GOVERNANÇA DE DADOS NO SETOR PÚBLICO

DADOS ABERTOS,
PROTEÇÃO DE DADOS PESSOAIS
E SEGURANÇA DA INFORMAÇÃO
PARA UMA TRANSFORMAÇÃO
DIGITAL SUSTENTÁVEL

AUTORES
Luca Belli
Larissa Magalhães
José Luiz Nunes
Ana Paula Vasconcellos
Walter B. Gaspar
Bruna Franqueira
Erica Bakonyi
Fernanda Scovino
João Carabetta

Lumen Juris Direito | 35 anos

GOVERNANÇA DE DADOS NO SETOR PÚBLICO

Lumen Juris Editora
www.lumenjuris.com.br

Filiais

Sede: Rio de Janeiro
Rua Newton Prado, nº 43
CEP: 20930-445
São Cristóvão
Rio de Janeiro – RJ
Tel. (21) 2580-7178

Maceió
(Divulgação)
Cristiano Alfama Mabilia
cristiano@lumenjuris.com.br
Maceió – AL
Tel. (82) 9-9661-0421

GOVERNANÇA DE DADOS NO SETOR PÚBLICO

DADOS ABERTOS,
PROTEÇÃO DE DADOS PESSOAIS
E SEGURANÇA DA INFORMAÇÃO
PARA UMA TRANSFORMAÇÃO
DIGITAL SUSTENTÁVEL

AUTORES
Luca Belli
Larissa Magalhães
José Luiz Nunes
Ana Paula Vasconcellos
Walter B. Gaspar
Bruna Franqueira
Erica Bakonyi
Fernanda Scovino
João Carabetta

Editora Lumen Juris
Rio de Janeiro
2024

Categoria: Direitos Humanos

Editor: João Luiz da Silva Almeida
Produção editorial: Angel Cabeza
Assistente editorial: Thiago Duarte
Designer editorial: Rebecca Ramos e Thassiel Melo
Diagramação: Alex Sandro Nunes de Souza
Gerente administrativo-financeiro: Carla Sampaio
Financeiro: Juliano de Oliveira
Assistente financeiro: Jefferson Badaró
Gerente comercial e logística: Arlei Rocha
Comercial e relacionamento: Cristiano Mabilia
Eventos: Arianna Pacheco
E-Commerce e atendimento: Maxwell de Souza

Impresso no Brasil | *Printed in Brazil*

Dados Internacionais de Catalogação na Publicação (CIP)

G721

Governança de dados no setor público : abertura de dados governamentais, proteção de dados pessoais e segurança da informação para uma transformação digital sustentável / Luca Belli... [et. al]. – Rio de Janeiro : Lumen Juris, 2024.
188 p. ; 23 cm.

Inclui bibliografia.

ISBN 978-85-519-2992-6

1. Proteção de dados - Legislação. 2. Segurança da informação. 3. Dados abertos. 4. Governança de dados. I. Belli, Luca (autor). II. Título.

CDD 342.810858

Ficha catalográfica elaborada por Ellen Tuzi CRB-7: 6927

Editora Lumen Juris
Rua Newton Prado, 43, São Cristóvão, Rio de Janeiro/RJ
CEP: 20930-445
Telefone: (21) 2580-7178 | atendimento@lumenjuris.com.br

Sobre os autores

Ana Paula Vasconcellos é doutora em estratégias, desenvolvimento e políticas públicas pelo PPED/UFRJ; mestre em Direito pela UERJ e pós-graduada em Direito e Novas Tecnologias pela UERJ/ITS. É a encarregada de dados pessoais na Secretaria Municipal de Integridade, Transparência e Proteção de Dados Pessoais. Atualmente, coordena a implementação do Programa Municipal de Proteção de Dados Pessoais e da Privacidade na Prefeitura da Cidade do Rio de Janeiro.

Bruna Franqueira é mestre em Teoria do Estado e Direito Constitucional pela PUC-Rio. Graduou-se na FGV Direito Rio em 2020. É pesquisadora do Centro de Tecnologia e Sociedade da FGV e advogada na Bioni Consultoria, onde atua com temas de proteção de dados pessoais e direito digital.

Fernanda Scovino é diretora de dados e inovação na Secretaria Municipal de Transportes do Rio de Janeiro e cofundadora do Instituto Base dos Dados. Atua na intersecção entre dados, tecnologia e políticas públicas, com experiência na Impulso-gov, Elogroup e Centro de Tecnologia e Sociedade (FGV/CTS).

Erica Bakonyi é mestre em Direito pela Universidade de Coimbra, possui MBA em Gestão da Segurança da Informação e especialização lato sensu em Licitações e contratos administrativos. É advogada e atua na área de privacidade e proteção de dados. É pesquisadora do Centro de Tecnologia e Sociedade, da FGV Direito Rio; mentora na área de privacidade e proteção de dados na Associação Brasileira de Lawtechs e Legaltechs (AB2L).

José Luiz Nunes é professor assistente de Direito e Ciência de Dados da FGV Direito Rio e pesquisador do CTS-FGV; bacharel em Direito pela FGV Direito Rio; mestre em Ciência de Dados e doutorando em Informática pela PUC-Rio.

Larissa Galdino de Magalhães Santos é pesquisadora associada da Universidade das Nações Unidas, unidade de Governança Eletrônica (UNU-EGOV); pesquisadora no Centro de Tecnologia e Sociedade da FGV e no CyberBRICS, da FGV Direito Rio; doutora em Ciência Política pela Unicamp.

Luca Belli, PhD, é professor da FGV Direito Rio, onde coordena o Centro de Tecnologia e Sociedade da FGV e o projeto CyberBRICS; membro do Board da Alliance for Affordable Internet, editor do International Data Privacy Law Journal da Oxford University Press, e diretor da conferência CPDP LatAm, Computers Privacy and Data Protection Latin America. Luca é doutor (PhD) em direito público pela Université Panthéon-Assas, Paris 2.

João Luiz Carabetta atua como Chief Data Officer da cidade do Rio de Janeiro. É formado em Física e mestre em Modelagem Matemática pela FGV. Carabetta é conhecido por estabelecer a ONG Base dos Dados em 2020, que supervisiona um *datalake* e facilita a acessibilidade aos dados no Brasil. Sua trajetória profissional inclui: Banco Interamericano de Desenvolvimento, Data Science for Social Good e o Centro de Tecnologia e Sociedade da FGV.

Walter B. Gaspar é advogado; mestre em Saúde Coletiva pelo Instituto de Medicina Social da UERJ e estudante de doutorado do Programa de Políticas Públicas, Estratégias e Desenvolvimento do IE-UFRJ; pesquisador do CTS-FGV; diretor-executivo da CPDP LatAm; e membro do Comitê de Programação do Open Forum Academy Symposium.

Os autores gostariam de expressar um sincero agradecimento aos professores Bruno Bioni, Gregory Michener e Luiz Cláudio Diogo Reis pela inestimável contribuição na revisão de uma versão preliminar deste livro. As análises cuidadosas, os comentários detalhados e sugestões valiosas dos revisores foram fundamentais para aprimorar o conteúdo, tornando-o mais claro, preciso e relevante.

Sumário executivo

Este livro apresenta as principais questões da governança e regulação de dados no setor público, estimulando uma visão sistêmica capaz de conectar as exigências da abertura de dados, da proteção de dados pessoais e da segurança da informação. Assim, o objetivo geral deste trabalho é interconectar estas dimensões fundamentais da governança de dados, destacando a necessidade de tal associação para uma transformação digital sustentável.

Este trabalho tem três objetivos específicos e complementares relativos à governança de dados no setor público, que devem se fortalecer reciprocamente. Primeiramente, traçar um diagnóstico detalhado do arcabouço regulatório em vigor no Brasil. Em segundo lugar, identificar as boas práticas que deveriam ser adotadas por administradores públicos a fim de favorecer uma transformação digital sustentável e, por fim, consolidar o arcabouço normativo e as boas práticas baseado numa série de recomendações e um modelo de avaliação de impacto sobre abertura, proteção e segurança de dados. Cabe frisar que, além das recomendações, os elementos do modelo, elaborado na parte conclusiva deste trabalho, serão embutidos numa ferramenta interativa, disponibilizada em acesso livre para suportar administradores públicos em suas atividades de abertura, proteção e segurança de dados.[1]

Com base nas análises desenvolvidas ao longo deste trabalho, os autores destacam a necessidade de se considerar a criação de um Escritório de Governança de Dados em cada unidade da administração pública, a fim de combinar as competências e facilitar a constante interação dos profissionais responsáveis pela abertura, proteção e segurança de dados. Como destacamos, a criação de um escritório responsável pela abertura de dados já é boa prática na administração pública. Já a identificação de um Encarregado — *Data Protection Officer* (DPO) é uma obrigação definida pela Lei Geral de Proteção de Dados. Porém, não existe, por enquanto, uma obrigação de definir um Chefe de Segurança de Informação — *Chief information security officer* (CISO).

---

1 Disponível em: www.cyberbrics.info/data-gov.

Nos parece que para favorecer uma transformação digital sustentável, não somente estas figuras são essenciais, mas é absolutamente fundamental que elas interajam e se coordenem da maneira mais eficiente, efetiva e harmoniosa possível. Assim, sugerimos que a criação de um Escritório de Governança de Dados que reúna os profissionais com background técnico e jurídico seja uma opção altamente desejável. Este trabalho está estruturado em quatro partes que oferecem elementos essenciais voltados a informar a governança de dados no setor público.

Enfim, a abordagem da governança de dados promovida neste trabalho relaciona-se com o estabelecimento de Ambientes de Pesquisa Confiáveis ou Sandboxes de Pesquisa. Ambientes de Pesquisa Confiáveis são baseados no modelo britânico dos *Trusted Research Environments* (TREs), também conhecidos como "enclaves de dados" ou "portos seguros de dados", já que são ambientes analíticos físicos ou virtuais que podem conter vários conjuntos de dados, atuando como uma sandbox voltada à pesquisa. Assim, o objetivo destes ambientes é conjugar as exigências da pesquisa baseada em processamento maciço de dados (abertos e/ou pessoais), com o pleno respeito de direitos, obrigações legais, e segurança, no âmbito de uma colaboração contínua entre setor público, setor acadêmico e setor privado, baseada em princípios éticos.

Esse estudo inclui também um anexo que descreve um protótipo de ferramenta desenvolvida com base nas recomendações elaboradas ao longo do documento. O objetivo de tal ferramenta é subsidiar o processo de tomada de decisão, em especial, na indicação de alguns pontos importantes, mas não exaustivos, que devem ser considerados no processo de governança de dados pelos entes públicos. A ferramenta, portanto, oferece um apoio — apesar de não automatizar completamente — na definição do processo de governança de dados, com base na extensa legislação e boas práticas existentes.

Parte I — Dados Abertos

A primeira parte do relatório fornece uma visão geral do estado das políticas relativas a dados públicos, acesso à informação e de dados abertos governamentais no Brasil. Foram revisadas as normas, políticas e iniciativas relativas aos dados, no âmbito do governo federal, e que estão relacionadas à evolução dos programas de governança eletrônica e digital.

Além de apresentar a concepção da Infraestrutura Nacional de Dados Abertos, o relatório indica as medidas de planejamento de execução de abertura de dados da Administração Pública Federal. Embora existam orientações contemporâneas sobre a abertura de dados, associada ao acesso à informação e governo digital, e políticas inovadoras sobre governança de dados no contexto dos estados, a falta de uma Política Nacional de Dados Abertos resulta em lacunas para aqueles municípios que pretendem abrir seus dados.

Assim, o relatório apresenta boas práticas a fim de apoiar melhorias relacionadas à disponibilidade, acessibilidade e reutilização de dados de forma responsável e segura. O relatório também destaca compromissos e práticas de governança de dados capazes de guiar governos, para abrir dados de boa qualidade com intuito de criar valor público, ou seja, para construir um ecossistema de dados abertos e sustentáveis. Esta parte aborda os seguintes assuntos:

- Adoção de uma política abrangente de abertura de dados que incentive diferentes esferas do governo a adotar a abertura de dados, e de normas que forneçam orientações claras sobre a coleta, armazenamento, compartilhamento e anonimização, garantindo que dados pessoais sejam protegidos e seguros quando da abertura de dados governamental;
- Estabelecimento de um paradigma técnico para metadados, consumo de dados, licenciamento de dados e anonimização, como regra geral, e principalmente, em casos de abertura de dados que envolvem dados pessoais;
- Estabelecimento de padrões de revisão e transparência para os casos de abertura de dados a partir de dados pessoais, e em casos de incidentes e ameaças cibernéticas;
- Realização de estudo de avaliação de impacto relativo aos riscos de abertura de dados, e estabelecimento de medidas de intervenção;
- Realização de auditorias sobre os dados que estão sendo abertos, criados, mantidos e gerenciados em ambiente controlado;
- Estabelecimento de um processo de governança de dados voltado a facilitar a transformação digital, incluindo pipelines de dados,

requisitos de qualidade de dados enquanto insumo para as tecnologias emergentes e modelos de tomada de decisão;

- Estabelecimento de uma estrutura de governança de dados composta por conselho ou comitê capaz de envolver e representar os interesses relativos à governança de dados sustentável, e, portanto, incluindo servidores, partes interessadas e especialistas;
- Promoção de treinamentos e educação para agências governamentais sobre como implementar as melhores práticas de proteção e cibersegurança ao abrir dados governamentais, e realização de campanhas de conscientização pública sobre o reuso de dados abertos;
- Estabelecimento de cooperação com parceiros a fim de compartilhar práticas e experiências para abertura sustentável de dados governamentais;
- Incentivos e promoção à aderência de políticas estaduais e municipais relativas à abertura de dados.

