidades de estado sólido (SSDs), discos de vídeo digital (DVDs), dispositivos de armazenamento de dados de barramento serial universal (USB):
    1. Destruição Física:
        a. Trituração;
        b. Desmontagem
- Unidades de disco rígido (HDDs) e outras mídias magnéticas, incluindo unidades de disco rígido de impressoras e copiadoras:
    1. Sobrescrever;
    2. Destruição Física:
        a. Esmagamento;
        b. Desmontagem; e
        c. Desmagnetização.
- Cartuchos de fita:
    1. Destruição Física:
        a. Trituração;
        b. Esmagamento;
        c. Desmagnetização.

[14] https://www.cisecurity.org/insights/white-papers/data-management-policy-template-for-cis-control-3

Sempre que possível, o órgão deve garantir que os contratos com prestadores de serviços terceirizados incluam cláusulas para descarte de todos os dados a pedido do órgão. Caso seja usado um fornecedor terceirizado de descarte, deve-se adotar os padrões de proteção adequados para a destruição, de acordo com o nível de classificação do dado e registros de garantia de que os serviços foram realizados.

A ação de descarte de dados deverá ser registrada, para que se mantenha a rastreabilidade dessa atividade.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2013: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação - Requisitos**. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2013: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27701:2019: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes**. Rio de Janeiro, 2019.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS - ANPD. **Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público. Junho de 2023.** Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf >. Acesso em: 08 mar. 2023.

BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 05 de março de 2023.

BRASIL. Presidência da República. **Decreto n° 10.046, de 09 de outubro de 2019. Compartilhamento de Dados na Administração Pública Federal**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm >. Acesso em: 05 de março de 2023.

BRASIL. Presidência da República. **Gabinete de Segurança Institucional. Portaria nº 93, de 18 de outubro de 2021**. Glossário de Segurança da Informação. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370 >. Acesso em: 07 de março de 2023.

BRASIL. Presidência da República. **Secretaria de Segurança da Informação e Cibernética. Departamento de Segurança da Informação e Cibernética. Gabinete de Segurança Institucional**. Legislação< https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/legislacao > Acesso em 06 março 2023.

BRASIL. Presidência da República. **Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa nº 01, de 27 de maio de 2020**. Brasília, DF, GSI/PR, 2020. Disponível em: < http://dsic.planalto.gov.br/assuntos/editoria-c/documentos-pdf-1/instrucao-normativa-no-1-de-27-de-maio-de-2020-1.pdf >. Acesso em: 13 de março 2023.

CENTER INTERNET SECURITY. **CIS Controls, versão de 8 maio de 2021**. Disponível em: < https://learn.cisecurity.org/control-download >. Acesso em: 01 de março de 2023.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia de Inventário de Dados Pessoais**. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf >. Acesso em: 25 mar. 2023.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação**. Novembro 2022. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em: 01 mar. 2023.