Parte II — Proteção de Dados Pessoais

Na segunda parte, após um breve histórico e descrição da Lei Geral de Proteção de Dados Pessoais brasileira, empreende-se uma incursão no tema da proteção de dados a partir de duas estratégias de revisão documental. Primeiro, os decretos estaduais regulamentadores da organização administrativa da proteção de dados pessoais na administração pública estadual direta e indireta foram revisados, buscando-se elementos em comum e divergentes que indiquem os caminhos adotados na concretização deste direito. O enfoque principal, neste ponto, é na distribuição das competências, o formato adotado para a figura do Encarregado e as salvaguardas e cuidados que cercam a sua atividade.

Segundo, empreendeu-se uma revisão de documentação advinda de órgãos públicos e entidades privadas relativa a boas práticas em proteção de dados pessoais, resumindo-se de forma esquemática as principais recomendações em formato descritivo. A conjunção dessas estratégias construiu uma primeira aproximação a respeito das formas concretas, da operacionalização da proteção de dados quando se converte a generalidade da

lei em ordenamentos, rotinas e estruturas práticas. Esta parte aborda os seguintes assuntos:

- Estabelecimento da Lei Geral de Proteção de Dados para harmonizar o regime de proteção de dados pessoais no Brasil;
- Estados brasileiros, especialmente após a LGPD, têm produzido normas que organizam a governança de dados pessoais, criando corpos de governança novos e/ou se aproveitam dos já existentes;
- Há sobreposição entre competências de estruturas institucionais pré-existentes no eixo acesso à informação — dados pessoais — segurança cibernética, de modo que um esforço de harmonização é necessário para tirar proveito de possíveis sinergias;
- A organização do papel do Encarregado é um ponto de considerável variação nas estruturas criadas nos estados. O papel do Encarregado deve estar cercado de garantias de independência e dotado dos recursos e acesso necessários;
- Já há uma extensa produção de guias e recomendações, inclusive oficiais, sobre boas práticas em se tratando de proteção de dados pessoais. Emprega-se, aqui, uma divisão esquemática baseada em uma visão do ciclo de vida do dado pessoal, que agrupa ações em oito chaves temáticas apresentadas de forma resumida.

Parte III — Segurança da Informação

Na última parte do relatório, é apresentado um breve mapeamento dos principais instrumentos normativos que abordam a promoção de segurança nas atividades realizadas nos meios digitais. Foram mapeados instrumentos normativos que trazem disposições gerais, em nível nacional e em nível estadual (utilizando-se como exemplo o Estado do Rio de Janeiro). Em seguida, apresentam-se boas práticas de segurança, orientadas por padrões internacionais (como NIST e ISO), além de outros relatórios já produzidos e que também tratam de temas relacionados à promoção de segurança nos meios digitais.

Como principais achados, apontam-se as seguintes medidas:

- No caso de entes ou órgãos no âmbito Federal, adotar o arranjo ("*framework*") de privacidade e segurança da informação e envio

à Secretaria de Governo Digital, conforme prevê a Portaria SGD/MGI nº 852/2023;

- No caso de entes ou órgãos no âmbito estadual ou municipal, recomenda-se adotar este arranjo como boa prática de segurança cibernética;
- Instituir mecanismos de cooperação de segurança cibernética com outros órgãos e entes, principalmente, com entidades ou órgãos públicos que também acessam e/ou realizam operações com os dados que serão abertos; trocas de experiências em situações de incidentes ou de rotinas de segurança;
- Elaborar política de segurança cibernética de fácil compreensão, acompanhada de documentos complementares, para informar sobre as medidas usadas para assegurar os dados pessoais objeto de abertura, e, ao mesmo tempo, dar transparência sobre eventuais impactos no direito de privacidade, de pessoas que interagem com as plataformas de dados abertos, diante da adoção de medidas de segurança;
- Investir em medidas de informação, comunicação, treinamento e educação em temas de segurança cibernética, estimulando comportamentos seguros no ambiente digital, e fornecendo transparência sobre quaisquer incidentes com dados pessoais, ou dados anonimizados, em geral, envolvidos na abertura de dados;
- Estimular a participação social na definição dos arranjos de segurança cibernética;
- Empreender esforços para que essas medidas alcancem não somente as/os agentes públicos, mas também fornecedores envolvidos no plano de dados abertos, e pessoas em geral que irão interagir com a plataforma de dados abertos;
- Garantir medidas de auditabilidade sobre a interação com sistemas e infraestruturas necessárias para abertura de dados, que sejam compatíveis com a garantia da privacidade e proteção de dados pessoais;
- Instituir instrumentos de responsabilização por descumprimento de obrigações de segurança cibernética a todas as pessoas jurídicas envolvidas nos processos de abertura de dados;

- Adotar ferramentas de segurança que permitam o acompanhamento contínuo de ameaças, vulnerabilidades e ataques de segurança;
- Sempre que possível, priorizar ferramentas não proprietárias/comerciais, open source (código aberto);
- Adotar esforços para incorporar, principalmente, os controles da ISO/IEC 27001:2013, indicados na Tabela II desta seção, para elaboração do sistema de segurança da informação do Plano de Dados Abertos, na medida daquilo que for cabível diante do contexto e realidade concreta da organização que está executando o plano de dados abertos.

Parte IV — Recomendações e Modelo de Avaliação de Impacto Sobre Abertura, Privacidade e Segurança de Dados

Por fim, este relatório oferece uma série de recomendações para tomadores de decisões e um modelo voltado a assistir administradores públicos na avaliação de impacto sobre abertura, privacidade e segurança de dados. É importante destacar que estas três dimensões precisam ser consideradas conjuntamente e, idealmente, cada órgão público deveria estabelecer um escritório de dados, no âmbito do qual profissionais preparados possam apoiar a abertura, proteção e segurança de dados, dialogando e cooperando continuamente.

A conclusão deste trabalho oferece um modelo que inclui orientações e boas práticas no que diz respeito à governança de dados, às operações de tratamento e à análise de riscos, suportando as atividades dos profissionais responsáveis pela transformação digital do setor público. Esta parte oferece orientações valiosas sobre as etapas necessárias a fim de facilitar as atividades de abertura, proteção e segurança de dados, com enfoque particular nos seguintes assuntos:

- Visão geral do tratamento e caracterização dos dados tratados;
- Descrição e controle das operações de tratamento e dos instrumentos de suporte com enfoque especial nas operações de tratamento, abertura dos dados e garantia de direitos do titular de dados;
- Estudo dos riscos de segurança de dados, com enfoque nos controles implementados para tratar os riscos relacionados à

segurança de dados, na descrição e avaliação dos controles gerais de segurança e dos controles organizacionais (governança);

- Avaliação de risco com particular enfoque nas possíveis violações da privacidade;
- Validação do modelo proposto, no que diz respeito às informações relativas a compartilhamento de dados com terceiros, à avaliação de conformidade a princípios fundamentais, de cumprimento das boas práticas de segurança de dados, de proporcionalidade e necessidade do tratamento, e de controles para proteger os direitos dos titulares dos dados;
- Avaliação das ações de mitigação de riscos, e elaboração de plano de ação;
- Documentação do modelo proposto com enfoque no resumo das respostas à tomada de subsídios, validação formal do encarregado pelo tratamento de dados pessoais, e validação formal do controlador.

Recomendações para tomadores de decisões

As seguintes recomendações são direcionadas aos tomadores de decisões e visam assistir o planejamento de políticas e mecanismos de governança de dados ao nível municipal. Neste sentido, as administrações locais deveriam:

- Promover a cooperação e participação multissetorial;
- Garantir a transparência significativa da governança de dados;
- Estabelecer um Escritório de Governança de Dados que inclua responsáveis de abertura de dados, encarregados de proteção de dados e chefes de segurança de informação;
- Criar uma estrutura de governança de dados composta por conselho ou comitê capaz de envolver e representar os interesses relativos à governança de dados sustentável, incluindo servidores, e partes interessadas e especialistas;
- Estabelecer "Ambientes de Pesquisa Confiáveis" ou "Sandboxes de Pesquisa" para permitir a pesquisa e desenvolvimento baseada em processamento de dados abertos e/ou pessoais no pleno respeito de direitos e obrigações legais;

- Estabelecer um processo de consulta pública multissetorial para receber comentários sobre as iniciativas propostas em termos de governança de dados;
- Adotar uma política abrangente de abertura de dados que incentive diferentes esferas do governo a adotar a abertura de dados;
- Adotar normas que forneçam orientações claras sobre a coleta, armazenamento, compartilhamento e anonimização, garantindo que dados pessoais sejam protegidos e seguros;
- Estabelecer um processo de governança de dados, incluindo requisitos de qualidade de dados enquanto insumo para as tecnologias emergentes e modelos de tomada de decisão;
- Estabelecer padrões técnicos para metadados, consumo de dados, licenciamento de dados e anonimização, nos casos de abertura de dados que envolvem dados pessoais e eventos relativos à cibersegurança;
- Estabelecer padrões de revisão e transparência para os casos de abertura de dados a partir de dados pessoais e em casos de incidentes e ameaças cibernéticas;
- Determinar a realização de estudo de avaliação de impacto e medidas de intervenção relativas aos riscos de abertura de dados;
- Realizar auditorias sobre os dados que estão sendo abertos, criados, mantidos e gerenciados em ambiente controlado;
- Promover treinamentos e educação para servidores públicos sobre como implementar as melhores práticas de proteção de dados e cibersegurança;
- Realizar campanhas de conscientização pública sobre governança de dados nas suas diferentes dimensões (abertura, proteção e segurança);
- Estabelecer parcerias a fim de compartilhar práticas e experiências para governança de dados;
- Incentivar o uso de *sandbox* de pesquisa para elaboração de tecnologia de gestão de dados;

- Promover avaliação de impacto de processamento de dados, com enfoque especial nos controles implementados para mitigar os riscos relacionados à segurança de dados, à privacidade e proteção de dados pessoais, e a discriminação;
- Promover a avaliação das ações de mitigação de riscos;
- Promover a documentação detalhada dos processos de governança de dados.

Sumário

Prefácio

É com notável apreço que apresentamos o livro *Governança de Dados no Setor Público*, resultado de uma colaboração excepcional entre o CTS-FGV, Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, e a UNU-EGOV, United Nations University Operating Unit on Policy-Driven Electronic Governance. Este trabalho emerge do Memorando de Entendimento recentemente estabelecido entre as duas instituições, refletindo seu comprometimento conjunto com a promoção e aprimoramento das práticas de governança digital e transformação digital no âmbito do setor público.

A parceria entre o CTS-FGV e a UNU-EGOV reforça o papel vital da cooperação internacional na produção e promoção do conhecimento, da inovação e da governança eficaz no setor público e na sociedade. Esperamos que este livro apoie o aprimoramento das estratégias de governança de dados no setor público, inspirando futuras iniciativas e pesquisas na área.

Este livro espelha o compromisso contínuo com a excelência acadêmica e experiência conjunta das instituições na busca por soluções eficazes e inovadoras no campo da governança digital. Os temas abordados destacam as melhores práticas e desafios enfrentados na governança de dados no cenário contemporâneo.

Boa leitura!

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

UNU

Centro de Tecnologia e Sociedade — FGV Direito Rio

O CTS-FGV, Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getulio Vargas Rio de Janeiro foi fundado em 2003, tornando-se o primeiro centro de pesquisa estabelecido no Brasil para analisar o impacto da tecnologia na sociedade. A missão do CTS-FGV é estudar as implicações jurídicas, sociais e culturais decorrentes do avanço das tecnologias de informação e comunicação, com particular enfoque nas áreas de governança digital, cibersegurança, proteção de dados, governança de Inteligência Artificial (IA), ciência de dados, regulação de plataformas e acesso à internet.

Nos últimos 20 anos, o CTS-FGV desempenhou um papel fundamental, moldando o ecossistema de políticas digitais brasileiro, latino-americano e global, conduzindo pesquisas reconhecidas internacionalmente pela qualidade acadêmica e pelo impacto, estimulando o diálogo com uma ampla gama de partes interessadas, incluindo governos e reguladores, organizações internacionais, empresas, centros de pesquisa e organizações da sociedade civil. Nas últimas duas décadas, o CTS-FGV organizou mais de 100 eventos internacionais e publicou mais de 300 pesquisas sobre uma variedade de questões de governança, regulação e transformação digital. Mais de 100 pesquisadores de mais de 30 nacionalidades já trabalharam no CTS-FGV e a maior parte das publicações do CTS-FGV pode ser acessada em acesso aberto na Biblioteca Digital da FGV e no site do Centro, disponível em: http://cts.fgv.br/.

Unidade Operacional em Governação Eletrônica da Universidade das Nações Unidas

A Unidade Operacional em Governação Eletrônica da Universidade das Nações Unidas (UNU-EGOV), instalada em Portugal (Guimarães) desde 2014, é um laboratório de ideias global (*think tank*) orientado para a investigação, assessoria e formação na área da governação digital, estabelecendo a ponte entre investigação e políticas públicas neste domínio. Parte integrante da Universidade das Nações Unidas, a UNU-EGOV tem como missão apoiar as Nações Unidas (ONU), bem como os seus Estados-Mem-

bros, na transformação dos mecanismos de governação e na construção de capacidades de governação eficazes, através da aplicação estratégica de tecnologias digitais, contribuindo assim para o desenvolvimento socioeconômico inclusivo, sustentabilidade ambiental, e paz e segurança.

Considerada uma referência internacional na área da governação digital e um parceiro sólido no universo da ONU, a UNU-EGOV reúne uma equipe multidisciplinar e multicultural de mais de 30 investigadores de 18 nacionalidades atuando em torno de problemas complexos e desafios emergentes. Desde o seu estabelecimento, a UNU-EGOV já desenvolveu mais de 60 projetos de governação digital em mais de 18 países, colaborou com 19 organizações internacionais, organizou mais de 90 eventos e realizou mais de 300 publicações. A UNU-EGOV coordena e organiza anualmente a Conferência ICEGOV, agregando uma comunidade de mais de 6.500 autores, acadêmicos, investigadores e profissionais atuantes na área da governação digital. Mais informações sobre a operação e publicações da UNU-EGOV encontram-se disponíveis em: https://egov.unu.edu/.

Introdução

A importância crucial da transformação digital do setor público, provavelmente ainda maior que no setor privado, não pode ser superestimada. Para tal transformação acontecer de maneira sólida, sustentável e bem-sucedida, é essencial que a governança de dados seja inclusiva, bem estruturada e executada.

Existe um amplo leque de oportunidades que podem ser aproveitadas para impulsionar a transformação e também um número cada dia maior de riscos suscetíveis de atrapalhá-la. Neste contexto, este relatório pretende acompanhar administradores públicos na complexa tarefa da transformação digital, oferecendo indicações concretas sobre como a governança de dados deve ser conduzida a fim de acelerar avanços sociais e econômicos, estabelecendo uma governança de dados, não somente em pleno respeito da legislação em vigor, mas também capaz de integrar as melhores práticas existentes.

A consideração em conjunto das três principais preocupações destacadas neste relatório — a abertura de dados, a proteção de dados pessoais e a segurança de dados — favorece uma abordagem holística suscetível de criar uma base sólida para a transformação digital do setor público. Para favorecer o sucesso e evitar o fracasso da transformação digital, as abordagens adotadas pelos administradores públicos devem considerar não somente as enormes oportunidades, mas também os potenciais riscos e externalidades negativas trazidos pelo uso apropriado de dados.

Nesta perspectiva, este trabalho procura abordar os desafios da governança de dados para uma transformação digital sustentável do setor público, com um particular enfoque em como órgãos municipais e estaduais podem estruturar sua governança de dados. Os autores deste relatório acreditam que uma governança de dados sólida e bem estruturada não seja somente instrumental para alcançar uma transformação digital completa, mas também permita alcançar a soberania digital, rumo a um verdadeiro Estado Digital capaz de estimular a inovação na perspectiva do interesse público (Belli; Guglielmi, 2022).

É sabido que dados abertos têm um grande potencial de desenvolvimento e benefícios tanto para a sociedade quanto para a economia (Zeleti; Ojo; Curry, 2016). Porém, é também reconhecido que as exigências legítimas de abertura e processamento de dados podem entrar em conflito, com as igualmente legítimas exigências de proteção de dados pessoais e cibersegurança.

Valores democráticos, tais como transparência, confiabilidade, acessibilidade e orientação para serviços e tomada de decisão têm sido associados aos programas de abertura de dados, publicação, catalogação e repositório de informações no setor público. Uma gama de políticas, projetos e estratégias vêm sendo implementadas, no nível global e local, a fim de garantir que as informações governamentais estejam disponíveis ao público, como dados acessíveis e reutilizáveis. Em parte, esse *framework* endereça respostas às leis de acesso à informação enquanto direito do cidadão, assim como acesso aos paradigmas da nova governança pública e digital.

No que concerne aos dados abertos governamentais, há uma série de recomendações que são introduzidas como boas práticas e vêm se consolidando através das comunidades de padronização da World Wide Web — por exemplo, W3C,[1] e dos princípios orientadores da gestão de objetos digitais, principalmente dados científicos (Schultes; Wittenberg, 2019).

A prática de abertura de dados faz parte das atividades do governo federal brasileiro desde as iniciativas introduzidas a partir da Lei de Acesso à Informação, tais como a criação do Portal de Transparência em 2004,[2] a Parceria para o Governo Aberto em 2011 e a Infraestrutura Nacional de Dados Abertos combinada com o quadro da Política de Dados Abertos e respectivas orientações.

No âmbito governamental, a Controladoria-Geral da União e os demais órgãos do governo federal têm operacionalizado os planos de dados abertos, enquanto instrumento que pautam a abertura de dados governamentais, o monitoramento e a gestão da política por meio do Portal Brasileiro de Dados Abertos.[3]

---

1 Melhores práticas para a publicação de dados na web. World Wide Web. Disponível em: https://w3c.br/traducoes/DWBP-pt-br/#intro.

2 Portal de Transparência lançado pela Controladoria-Geral da União frente às demandas e obrigações de transparência. Disponível em: https://bityli.com/Gi6hE.

3 Disponível em: https://dados.gov.br/home.

Entretanto, a operacionalização das ações e a implementação da abertura de dados têm pelo menos dois desafios. Primeiro, a falta de incidência direta em municípios e estados, já que a política não tem abrangência nacional; segundo, as questões legais. Pois, a abertura e reutilização das informações do setor público suscita preocupações relativas ao quadro jurídico de requisitos mínimos para proteção dos dados pessoais e o quadro mínimo para segurança da informação.

Relatórios de pesquisa (Wood; O'Brien; Gasser, 2016) já discutiam a tensão relativa entre as iniciativas de abertura de dados e a privacidade, e a necessidade de estabelecer um equilíbrio entre a manutenção do valor dos dados e a proteção de dados, mesmo antes da popularização dos recentes quadros jurídicos de proteção de dados pessoais.

A recém-criada Autoridade Nacional de Proteção de Dados, que zela pela proteção de dados pessoais nos termos da Lei Geral de Proteção de Dados Pessoais, está caminhando na elaboração de regulamentações que possam guiar o tratamento de dados pessoais de maneira mais específica e segura.

No entanto, à medida que as tecnologias emergentes impulsionam o avanço de recursos analíticos de dados, os riscos de conflito relativos aos interesses fundamentais protegidos pelos direitos à privacidade e proteção de dados cresceram, desafiando as abordagens tradicionais. O uso de dados de alto valor[4] — dados que podem ser aproveitados por empresas ou organizações, tais como registros de saúde durante a crise pandêmica, evidenciaram problemas de identificação, e a natureza conflituosa das técnicas de desidentificação ou agregação, quando utilizadas sem medidas de transparência.

Do ponto de vista regulatório, governos estaduais e municipais contam com um conjunto de ferramentas e medidas de mitigação restritas, na maioria das vezes, formatadas dentro das fronteiras da burocracia. Neste contexto, a tomada de decisão está atrelada aos silos da governança pública que carecem de vontade política, de capacidade de interpretação de padrões regulatórios e da capacidade de oferecer um ambiente robusto e seguro para os ativos digitais.

4 Dados de alto valor é uma expressão utilizada na Estratégia da União Europeia para dados (2020), visando a criação de um mercado único de dados. Mais informações disponíveis em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

Com relação ao debate em torno da segurança no meio digital, em geral, a cibersegurança esteve tradicionalmente associada à segurança da informação e à tecnologia da informação (van den Berg, 2020). Tratava-se de um campo de discussões voltado para a garantia da confidencialidade, integridade, autenticidade e disponibilidade das informações — os "princípios CIA" e os princípios "IAA", que trazem os critérios para assegurar a identificação, autenticação e acesso (van den Berg, 2020). Ademais, trabalhos mais recentes sugerem que as novas propostas para promoção de um ambiente digital trazem advertências sobre a adoção de comportamentos seguros pelos usuários e desenvolvedores[5] (van den Berg, 2020) e incorporam preocupações que colocam a segurança das pessoas no centro das discussões[6] (Liaropoulos, 2015; Whyte, 2022).

Recentemente, a percepção acerca das ameaças que atuam em meios digitais sofreu transformações: a proteção deixa de ser voltada a objetos e passa a direcionar o cuidado com sujeitos. Ou seja, a atenção passou do tradicional enfoque nos sistemas, infraestruturas, bases de dados, para a centralidade das pessoas ou grupos de pessoas que são alvo de ataques virtuais (Whyte, 2022, p. 343)[7] ou que podem ser afetadas por eles de maneira mais severa.

---

5 Partindo do conceito de ciberespaço, van den Berg (2020) propõe um modelo de três camadas para pensar a implementação de medidas que deem ênfase aos aspectos sociotécnicos da segurança no espaço digital. Segundo o autor, tal separação do ciberespaço em camadas, para que se possa conceituar a segurança à luz de cada uma delas, é útil para reforçar a principal preocupação em relação a atividades "cibernéticas": *i.e.* a preocupação com a adoção de comportamentos seguros na atuação no meio digital. Importante notar que o autor diferencia a cibersegurança da mera segurança da informação.

6 Liaropoulos (2014), em seu artigo *A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia*, defende, justamente, uma visão acerca da *cibersegurança*. O autor, portanto, lida com este conceito, e não com segurança cibernética - ambos, sem uma definição uníssona, e que se opõem à percepção limitada de campo a partir de uma perspectiva militarizada, vinculada à segurança nacional. Nesse sentido, defende uma visão sobre a cibersegurança de caráter holístico, cujo foco nas pessoas enfatiza a defesa pela cibersegurança enquanto um direito humano. A opção sobre o tom da abordagem da segurança no campo digital, conforme defende o autor, reflete uma escolha política: "cyber threats are classified as national security threats primarily for political reasons" (Liaropoulos, 2014, p. 16-7).

7 "While cybersecurity has traditionally been understood as the protection of digital networks and infrastructures, post-2016 cybersecurity discourses have stressed its increasingly human dimensions, notably around the issues of disinformation, manipulation, and political influence. As one 2019 trade conference suggested, cyber operators from the military and government are now faced by a new question: 'who, not what, will be targeted by hostile cyber operators?'. In

Independentemente da abordagem pretendida, a adoção de mecanismos de cibersegurança é essencial para a proteção não só das: *i)* pessoas — usuárias ou trabalhadoras de serviços públicos — a quem se referem as informações ou pelas quais os serviços públicos digitais desempenham um papel essencial, mas também; *ii)* daquelas usuárias e desenvolvedoras dos sistemas necessários para divulgação dos dados em plataformas digitais públicas; e *iii)* daquelas que, porventura, venham a realizar trabalhos ou modelagem sobre os dados publicizados pelo Poder Público.[8]

A centralidade da preocupação com os sujeitos da segurança digital não afasta a indispensabilidade da proteção de infraestruturas, redes, dados e sistemas, ou seja, objetos que sempre estiveram no campo de cuidados da segurança digital e que são instrumentos para a proteção dos sujeitos. As iniciativas não podem ficar restritas à segurança da informação. Portanto, a partir dessa perspectiva, o debate de segurança cibernética,[9] soma-se às orientações e boas práticas de proteção de dados e abertura de dados, devendo apoiar políticas nesse sentido implementadas pelos diferentes entes federativos brasileiros.

Na perspectiva de favorecer a abertura de dados de maneira responsável, este relatório oferece indicações particularmente valiosas para conjugar as necessidades de transparência e uso de dados com os imperativos de segurança e proteção de dados pessoais. Todavia, nos parece essencial destacar, preliminarmente, que a cibersegurança nunca pode ser uma certeza total. Assim, o objetivo desta obra é proporcionar a mitigação de riscos,

tracing its human turn, this article explores how the politics of race and truth have been central to a new and expansive vision of cybersecurity." (Whyte, 2022, p. 343).

8 Segundo van den Berg (2020, p. 28), quando apresenta a noção triangular – Pessoas, Processos e Tecnologia –, que faz parte da abordagem adotada pelos institutos de padronização de arranjos de segurança, a camada referente às pessoas pode ser dividida em usuários finais e desenvolvedores das aplicações. No entanto, essa visão mercadológica não necessariamente é adequada para responder à governança de segurança digital nas atividades de publicação de dados abertos, em plataformas. Por isso, apresentam-se outros grupos de pessoas que poderiam ser afetados e preservados por medidas de segurança.

9 Fichtner (2018) discute quatro abordagens para segurança cibernética, baseadas em: proteção de dados, salvaguardas de interesses financeiros, proteção de infraestruturas públicas e políticas e controle de fluxos de informação e comunicação. Para uma análise de diferentes conceituações de cibersegurança, ver também Wolff (2016); Belli (2020).

oferecendo caminhos valiosos para reduzir os riscos, capacitar administradores e incrementar a cibersegurança.

No Brasil, parece estar institucionalizando-se uma percepção de segurança focada nos dados, sistemas, infraestruturas e redes, sem atribuir a necessária centralidade à minimização dos riscos que o ambiente digital oferece às pessoas. A partir desta visão limitada, o glossário de segurança da informação, publicado em 2018 pelo então Governo Federal, através do Gabinete de Segurança Institucional, entende a cibersegurança como:

> Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis. (Brasil, 2018)

Este relatório pretende analisar a cibersegurança principalmente pelo prisma da segurança da informação, que nos parece um pilar essencial a fim de garantir uma governança de dados sólida. Enquanto assistimos à emergência de iniciativas inovadoras, como a Estratégia Europeia de Dados (European Commission, 2020), que vem promovendo um mercado único de dados abertos de alto valor a fim de conectar empresas, pesquisadores e a administração pública, parece necessária uma boa dose de pragmatismo para reconhecer os obstáculos existentes na prática. Particularmente, no nível local, os municípios encaram desafios para atrelar melhores práticas de abertura, ao arcabouço legal da proteção de dados pessoais e aos quadros favoráveis de segurança da informação.

Tendo em vista as diferentes abordagens de governança para lidar com estes desafios, este relatório apresenta um quadro sobre dados abertos governamentais no Brasil, a Lei Geral de Proteção de Dados Pessoais e outros dispositivos, e as iniciativas de segurança da informação no ambiente digital. O mapeamento vem acompanhado de boas práticas, recomendações e um roteiro a fim de apoiar a governança de dados para administradores públicos empenhados desde a abertura de dados.

Métodos qualitativos de pesquisa foram utilizados na elaboração deste relatório. Na primeira etapa de elaboração das hipóteses e do debate, foram priorizadas a análise documental de diferentes fontes e a pesquisa

bibliográfica em artigos e livros. Na segunda etapa de refinamento do documento, os pesquisadores foram envolvidos no debate de casos que envolvem a governança de dados. Finalmente, o relatório foi revisado por especialistas externos em dados abertos, proteção de dados pessoais e segurança da informação a fim de garantir a pertinência, qualidade e alcance das contribuições propostas.

Este relatório apresenta as principais questões da governança de dados no setor público, estimulando uma visão sistêmica capaz de conectar as exigências da abertura de dados, da proteção de dados pessoais e da segurança da informação. Assim, o objetivo deste trabalho é interconectar estas dimensões fundamentais da governança de dados, destacando a necessidade de tal associação para uma transformação digital sustentável. Na primeira seção, apresentamos o histórico e situação atual do arcabouço de dados abertos governamentais, focando em normas federais que servem de base para as recentes adaptações estaduais e municipais. Em seguida, exibimos um panorama das normas de proteção de dados pessoais, em especial como é sua implementação dentro das Administrações estaduais e de capitais brasileiras. Dando fim à parte mais descritiva, apresentamos um mapeamento de documentos normativos sobre segurança da informação, e a título de exemplo, a aplicação das normas no nível estadual.

Por fim, este relatório oferece um modelo voltado a assistir administradores públicos na avaliação de impacto sobre abertura, privacidade e segurança de dados. O modelo corrobora que estas três dimensões precisam ser consideradas conjuntamente e, idealmente, cada órgão público deveria estabelecer um escritório de dados no âmbito do qual profissionais formados na abertura, proteção e segurança de dados dialogam e cooperam continuamente. O modelo inclui, como conclusão deste trabalho, orientações baseadas em práticas e normas, no que diz respeito à governança de dados, às operações de tratamento e à análise de riscos, apoiando as atividades dos profissionais responsáveis pela transformação digital do setor público.

Parte I
Open Data: a evolução da abertura de dados no Brasil

Resumo em tópicos

Esta parte analisa a evolução dos dados abertos no Brasil, abordando os seguintes assuntos:

- Adoção de uma política abrangente de abertura de dados que incentive diferente esferas do governo a adotar a abertura de dados, e de normas que forneçam orientações claras sobre a coleta, armazenamento, compartilhamento e anonimização, garantindo que dados pessoais sejam protegidos e seguros quando da abertura de dados governamental;
- Estabelecimento de um paradigma técnico para metadados, consumo de dados, licenciamento de dados e anonimização, como regra geral, e, principalmente, em casos de abertura de dados que envolvem dados pessoais;
- Estabelecimento de padrões de revisão e transparência para os casos de abertura de dados a partir de dados pessoais, e em casos de incidentes e ameaças cibernéticas;
- Realização de estudo de avaliação de impacto relativo aos riscos de abertura de dados, e estabelecimento de medidas de intervenção;
- Realização de auditorias sobre os dados que estão sendo abertos, criados, mantidos e gerenciados em ambiente controlado;
- Estabelecimento de um processo de governança de dados voltado a facilitar a transformação digital, incluindo pipelines de dados, requisitos de qualidade de dados enquanto insumo para as tecnologias emergentes e modelos de tomada de decisão;
- Estabelecimento de uma estrutura de governança de dados composta por conselho ou comitê capaz de envolver e representar

os interesses relativos à governança de dados sustentável, e, portanto, incluindo servidores, partes interessadas e especialistas;

- Promoção de treinamentos e educação para agências governamentais sobre como implementar as melhores práticas de proteção e cibersegurança ao abrir dados governamentais, e realização de campanhas de conscientização pública sobre o reuso de dados abertos;
- Estabelecimento de cooperação com parceiros a fim de compartilhar práticas e experiências para abertura sustentável de dados governamentais;
- Incentivos e promoção à aderência de políticas estaduais e municipais relativas à abertura de dados.

Introdução

O acesso a informações e abertura de dados públicos, conhecidos também como open data, apesar de instituídos como direitos fundamentais, só tiveram avanços substanciais com a criação da Lei de Acesso à Informação (LAI) em 2011. Desde então, diferentes programas e iniciativas do governo federal imputaram incentivos à abertura de dados e à disseminação dos instrumentos e técnicas de coleta e disponibilização dos dados no âmbito do governo federal.

Entretanto, há uma lacuna na adoção de uma política de dados abertos nacional, abrangente para estado e municípios, combinando recursos de planejamento e sustentabilidade da abertura entre as organizações do setor público. Há também um atraso na definição de um quadro de governança de dados para o setor público acompanhar as demandas da sociedade e melhorar continuamente suas operações e serviços por meio de tecnologias digitais.

A falta de ações de capilarização da abertura de dados para todas as organizações do setor público impacta na lacuna de orientações claras sobre a coleta, armazenamento e uso de dados pessoais, incluindo diretrizes de anonimização de dados e compartilhamento de dados, bem como a garantia de infraestrutura de segurança cibernética adequada, com protocolos claros para responder ameaças e incidentes.

Além disso, no contexto da transformação digital governamental, a abertura de dados, associada à sua governança, é um recurso central para elaboração de políticas públicas e para subsidiar o uso de tecnologias emergentes, tais como, inteligência artificial, no setor público. Portanto, é imprescindível fomentar a governança de dados sustentável que envolva as diferentes estruturas e iniciativas governamentais, com o respaldo de garantias de que os dados pessoais sejam protegidos e seguros ao abrir dados do governo.

Prioridades:

- Adoção de uma política abrangente que incentive diferentes esferas do governo a adotar a abertura de dados;
- Adoção de orientações ou normas com instruções claras sobre a coleta, armazenamento, compartilhamento e anonimização —

garantindo que dados pessoais sejam protegidos e seguros no processo de abertura de dados governamental;

- Estabelecer paradigma técnico para metadados, consumo de dados, licenciamento de dados e anonimização, nos casos de abertura de dados que envolvem dados pessoais e eventos relativos à cibersegurança;
- Estabelecer padrões de revisão e transparência para os casos de abertura de dados a partir de dados pessoais, e em casos de incidentes e ameaças cibernéticas;
- Determinar a realização de estudo de avaliação de impacto e medidas de intervenção relativas aos riscos de abertura de dados;
- Criar parâmetros que motivem a decisão de abertura frente ao risco de violação a outros direitos;
- Realizar auditorias sobre os dados que estão sendo abertos, criados, mantidos e gerenciados em ambiente controlado;
- Estabelecer a governança de dados estruturante para a transformação digital, incluindo pipelines de dados, requisitos de qualidade de dados enquanto insumo para as tecnologias emergentes e modelos de tomada de decisão;
- Criar uma estrutura de governança de dados composta por conselho ou comitê capaz de envolver e representar os interesses relativos à governança de dados sustentável, incluindo servidores e partes interessadas;
- Promover treinamento e educação para agências governamentais sobre como implementar as melhores práticas de proteção e cibersegurança ao abrir dados governamentais;
- Realizar campanhas de conscientização pública sobre o reuso de dados abertos;
- Estabelecer a cooperação com parceiros a fim de compartilhar práticas e experiências para abertura sustentável de dados governamentais;
- Promover à aderência às políticas estaduais e locais relativas à abertura de dados;

- Envolver especialistas e sociedade civil na estrutura da governança de dados sustentável, e na definição de políticas e normas;
- Integrar estrutura e processo decisório de abertura de dados com áreas de proteção de dados e segurança da informação.

1 Evolução normativa do acesso e abertura de dados governamentais

Entre 1965 e 1985, o sigilo foi regra na administração pública brasileira, sem qualquer prerrogativa relativa à transparência de informações e atos. Apesar do tratamento diferente de informações, cartas constitucionais anteriores aos períodos da redemocratização também não previam um direito de acesso à informação pública. Com a promulgação da Constituição em 1988, baseada na concepção do Estado Democrático de Direito, o acesso à informação pública tornou-se um direito fundamental.

Cabe destacar que o verdadeiro valor constitucional da abertura de dados governamentais, além das inúmeras oportunidades econômicas e científicas que tal processo é susceptível de proporcionar, está associada à governança dos dados. Assim, tal abertura deve ser efetuada de maneira responsável, operando uma necessária ponderação entre interesses constitucionais divergentes, nomeadamente no que diz respeito aos direitos à privacidade, segurança e o recém-constitucionalizado direito à proteção de dados (Belli; Barros; Reia, 2018).

O artigo 5º da Constituição Federal determinou o direito de acesso à informação e assegurou a proteção de informações de interesse particular, coletivo ou geral. Ainda, estabeleceu uma ação própria de *habeas data* para assegurar acesso a dados relativos ao impetrante. No que se refere à publicidade dos atos da Administração Pública, o artigo 37 estabeleceu o princípio da publicidade, garantindo que todos os atos da Administração Pública sejam expostos aos cidadãos.

Já o artigo 216 da Constituição determinou que a Administração Pública deveria, na forma de lei, resguardar a gestão da documentação governamental e dar providências para viabilizar a consulta às informações por aqueles que necessitam. De fato, os dispositivos contidos na Constituição

Federal tratam da informação pública como um bem público. No entanto, faltava à legislação normativas especificidades capazes de resguardar o direito de acesso.

Até a regulamentação da Lei de Acesso à Informação em 2011, outros dispositivos apoiaram indireta e transversalmente o acesso e manutenção das informações públicas. Em 1991, a Lei nº 8.159 estabeleceu a Política Nacional de Arquivos Públicos e Privados, estabelecendo como dever do Poder Público a gestão da documentação. Contudo, não há norma para orientar a execução de um direito de acesso.

Nos anos 2000, a Lei Complementar nº 101, conhecida como Lei de Responsabilidade Fiscal, e as modificações introduzidas pela Lei Complementar nº 131/2009, determinou a disponibilização de informações de gestão fiscal. Embora a Lei determinasse a divulgação de gastos públicos, entre outros dados, na forma de transparência ativa em páginas web, não especificou o direito à transparência passiva, ou seja, pedido e recebimento de informações públicas, nem padrões de qualidade ou formatação de dados.

Resumindo, até a Lei de Acesso à Informação (LAI) de 2011 não havia dispositivo legal que determinasse e garantisse o acesso gratuito, atualizado, qualificado, sistematizado e organizado das informações públicas, como determinado através de dados abertos governamentais. Portanto, anteriormente à LAI, a disponibilização de dados governamentais era um fenômeno esporádico e não organizado.

1.1. Dados públicos x dados abertos governamentais: ações de governo eletrônico

As primeiras ações relativas à política de disseminação de dados e informações governamentais para livre uso estão alinhadas com o governo eletrônico em meados de 2000. Até então, todas as informações eram imprecisamente tratadas como dados públicos, sem uma regulamentação ou norma de orientação ao tratamento, disponibilização e acesso.

O Departamento de Governo Eletrônico, criado em 2004, alinhou suas ações a um momento global de democratização do acesso a informações (Brasil, 2004). No mesmo ano, o governo lançou os "Padrões de Interoperabilidade em Governo Eletrônico" (e-PING), instrumento essencial para

viabilizar o ecossistema de dados e informações governamentais de forma eficiente e fazendo o uso pleno de tecnologias.

A adoção do e-PING tornou-se obrigatória para o executivo federal em 2014.[10] Tal medida afirma que todos os sistemas de informação, aquisições e atualizações de tecnologias da informação e comunicação devem se adequar, preferencialmente, a padrões abertos. Padrões abertos são modelos comuns baseados em consenso, para a troca e compartilhamento facilitado. Padrões proprietários são aceitos somente mediante determinadas condições.[11] A atualização mais recente do e-PING foi em 2018, mas não há orientações sobre padrões de dados abertos e abertura de base de dados pessoais.

Outras ações,[12] tais como a criação do Guia Livre de Referência para Software Livre, a criação dos Padrões Brasil e-GOV e a Estratégia Geral de Tecnologia da Informação no âmbito do Sistema de Administração dos Recursos de Informação e Informática do governo federal, contribuíram na disponibilização de dados públicos, fomentando o ecossistema de dados abertos governamentais

1.2 Parceria para o Governo Aberto, acesso às informações e a abertura

Em 2010, o Ministério do Planejamento, Orçamento e Gestão, Secretaria de Logística e Tecnologia da Informação, lançou a Estratégia Geral de Tecnologia da Informação 2011-2012,[13] cuja meta 12 tratava de promover o aumento do nível de maturidade na adesão dos padrões e-PING através da implementação da Infraestrutura Nacional de Dados Abertos (INDA).

Em meados de setembro de 2011,[14] o Brasil, junto da África do Sul, Estados Unidos, Filipinas, Indonésia, México, Noruega e Reino Unido, assinou a Declaração de Governo Aberto criado pela *Open Government Partnership*.

10 Disponível em: https://is.gd/ikeyex.

11 As condições para padrões proprietários são: quando da inexistência de padrão aberto, na qual poderão ser adotados padrões proprietários até que um padrão aberto esteja disponível; e de forma transitória, em soluções de TIC do legado (e-Ping, 2018).

12 A cronologia das ações governamentais está disponível em: https://is.gd/odekis.

13 Disponível em: https://is.gd/QOSdkN.

14 Disponível em: https://is.gd/CC5Zi2.

No mesmo ano, o governo lança o Plano de Ação Nacional sobre Governo Aberto que chancela a criação da *Open Government Partnership*. O Plano[15] teve como objetivo difundir boas práticas governamentais em incentivo à transparência, acesso à informação pública e participação social, determinando o aumento da disponibilidade de dados, a criação da infraestrutura de governança e aparato legal para a abertura governamental de um modo geral. Também foi criado o Comitê Interministerial Governo Aberto (CIGA), composto por diversos órgãos do governo a fim de coordenar e facilitar a implementação do plano.

Apesar das estratégias e diretrizes criadas para orientar a disponibilização de dados públicos como dados abertos, as condições sobre a obrigatoriedade da publicação das informações geridas pelo governo ainda eram confusas.

Entretanto, a LAI que data da mesma época, concretizou o direito constitucional de acesso dos cidadãos às informações públicas. A Lei determinou os procedimentos de acesso à informação tanto para os órgãos e entidades públicas, quanto para entidades envolvidas com recursos públicos. Principalmente o cidadão, passa a poder solicitar informações, desde que não sejam classificadas como sigilosas, obedecendo às regras, prazos e instrumentos de controle, consolidando o princípio da publicidade como preceito geral, e do sigilo como exceção.

Assim, de acordo com a LAI, o cidadão deve ser orientado também sobre os procedimentos de acesso à informação, o que inclui o princípio de abertura de dados como estímulo à disponibilização de dados. O artigo 8º da LAI estabeleceu as condições de visualização e busca das informações, além das recomendações gerais para disponibilização da informação via formato aberto, estruturado e legível por máquina.

No que tange à transparência ativa, cabe aos órgãos serem proativos quanto à divulgação das informações com conteúdos mínimos, para além da transparência passiva que consiste no pedido de informação feito pelo cidadão.

Claramente, o legislador considerou a necessidade de que se mantenha o sigilo, no que diz respeito às informações cuja divulgação não seja justificada pelo interesse público, cuja divulgação pode causar grave dano à segurança da sociedade e do Estado. Também são estabelecidos prazos de restrição do sigilo e quais autoridades têm competência para classificar informação.

15 Disponível em: https://is.gd/oMg4Uq.

Apesar de a Lei compilar as especificidades de proteção do direito de acesso à informação, determinando as condições de divulgação das informações e a responsabilidade com a transparência da gestão pública, os artigos nºs 43 e 44 delegam as orientações sobre o tratamento de dados pessoais ao Gabinete de Segurança Institucional da Presidência da República. Assim, o acesso, divulgação e tratamento de informações fica restrito às pessoas que tenham necessidade conhecida e que sejam credenciadas pelo gabinete presidencial.

1.3 Infraestrutura Nacional de Dados Abertos (INDA): uma iniciativa multissetorial

Em 2012, a Instrução Normativa nº 4[16] criou a Infraestrutura Nacional de Dados Abertos. A instrução conectou o marco regulatório do acesso à informação, da abertura de governos e o plano de ação da Estratégia Geral de Tecnologia da Informação do governo federal. A INDA foi criada em conformidade com os Padrões de Interoperabilidade de Governo Eletrônico (ePING).

A instrução determina a metodologia que deve ser utilizada pelos órgãos públicos para divulgar os dados em formato aberto, através do Portal Brasileiro de Dados Abertos. A norma também determinou a estrutura de governança, a implementação do Portal e os objetivos.[17] Também fomentou a participação de entidades e da sociedade civil através de adesão voluntária.

Um dos desafios da implementação da política de dados abertos foi a criação de um modelo de governança que conseguisse dialogar com o cidadão e dar sustentabilidade à iniciativa (Herrmann, 2020). Primeiro, porque não havia um orçamento dedicado às ações relativas aos dados abertos; e, segundo, porque uma instrução normativa não era capaz de angariar o mesmo apoio político de um decreto ou política. Boa parte das ações foi feita artesanalmente pelo Comitê Gestor da INDA, que foi instituído pela mesma Instrução Normativa, e entidades engajadas.

16 Disponível em: https://www.gov.br/governodigital/pt-br/legislacao/InstrucaoNormativaINDA42012.pdf.

17 De modo geral, os objetivos da INDA visam garantir e facilitar o acesso aos dados e informações produzidas ou custodiadas pelo Poder Executivo federal, pelas diversas instâncias do setor público.

A organização do Comitê Gestor da Internet no Brasil (CGI.br) foi o modelo que inspirou a governança e as interações da INDA. Nesse modelo, as primeiras reuniões para discutir o planejamento da INDA envolveram servidores públicos e entidades da sociedade civil. Este formato continuou refletindo a estrutura do Comitê e fomentou eventos, tais como o I Encontro Nacional de Dados Abertos.

Entre 2011 e 2012, os projetos da Infraestrutura Nacional de Dados Abertos foram mantidos de forma colaborativa com a presença do Comitê e de representantes de entidades tais como Transparência Hacker e *Open Knowledge Foundation*.[18]

O Comitê Gestor da INDA é composto por integrantes de diversos órgãos federais, representantes da sociedade civil e um representante do setor econômico. Entre as funções do novo comitê, está a criação de procedimentos para que os órgãos apresentem plano de adequação a fim de que os dados públicos sejam dados abertos. Isso inclui quaisquer considerações sobre a abertura de dados que contenham informações sensíveis ou pessoais, ou seja, a adequação à Lei Geral de Proteção de Dados.

Portanto, a INDA estabeleceu um conjunto de padrões, tecnologias, procedimentos e mecanismos de controle necessários para atender às condições de disseminação e compartilhamento de dados e informações públicas.

De acordo com o Capítulo 1, artigo 2º da Instrução Normativa INDA, dados abertos são "dados públicos representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na rede mundial de computadores e disponibilizados sob licença aberta permitindo livre utilização, consumo ou cruzamento". A diretriz geral é baseada na definição da *Open Knowledge International*. As três leis de David Eaves e oito princípios de dados abertos governamentais também são adotadas pelas organizações do setor público.[19]

A instrução normativa de criação da INDA, assim como o *framework* de abertura do governo, determinou a criação do Portal Brasileiro de Dados Abertos como ponto central para publicação de dados abertos governamentais.

---

18 Disponível em: https://is.gd/EIorKp.

19 Para recomendações da W3C. Disponível em: https://is.gd/c2VYZ6. Acesso em: 19 jan. 2022.

A versão beta do Portal foi lançada em 2012. No entanto, a iniciativa também teve desafios orçamentários e de apoio institucional. A saída foi chamar outras entidades e *experts* para participar colaborativamente.[20] A Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento conduziu as atividades de desenvolvimento ágil entre ativistas e servidores públicos e utilizou plataformas abertas de software livre para disponibilizar o Portal.

1.3.1. Política de Dados Abertos do Governo Federal

A Política de Dados Abertos do Executivo Federal foi instituída pelo Decreto nº 8.777 de 2016[21] e definiu as regras para a disponibilização de dados abertos governamentais no âmbito do Poder Executivo Federal e outros incentivos, tais como transparência pública, controle social e desenvolvimento de tecnologias voltadas à gestão pública. A política é composta por uma série de documentos normativos, de planejamento e de orientação para a abertura de dados.

De acordo com o Artigo 1º, os principais objetivos da Política são a promoção da publicação de dados contidos nas respectivas bases de dados governamentais, sob o formato de dados abertos; fomento à transparência pública; facilitação e acesso de forma aberta para o cidadão. Além disso, todos os órgãos e entidades da administração pública devem publicar Planos de Dados Abertos a cada dois anos, seguindo também as orientações e resoluções do Comitê Gestor da Infraestrutura Nacional de Dados Abertos.

A Política atribui à INDA o estabelecimento de normas complementares através dos Planos de Dados Abertos, e a orientação gerencial e normativa relacionada à proteção de informações pessoais na publicação de bases de dados, conforme o artigo 5º, III. O Plano é um documento que orienta desde a implementação das ações até os padrões mínimos de qualidade dos dados.

Portanto, os dados passíveis de abertura são todos aqueles dados que não contenham informações protegidas, nos termos da LAI, conforme o Artigo 8º do Decreto nº 8.777/16. A LAI, em seu artigo nº 31, determina que o tratamento das informações pessoais deve ser feito de forma transparente,

20 Disponível em: https://is.gd/2hymC5.

21 Disponível em: https://is.gd/6ueltn.

com respeito à intimidade, à vida privada e às liberdades e garantias individuais. Neste sentido, parece essencial ler a LAI em conjunção com o arcabouço normativo de proteção de dados pessoais (Belli; Barros; Reia, 2018) e, particularmente, cuidando de efetuar uma justa ponderação entre as exigências de abertura de dados e as de proteção de dados pessoais, definidas na próxima seção.

Em outubro de 2017, o Comitê Gestor da INDA aprovou a Resolução nº 3,[22] estabelecendo as normas de elaboração e publicação dos Planos de Dados Abertos, conforme determinação da Política de Dados Abertos.

O Decreto nº 9.903[23] de 2019 disciplinou a gestão e direitos de uso de dados abertos, determinando a utilização gratuita das bases de dados, e conferindo à Controladoria-Geral da União (CGU) a coordenação da política por meio da INDA. A CGU deve também acompanhar o andamento dos Planos de Dados Abertos, bem como a conformidade do cronograma de publicação.

1.3.2. Planos de Dados Abertos

Plano de Dados Abertos (PDA) é um instrumento que operacionaliza a Política de Dados Abertos do Poder Executivo Federal, uma vez que serve para o planejamento das ações de abertura e sustentabilidade da abertura de dados nas organizações públicas, com vigência de dois anos.

O PDA foi regulamentado pela Resolução nº 3[24] do Comitê Gestor da INDA em 2017. Para ter validade, o PDA deve apresentar todos os itens contidos na resolução, ou seja, o *checklist* completo é obrigatório.

De acordo com a resolução, as normas de elaboração do plano determinam que as bases devem ser disponibilizadas em função do seu potencial interesse público. Para isso, deve haver mecanismos de participação social para definir as prioridades. A resolução prevê, outrossim, que a abertura dos dados georreferenciados deve acontecer na observância das normas estabelecidas pela Infraestrutura Nacional de Dados Espaciais.[25]

22 Disponível em: https://is.gd/Sx7p2B.

23 Disponível em: https://is.gd/K1j5R9.

24 Disponível em: https://is.gd/qprFlF.

25 Disponível em: https://is.gd/6ushbL.

Os Planos devem conter a relação de todas as bases dos órgãos e o catálogo para identificar as bases já abertas, ou não, disponibilizadas, ou não, no Portal Brasileiro de Dados Abertos. Toda estratégia adotada pelos órgãos para viabilizar a abertura de dados deve ser descrita com cronograma. Após a aprovação do Plano dentro da instituição, os órgãos devem disponibilizar e manter as bases atualizadas e catalogadas no Portal Brasileiro de Dados Abertos.

A disponibilidade de dados é monitorada pela Controladoria-Geral da União (CGU) que disponibiliza os resultados de sua análise através do Painel de Monitoramento de Dados Abertos[26]. A CGU preparou um modelo de estrutura formal[27] de um plano de dados abertos. O modelo sugerido pela CGU consiste nas seguintes etapas:

1. Realização de discussão por meio de um grupo de trabalho, e definição dos responsáveis pela elaboração e cumprimento do PDA de cada órgão;
2. Elaboração do inventário da base de dados de cada órgão ou entidade, inserido separadamente o setor, departamento, além da relação das bases já abertas e catalogadas no Portal Brasileiro de Dados Abertos; relação das bases que ainda não foram catalogadas no Portal; e relação das bases que ainda não foram disponibilizadas no formato aberto até a publicação do plano;
3. Adoção de um mecanismo de participação social, tal como a consulta pública, a fim de identificar a demanda do cidadão de acordo com as bases de dados do órgão. O inventário deve ser disponibilizado para votação no portal do órgão/entidade;
4. Elaboração de uma matriz de prioridades a fim de direcionar os critérios de publicação conforme a recomendação da Resolução nº 3 da INDA: relevância para o cidadão, controle social, obrigatoriedade legal ou compromisso, dados de projetos governamentais estratégicos, dados de serviços públicos, dados para fomento do desenvolvimento sustentável, dados para o fomento de negócios na sociedade, dados mais solicitados em transparência passiva da LAI;

26 Disponível em: https://is.gd/wXOysW.

27 Recomendações presentes no Manual de Publicação do PDA. Disponível em: https://is.gd/IRSJTa.

5. Listagem das bases que serão abertas durante a vigência do PDA;
6. Determinar um cronograma de abertura de bases conforme os critérios de prioridade;
7. Definir uma estratégia com cronograma de publicação, sustentação e difusão dos dados;
8. Todas as ações devem ser registradas no Plano de Dados Abertos.

No que tange à abertura de bases de dados selecionadas, cujas informações possuam restrições de sigilo e privacidade do cidadão, de acordo com a Seção II e artigo nº 17 da Lei Geral de Proteção de Dados Pessoais, cabe ao órgão observar as seguintes recomendações:

1. Adotar um tratamento adequado, considerar o grau de sensibilidade e os elementos da informação para decidir sobre a supressão, mascaramento ou agregação;
2. O tratamento de dados das bases selecionadas para abertura prioriza as bases que contêm informações relativas aos sistemas estruturantes da Administração Pública, tais como compras públicas, orçamento e servidores públicos;
3. No caso de bases que contenham informações relacionadas aos sistemas estruturantes e que são especializadas, é importante realizar a abertura. Por exemplo, professores de universidades públicas que sejam servidores públicos, cujas informações adicionais, como o currículo, são úteis à sociedade.

1.3.3. Orientações técnicas para publicação de dados abertos governamentais

A Cartilha Técnica para Publicação de Dados Abertos no Brasil v1.0[28] foi criada para orientar as organizações governamentais quanto às boas práticas técnicas de publicação de dados na Internet.

Segundo a Cartilha, cada órgão é responsável pela preparação, validação e publicação de um conjunto de dados públicos em formato aberto. A

28 SLTI, MP. Cartilha Técnica para Publicação de Dados Abertos no Brasil. Disponível em: https://is.gd/FnNjVr.

Cartilha reúne um conjunto de orientações técnicas, tais como formatos desejáveis de dados, definição de metadados e princípios da catalogação.

Outros Manuais e Orientações[29] estão disponíveis no site do Ministério da Gestão e da Inovação em serviços,[30] tais como: Manual de Elaboração de Plano de Dados Abertos, Guia de Abertura de Dados e Arquitetura Técnica Referencial de Abertura de Dados.

Grande parte do material de apoio[31] disponível sobre a abertura e publicação de dados são heranças das primeiras ações da Infraestrutura Nacional de Dados Abertos, portanto, foram produzidos entre 2011 e 2012 e não há atualizações que tratam da abertura de base com dados pessoais.

1.4 Estratégias governamentais e dados abertos

A primeira versão da Estratégia Brasileira de Governança Eletrônica foi lançada em janeiro de 2016 e revisada em 2018, após a criação da Estratégia Brasileira de Transformação Digital (E-Digital).

Ambas as estratégias tinham entre seus objetivos o fomento à disponibilização de dados abertos governamentais, formatando a transparência pública e implementação da Política de Dados Abertos no âmbito do governo federal. Apesar das recomendações versarem sobre a criação de um ecossistema de dados públicos em formato aberto, disponível por meio do Portal Brasileiro de Dados Abertos, não houve alterações significativas com relação às ações que já vinham ocorrendo.

De um modo geral, a E-Digital foi pensada para conduzir políticas públicas que garantem a adoção de tecnologia para sociedade e para o governo, tendo eixos capacitadores e eixos de transformação digital. A versão 2018 determinou cerca de cem ações. Além disso, o ciclo de atualização da estratégia foi institucionalizado pelo Sistema Nacional de Transformação Digital (SinDigital). O SinDigital é um sistema instituído pelo Decreto

29 Desde que o Portal Brasileiro de Dados Abertos foi remodelado pela Controladoria-Geral da União em dezembro de 2022, os materiais de apoio estão disponíveis na Base de Conhecimento do CGU. Disponível em: https://repositorio.cgu.gov.br/.

30 Governo Digital. Material de apoio. Gov.br. Disponível em: https://is.gd/VLUnF5.

31 Governo Digital. Material de apoio. Gov.br. Disponível em: https://is.gd/VLUnF5.

nº 9.319,[32] e que é composto pela Estratégia Brasileira para a Transformação Digital, seus eixos temáticos e sua estrutura de governança.

Com relação aos resultados da E-digital, o eixo relacionado ao governo digital foi o que mais avançou.[33] Neste sentido, as ações relacionadas à Estratégia de Governo Digital melhoraram a oferta e acesso aos serviços públicos digitalizados, além do crescimento na disponibilização de dados. Entretanto, ainda há pontos de melhoria que devem ser observados, como a necessidade de aperfeiçoamento na interoperabilidade dos dados governamentais, a proteção de dados pessoais dos usuários de serviços públicos digitais, e a criação de uma *data lake*[34] para apoiar a formulação de políticas públicas.

A revisão recém-lançada E-Digital, ciclo 2022-2026,[35] incluiu no eixo "Cidadania e transformação digital do governo", cujo objetivo inclui a concessão ampla à informação e aos dados abertos governamentais. Dentre as ações específicas para os dados abertos, consta o aprimoramento da política de dados abertos no âmbito nacional, a fim de envolver entes federados e sociedade civil, promovendo a interoperabilidade de serviços baseados em dados, sistemas e plataformas; e a padronização das formas de acesso e oferta de dados públicos.

1.4.1. Governo Digital e dados abertos governamentais

A Estratégia de Governo Digital 2020-2022, que é parte do eixo de ações da E-Digital, elencou entre seus objetivos a reformulação dos canais de transparência e dados abertos. Os objetivos, tais como integração de portais de transparência, de dados abertos e de ouvidoria ao portal único gov.br, ainda estão em andamento.

---

32 BRASIL. Decreto nº 9.319, de 21 de março de 2018. Disponível em: https://is.gd/8ghhbP.

33 A E-Digital 2022-2026 oferece um diagnóstico das ações da primeira versão. Disponível em: https://is.gd/GTBzGZ.

34 Data lake é um repositório para armazenamento de múltiplos conjuntos de dados, que pode ser aberto ao público geral ou não. O objetivo é agregar alto volume de dados estruturados e não estruturados em um mesmo servidor que permita também a consulta por diversos usuários. Esses serviços costumam ser oferecidos por empresas que oferecem processamento e armazenamento via máquinas virtuais, e são otimizados para tratamento/armazenamento/consulta dos dados.

35 Disponível em: https://is.gd/6ueltn.

Em março de 2021, a Lei do Governo Digital consolidou os instrumentos e regras para a transformação digital do governo. A Lei recomenda a adoção preferencial de formatos abertos e livres em concordância com o artigo nº 10 do Marco Civil da Internet.

A disponibilização dos dados relativos à prestação de serviços públicos é garantida pelo Artigo nº 29, desde que respeitada as normas de proteção de dados. O artigo também estabelece demais condições relativas à abertura de dados dos serviços públicos, enfatizando: o acesso em formato aberto e legível por máquina; permissão de uso irrestrito de todas as bases publicadas em formato aberto, semântica dos dados, qualidade e integridade; atualização periódica para atender às necessidades dos usuários; completude e granularidade.

Qualquer interessado pode solicitar a abertura de base de dados da Administração Pública, conforme artigo nº 30 da Lei de Governo Digital. Os prazos e procedimentos de abertura seguem as orientações da Lei de Acesso à Informação.

1.4.2. Compartilhamento de dados no setor público

No que se refere ao compartilhamento de dados, em 2019, o Decreto nº 10.046[36] dispôs sobre a governança no compartilhamento de dados no âmbito da administração pública federal e instituiu o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. O artigo nº 11 do Decreto determina que o compartilhamento de dados dispensa autorização prévia do gestor de dados e é realizado através dos canais existentes de promoção de dados abertos, no caso dos dados que podem ser amplamente compartilhados. Além disso, a Controladoria-Geral da União e o Comitê Interministerial de Governança de Dados poderiam recomendar a abertura de dados compartilhados. As informações sobre os dados advindos do compartilhamento também devem ser catalogadas no Portal Brasileiro de Dados Abertos.

Atendendo às ações ajuizadas sobre a alegação de que a governança compartilhada de dados possivelmente facilitaria vigilância massiva e

36 BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. Disponível em: https://is.gd/5lL3ux.

controle inconstitucional do Estado, o Supremo Tribunal Federal[37] determinou novos parâmetros para o compartilhamento de dados entre órgãos e entidades do governo federal e limitações à atuação do Comitê Central de Governança de Dados.

Assim, o compartilhamento tornou-se mais rigoroso, exigindo o fornecimento de informações claras e atualizadas sobre previsão legal, finalidade e práticas utilizadas. Os registros de acesso às bases e novas inclusões de dados devem ser registrados e controlados. O uso indevido de dados por agentes públicos pode resultar em responsabilização por ato de improbidade administrativa. A estrutura do Comitê deve ser alterada visando o fortalecimento dos mecanismos de proteção de dados pessoais.

1.4.3. Política de Transparência e Acesso à Informação do Governo Federal

Recentemente, a Lei de Acesso à Informação passou por mudanças com a publicação de três decretos. O decreto nº 11.527/2023 altera o sigilo das informações de agentes públicos, cujas informações não pessoais podem ser divulgadas mediante pedido de acesso. O decreto nº 11.529/2023 cria o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal, a fim de consolidar as diretrizes e princípios de transparência em todas as ações governamentais.

O decreto nº 11.529/2023 também cria a Política de Transparência e Acesso à Informação da Administração Pública Federal. A nova Política exige a observância dos princípios da Política de Dados Abertos do Governo Federal e da Política de Governo Aberto. A política reforça a competência da Controladoria-Geral da União para manutenção da transparência passiva através do Portal Brasileiro de dados abertos, e a obrigação pela manutenção do inventário de dados e catalogação de dados atualizados no referido Portal.

Há também princípios de observância da publicidade baseados em recomendações e boas práticas já formalizadas pelos princípios de dados

37 Informações sobre o processo de julgamento, decisão e ações estão disponíveis em: https://is.gd/Xi3RJg.

abertos, tais como, foco no cidadão para definição das prioridades para a abertura de dados; e outros princípios baseados nos incentivos de uso de tecnologias para disseminação e incentivo ao uso de dados, e o compartilhamento de informações visando pesquisa, inovação, geração de negócios e desenvolvimento econômico e social.

Apesar do novo texto que se refere ao estímulo à abertura de dados e uso de dados, não foram definidas medidas para viabilizar de fato o reuso dos dados.

No que se refere à solicitação de informações que possam conter dados pessoais, cabe aos órgãos e às entidades responsáveis pelo tratamento dos pedidos de informação, a indicação da existência de dados pessoais ou de informações protegidas por outras hipóteses legais de sigilo.

1.4.4. Abertura de dados governamentais em estados e municípios

Desde a Lei de Acesso à Informação, seguido do quadro político de regulatório de abertura de governo e dados abertos, estados e municípios implementaram estratégias próprias.

De modo geral, as leis estaduais e iniciativas municipais foram implementadas para atender os artigos 7º e 8º da LAI, que estabeleceu a obrigação das instituições em disponibilizar dados em formato aberto.

Os estados Minas Gerais,[38] Pernambuco,[39] Maranhão,[40] Pará,[41] Rio de Janeiro[42] e Bahia[43] estabeleceram resoluções, diretrizes ou leis específicas a fim de atender às exigências da LAI no âmbito da administração estadual, incluindo a criação de planos de abertura de dados e transparência de informação.

38 Disponível em: https://is.gd/6mNfEX

39 Disponível em: https://is.gd/4Jx3p9

40 Disponível em: https://is.gd/d3nIZf

41 Disponível em: https://is.gd/iJDBUR

42 Disponível em: https://is.gd/uY2HHg

43 Disponível em: https://is.gd/u1bqTi

Já os estados de Goiás,[44] São Paulo,[45] Espírito Santo,[46] Rondônia,[47] Mato Grosso,[48] Mato Grosso do Sul,[49] Distrito Federal[50] e Rio de Grande Sul[51] instituíram a política própria de dados abertos da Administração Pública. Nestes casos, o Plano de Dados Abertos tem sido uma boa prática de governança da política de dados abertos no nível estadual.

No que se refere aos municípios, há uma diversidade de políticas, regulações e parcerias delineadas nos últimos anos. A cidade de São Paulo é uma unidade subnacional da *Open Government Partnership* desde 2016.[52] Além disso, programas recentes da CGU, tais como o "Time Brasil para o Governo Aberto",[53] têm o objetivo de apoiar a elaboração de Planos de Ação de Governo Aberto para as unidades da federação e órgãos da Administração Pública em geral, a fim de disseminar a adoção de política, programas de transparência, corrupção e acesso à informação, além da participação social.

Apesar das iniciativas relacionadas à abertura de dados, e num sentido amplo, ao governo aberto, as ações endereçadas pela CGU são recomendadas, cuja adesão é voluntária, e não garantem ampla implementação. A CGU, como responsável pela Política de Dados Abertos e pelos Planos Nacionais de Governo Aberto, não determinou boas práticas a serem seguidas pelos entes federativos capazes de assegurar a publicidade dos dados como regra e o sigilo como exceção.

Ainda que o Plano de Dados Abertos seja a principal ferramenta para execução e manutenção da abertura de dados, este instrumento não de-

44 Disponível em: https://is.gd/ykBR52

45 Disponível em: https://is.gd/Ld0iVY

46 Disponível em: https://is.gd/PW72hv

47 Disponível em: https://is.gd/rovn3P

48 Disponível em: https://is.gd/vp6n6t

49 Disponível em: https://is.gd/5KCkLJ

50 Disponível em: https://is.gd/dlu8IH

51 Disponível em: https://is.gd/4IW8kE

52 Disponível em: https://is.gd/tHo9Ic

53 Disponível em: https://is.gd/fi6fa5

termina práticas efetivas de tratamento de dados pessoais, e medidas de segurança da informação.

1.5 Resumo de normas

- A Parceria para Governo Aberto (OGP), celebrada em setembro de 2011.
- A Lei nº 12.527, de 18 de novembro de 2011, a Lei de Acesso à Informação (LAI), que 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.
- A Instrução Normativa nº 4, de 12 de abril de 2012, que institui a Infraestrutura Nacional de Dados Abertos (INDA), que estabelece conceitos de dado, informação, dado público, formato aberto, licença aberta, dados abertos e metadados.
- A Portaria nº 92, de 24 de dezembro de 2014, que institui a arquitetura e-PING (Padrões de Interoperabilidade de Governo Eletrônico), definindo um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de serviços de Governo Eletrônico.
- O Decreto nº 8.777, de 11 de maio de 2016, institui a Política de Dados Abertos do Poder Executivo Federal.
- A Resolução nº 3, de 13 de outubro de 2017, do Comitê Gestor da Infraestrutura Nacional de Dados Abertos (INDA), aprova procedimentos complementares e diretrizes para elaboração de publicação de Planos de Dados Abertos.
- O Decreto nº 10.160, de 9 de dezembro de 2019, institui a Política Nacional de Governo Aberto e o Comitê Interministerial de Governo Aberto.
- O Manual de Elaboração de Planos de Dados Abertos é atualizado pela Controladoria-Geral da União, e inclui recomendações superficiais sobre o tratamento de dados, que possuem restrições

de sigilo e privacidade do cidadão, sem referência direta à Lei Geral de Proteção de Dados Pessoais.

- A Estratégia Brasileira de Governança Eletrônica, a Estratégia Brasileira de Transformação Digital (E-Digital) e a Estratégia de Governo Digital incluem a abertura de dados como objetivos para promoção da transparência e controle social.
- A Lei de Governo Digital garante a disponibilidade em formato aberto dos dados relativos à prestação dos serviços públicos.

TEMÁTICA	INICIATIVA	ESCOPO
Governança de dados	Legislação de Governança de Dados e Interoperabilidade	Decreto nº 10.046 de 2019 cria a governança no compartilhamento de dados no âmbito da Administração Pública federal, estabelecendo regras e diretrizes para compartilhamento de dados entre órgãos e entidades. Cria o Cadastro da Base do Cidadão como base integradora e de troca de dados que serve de base referencial de informações sobre o cidadão para os órgãos e entidades do Poder Executivo Federal. O Comitê Central de Governança de Dados é responsável pelas diretrizes para a categorização e compartilhamento de todos os dados.[54]
Interoperabilidade de dados	Padrões de Interoperabilidade de Governo Eletrônico	Padrões de Interoperabilidade de Governo Eletrônico definem diretrizes sobre formatos abertos para uso de Tecnologia da Informação e Comunicação em serviços governamentais no item 3.1. sobre Especificações Técnicas para Meios de Publicação.[55]

54 Disponível em: https://www.gov.br/governodigital/pt-br/legislacao/legislacao-governanca-de-dados-e-interoperabilidade

55 Disponível em: http://eping.governoeletronico.gov.br/

Estrutura de dados abertos	Infraestrutura Nacional de Dados Abertos	A Infraestrutura Nacional de Dados Abertos (INDA) apoia a definição de um conjunto de padrões, tecnologias, procedimentos e mecanismos de controle necessários para atender às condições de disseminação e compartilhamento de dados e informações públicas. A infraestrutura foi instituída pelo primeiro Plano de Ação Nacional de Governo Aberto.[56]
Coordenação de dados abertos	Controladoria-Geral da União	Em 2019, a Controladoria-Geral da União assumiu a gestão da Política de Dados Abertos, criando painéis de monitoramento e acompanhamento da disponibilização das bases de dados abertos governamentais. A disponibilidade e cronograma da abertura das bases pode ser acompanhado através do Painel de Monitoramento de Dados Abertos.[57]
Política de dados abertos	Política de Dados Abertos do Governo Federal	Em 2016, foi instituída a Política de Dados Abertos do Governo Federal que define regras para a disponibilização de dados abertos governamentais no âmbito do Poder Executivo Federal. A política consiste em uma série de documentos normativos, de planejamento e de orientação.[58]

56 Disponível em: https://dados.gov.br/pagina/instrucao-normativa-da-inda

57 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9903.htm; http://paineis.cgu.gov.br/dadosabertos/index.htm

58 Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=DEC&numero=8777&ano=2016&ato=c90ATSq1EeZpWT24e

Orientações técnicas	Plano de dados abertos	Em 2017, a Resolução nº 3 definiu a criação de Planos de Dados Abertos para apoiar a publicação e catalogação de dados. A gestão da publicação de dados está definida no Plano de Dados Abertos, que é regulado por resoluções do Comitê Gestor de Infraestrutura de Dados Abertos. O plano define as etapas do projeto de abertura de dados, determina mecanismos de participação social, estabelece um cronograma de catalogação de dados no Portal Brasileiro de Dados Abertos. Após a aprovação do plano, a agência deve publicar os dados em uma seção de Acesso à Informação, conforme artigo 6º da Resolução nº 3 do Comitê Gestor do INDA, vinculado ao Portal Brasileiro de Dados Abertos.[59]
Estratégias governamentais	Estratégia de Governo Digital	Estratégia de Governo Digital que busca implementar um barramento de interoperabilidade de dados que facilite a integração e reutilização dessas informações para fornecer serviços aos cidadãos.[60]
Estratégias governamentais	Estratégia Brasileira de Transformação Digital 2018-2022/ 2022-2026	De um modo geral as estratégias visam aprimorar a Política de Dados Abertos. A estratégia mais recente enfatiza a necessidade de melhorias na interoperabilidade dos dados governamentais e criação de uma *datalake* para apoiar a formulação de políticas públicas.[61]

59 Disponível em: https://www.gov.br/governodigital/pt-br/legislacao/resolucaocginda22432017 pdf.pdf.

60 Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10332.htm#art12.

61 Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/eDigital.pdf; https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf.

Portal de dados abertos	Portal Brasileiro de Dados Abertos	O Portal Brasileiro de Dados Abertos é a principal plataforma de coleta e disponibilização de dados governamentais abertos.[62]
Orientações técnicas	Manual para o Desenvolvimento de Planos de Dados Abertos	O principal documento de orientação para elaboração de um Plano de Dados Abertos é o Manual para Elaboração dos planos, que detalha os procedimentos para se produzir um plano.[63]
Orientações técnicas para o Portal	Manual de Catalogação no Portal Brasileiro de Dados Abertos	Manual fornece instruções para publicação no Portal Brasileiro de Dados Abertos seguindo as recomendações em debate.[64]

1.6 Boas práticas para abertura de dados governamentais responsável, justa e inclusiva

Como detalhado acima, desde o estabelecimento da obrigatoriedade de disponibilização de informações atualizadas e em formato aberto, o governo federal vem ampliando a normatização a respeito dos dados abertos. Com a Infraestrutura Nacional de Dados Abertos e a Política de Dados Abertos do Governo Federal, as ferramentas de planejamento, execução e monitoramento de dados, tais como o Plano de Dados Abertos, tornaram-se práticas relevantes no setor público.

62 Disponível em: https://wiki.dados.gov.br/; https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10160.htm#art13.

63 Disponível em: https://wiki-dados-h.cgu.gov.br/GetFile.aspx?File=%2fManuais%2fPlanos%20de%20Dados%20Abertos%2f2018%2fManual%20de%20Elaboracao%20de%20Planos%20de%20Dados%20Abertos.pdf.

64 Disponível em: https://wiki.dados.gov.br/GetFile.aspx?File=%2fManuais%2fManual-de-Catalogo%C3%A7%C3%A3o-v1.0.pdf.

Entretanto, boa parte das diretivas e recomendações nacionais para dados abertos foram elaboradas em um período de anos seguindo a implementação da LAI. Por outro lado, a LGPD é ainda extremamente recente, de forma que ainda não foram incorporadas recomendações que considerem as normas para tratamento de dados pessoais. Boas práticas sobre o processo de abertura de dados e técnicas para garantia da privacidade carecem de orientação.

As consequências de compartilhamento de dados pessoais já receberam atenção até mesmo da imprensa,[65] apontando a necessidade de balancear os dois objetivos. Um exemplo é a possível identificação das pessoas a quem os dados se referem mesmo após um processo de anonimização.[66] É necessário estar atento que não há medidas que eliminem a possibilidade de identificação, mas opções para reduzir os riscos, os quais devem ser ponderados a partir dos fins, e a relevância dos dados a serem publicizados.

Dentre as práticas seminais, um relatório feito para o gabinete de governo do Reino Unido ainda em 2011[67] publicou recomendações para lidar com eventuais problemas de privacidade e transparência no governo. Estas são as recomendações elencadas:

- Criar um conselho ou comitê de transparência capaz de envolver e representar os interesses relativos à privacidade;
- Estabelecer paradigma técnico para balizar as ações;
- Determinar controles de consulta, divulgação e acesso;
- Criar um registro de ativos de dados e painéis setoriais;
- Criar um procedimento de pré-lançamento de dados abertos pode apoiar e garantir o respeito à privacidade;
- Estabelecer um modelo de riscos;
- Elaborar um manual de boas práticas e pesquisas atualizadas sobre a transparência;
- Estabelecer um padrão de revisão e controle;
- Estabelecer um procedimento de identificação de danos e soluções;

65 Disponível em: https://is.gd/XhiSmZ.

66 Exemplo de estudo a partir da divulgação de mapeamentos genéticos: https://is.gd/lnhzfu.

67 Disponível em: https://is.gd/mB3nIw.

- Usar a publicização dos dados para aumentar a conscientização sobre a responsabilidade da proteção de dados;
- Investigar as vulnerabilidades dos bancos de dados;
- Ser transparente sobre o uso de técnicas de anonimização.

Em seguida, as normas passaram a também ter a importância de comunicar ao público a tomada de decisão e eventuais processamentos (como anonimização) que sejam aplicados aos dados. Isso é importante para que quaisquer pesquisas ou aplicações desenvolvidas sobre o conjunto de dados possam considerar as limitações inerentes ao conjunto, e também aquelas impostas para sua divulgação.

De um modo geral, recomendações incorporaram visões sobre a proteção de dados e a abertura de dados como um processo decisório, cuja transparência é a regra.

A divulgação de dados abertos granulares, a partir de dados que podem conter informações confidenciais, resulta no dilema da ponderação entre o benefício da publicação e o risco. Os dados granulares são interessantes e importantes devido à potencial utilidade, no entanto, por conter informações detalhadas que desafiam a privacidade. Assim, quanto mais granulares, mais valiosos são os dados, porém, à medida que dados abertos possam envolver riscos à privacidade, tornam-se ineficazes. Portanto, é primordial desenvolver uma abordagem capaz de equilibrar esses dilemas.

O desenvolvimento do arcabouço político regulatório no Brasil se deu de forma oposta, tendo o processo de divulgação de dados abertos sendo estabelecido primeiro, e a normatização de proteção de dados sendo superveniente. Assim, não se pode deixar que o acesso à informação, bem como a disponibilização de dados em formato aberto, seja limitado pelo uso indevido dos recursos legais relativos à proteção de dados, como foi a prática em alguns casos recentes da Administração Pública do Executivo Federal.[68]

Dessa forma, é interessante, para que o acesso à informação, dados abertos governamentais e proteção de dados sejam contemplados, a integração entre os responsáveis pela publicação de dados e os responsáveis pela proteção de dados em órgãos públicos. Isso quer dizer que a tomada

68 Disponível em: https://is.gd/VFJpb0. Acesso em: 20 dez. 2022.

de decisão sobre abertura de dados pode atender às restrições para tratamento de dados pessoais, mas ponderando também o interesse público de abertura de dados.

A participação social e a transparência dos atos devem pautar o processo decisório, desde o processo de escolha, divulgação de *datasets*, até a definição das melhores técnicas de anonimização de dados.

No que tange à abertura de dados no nível local, as recomendações e boas práticas elaboradas pelo Berkman Klein Center (Green *et al*., 2017) são similares, destacando-se a: *i)* condução de análise de risco *vs* benefício para abertura de dados; *ii)* consideração da privacidade em todas as etapas de coleta e tratamento de dados; *iii)* criação de processos para avaliar riscos e benefícios na gestão de dados; e *iv)* e a manutenção do foco na participação social na gestão de dados.

No entanto, o acesso à informação e a gestão e abertura de dados possui desafios para além da compatibilização com a privacidade e as medidas de proteção. Dados de diferentes domínios revelam desafios específicos sobre a abertura e a divulgação de informações sensíveis, tais como dados de mobilidade,[69] dados educacionais e dados de saúde.[70]

Finalmente, a gestão de dados que combina a abertura de dados e a proteção de dados, conforme recomendações supracitadas, tem o potencial de criar a padronização apropriada dos dados, de modo que os dados não criem "jardins murados" nos quais governos e políticas se tornam dependentes. Dados abertos padronizados[71] permitem que os governos ou políticas comuniquem-se através destes ativos. A determinação de padrões permite desde a divulgação até a coleta de dados, estabelecendo um registro central, público, de dados estruturados que facilitam a atualização, auditoria, qualidade e confiabilidade dos dados.

---

69 Exemplos sobre os desafios da abertura de dados de mobilidade e padronização dos dados podem ser encontrados em: https://is.gd/yOjjzh. Acesso em: 20 dez. 2022.

70 Lições aprendidas das crises humanitárias e a proteção de dados e privacidade durante a pandemia do Covid 19. Disponível em: https://is.gd/Q6KruD.

71 Para obter exemplos sobre a padronização de dados abertos, veja o padrão de propriedade benéfica. Disponível em: https://is.gd/RUbR3b. Acesso em: 20 dez. 2022.

1.6.1. Técnicas e métodos para anonimização de dados

A iniciativa de dados abertos apresenta múltiplas oportunidades com a democratização das informações, no entanto, conforme salientado, as iniciativas podem representar ameaças à privacidade dos indivíduos. Através do uso de técnicas e processos apropriados, os dados podem se aderir aos regulamentos de proteção de dados, protegendo a privacidade e evitando danos.

Primeiramente, a aplicação de técnicas de anonimização é um processo composto por etapas que devem ser adaptadas à abertura de dados. Segundo, que as técnicas de anonimização devem obedecer às orientações da Lei Geral de Proteção de Dados. Isso quer dizer que o sucesso relativo da abertura de dados a partir de dados pessoais e sensíveis depende da combinação do arcabouço político e jurídico.

A literatura técnica também tem tentado oferecer soluções para a compatibilização da divulgação de dados, com a proteção de dados pessoais. Isso se dá principalmente pelo desenvolvimento de métodos e técnicas para anonimização dos dados, e na maioria dos casos várias técnicas podem ser associadas para reduzir o risco de reidentificação. Importante destacar que a anonimização não é isenta de riscos, por isso, as técnicas devem ser acompanhadas de medidas de mitigação de riscos, até que a ameaça à privacidade seja mínima.

Os processos de anonimização têm como objetivo retirar dos dados informações que possam ser utilizadas para identificar o sujeito. Por exemplo, informações que sejam de fato identificadoras, como RG e CPF, por óbvio não podem ser divulgadas sem autorização legal explícita. Contudo, outros conjuntos de informações, em especial se combinadas com conhecimento de pertencerem a uma mesma pessoa, podem ser utilizados para identificação.

A escolha por uma determinada técnica ou conjunto delas depende do objetivo e uso pretendido dos dados, pois isso acarretará avaliação de impacto da privacidade e nível de risco característico do conjunto de dados. No geral, as técnicas[72] e medidas de segurança comumente utilizadas são: supressão, randomização, generalização e pseudoanonimização. A diferença entre as técnicas é o quanto será mantido das informações, e,

72 Essas técnicas foram discutidas e apresentadas pelo Grupo de Trabalho de Proteção de Dados da União Europeia. Disponível em: https://is.gd/N3Rfwq.

consequentemente, o quanto outros atores poderão fazer uso dos dados divulgados e o risco de reidentificação.

- Técnicas de supressão removem dos conjuntos de dados qualquer característica identificadora, como o nome do indivíduo. No caso da aplicação da supressão recomenda-se a avaliação da utilidade dos dados, uma vez que supressões excessivas podem excluir dados primordiais para realização de objetivos.
- Técnicas de randomização alteram os dados através de ruídos ou embaralhando valores, sem, contudo, alterar as características e padrões no conjunto de dados. A randomização em si dificulta inferências sobre os indivíduos contidos no conjunto de dados. Técnicas adicionais podem ser utilizadas para garantir a não identificação.
- Técnicas de generalização ou diluição modificam a escala ou ordem de grandeza dos dados. Essas técnicas são apropriadas para evitar a reidentificação, no entanto, não efetiva a anonimização. Para impedir a vinculação ou inferência, são necessárias abordagens quantitativas específicas e sofisticadas.
- Pseudoanonimização é uma medida de segurança que consiste em substituir um identificador por um pseudônimo. A substituição reduz a reidentificação direta, mas não garante as inferências indiretas através de outras informações. A criptografia, *hashing* e tokenização são técnicas de pseudoanonimização.

Com relação à generalização, os dados são agregados. Por isso, deixa-se de ter dados na unidade de análise de cada indivíduo, gerando-se estatísticas para grupos. Por consequência, o risco de identificação é extremamente reduzido.[73] Por outro lado, perde-se também a possibilidade de gerar novas análises a partir dos dados individuais. Não será possível criar nenhuma nova estatística que dependa dos dados individualizados, ficando os atores que usam os dados restritos ao que é publicado pelo órgão.

73 Contudo, ainda não é zerado. Por exemplo, podemos agregar dados de todos os alunos de uma turma. No fim, exibimos a agregação por gênero. Caso determinado gênero possua apenas uma pessoa, seria possível a identificação de seus dados.

As demais técnicas consistem em diferentes alternativas de manter a unidade de dados disponíveis, mas removendo ou alterando informações para que não haja identificação dos indivíduos. No processo de anonimização, no geral, não estamos preocupados em manter relações entre múltiplas observações da mesma pessoa. Apenas são removidas variáveis que possam ser utilizadas para identificação.

Por outro lado, a identificação do mesmo sujeito pode ser de crucial importância para compreensão do cenário. Por exemplo, se queremos entender e avaliar o impacto de uma política pública de educação, é essencial analisarmos a evolução dos alunos, afinal, o desempenho em um ano isolado é muito pouco informativo se comparado à sua evolução em todo o período escolar.

Nesses casos, utilizamos técnicas de pseudoanonimização. Para isso, são criados valores que permitem identificar múltiplas observações de um mesmo indivíduo. Contudo, essas técnicas aumentam o risco de identificação do indivíduo.

1.6.2. Um guia dos procedimentos de anonimização

A tomada de decisão sobre técnicas de anonimização é um processo iniciado quando os dados são coletados, uma vez que as organizações devem considerar as implicações éticas e o efeito sobre o uso dos dados. Assim, quando os bancos de dados são criados, o estudo sobre os procedimentos de anonimização devem estar em conformidade com o quadro de proteção de dados pessoais, a fim de analisar riscos de reidentificação, e estabelecer medidas mitigatórias.

A avaliação de impacto na proteção de dados (ODI, 2018-2019) é o procedimento que descreve a natureza, escopo, contexto e finalidade do processamento; identificação e avaliação de riscos para os indivíduos, e projeta medidas para mitigação.

Recomenda-se os seguintes procedimentos de anonimização (Open Data Institute, 2020):

- Remoção dos identificadores óbvios;
- Identificação dos dados que permitem a identificação de forma única ou de um único indivíduo, os seja, pseudoidentificadores, e que só podem ser divulgados com medidas de proteção;

- Avaliar se os dados restantes contêm informações sobre os indivíduos, ou se podem ser utilizados para reconstruir pseudoidentificadores, ou permitir inferências sobre indivíduos a partir da base de dados;
- Definir medidas que possam reduzir os riscos de privacidade potencialmente identificados;
- Avaliar o resultado da anonimização antes da divulgação dos dados para compreender a eficácia e impacto. Esta avaliação pode apoiar o ajuste de parâmetros da anonimização;
- Os dados devem ser submetidos a um teste de avaliação regularmente, inclusive depois da abertura, à medida que se aprende sobre os novos bancos de dados;
- A metodologia de anonimização deve ser compartilhada com as partes interessadas, e publicada para o público geral a fim de garantir a transparência e supervisão.

As recomendações institucionais[74] para abertura de dados e anonimização estão sintetizadas no quadro abaixo.

1. Crie Diretrizes de Dados Abertos	Elaborar diretrizes de dados abertos é uma oportunidade de definir o compromisso do setor público com a publicação e compartilhamento de dados. O estabelecimento de uma política expressa pelas autoridades competentes é o desejável. No entanto, a determinação de diretrizes, como um documento aplicável aos diversos setores públicos, ajudará o governo, de um modo geral, a direcionar a abertura de dados com foco em benefícios de múltiplos atores.	A política ou as diretrizes devem minimamente:
		Definir dados abertos;
		Ter uma declaração geral de princípios que oriente a disponibilização, compartilhamento e reuso de dados em consonância com a segurança da informação e proteção de dados;
		Ter inventário de dados e tipos de dados coletados e gerados pela organização;
		Ter aderência às políticas e legislações nacionais e/ou estaduais.

74 Recomendações gerais foram obtidas a partir de Open Data Institute (2020, 2019, 2018) e Guia do Governo da Irlanda (Deirdre Lee, 2021).

2. Estabeleça uma base legal, administrativa e ética	Estabeleça a base legal e ética para lidar com os dados de categorias especiais.	A base deve apoiar o entendimento do que são os dados pessoais;
		A base legal deve apresentar garantias para o anonimato;
		A base legal deve considerar as implicações éticas relativas à coleta, uso e compartilhamento de dados;
		A base administrativa deve subsidiar a criação de um Escritório de Dados para trabalhar com departamentos e outras funções governamentais relativas aos dados;
		A análise ética deve incluir questões sobre as limitações e vieses dos dados, e como isso pode afetar grupos específicos;
		A base legal e ética deve considerar as técnicas de anonimização como medidas que auxiliam as organizações públicas no cumprimento das obrigações de proteção e acesso e disponibilização de informações.

3. Inclua e engaje as partes nas diretrizes	As diretrizes com um plano de ação devem cobrir o compromisso do governo em publicar, compartilhar e estimular o consumo e reuso de dados conectados a terceiros.	As diretrizes devem apoiar as partes internas das organizações do setor público na identificação de prioridade, medidas de compliance e sustentabilidade da iniciativa;
		As diretrizes devem apoiar as partes externas a compreender como ao setor público determina e mantém a abertura de dados, e como serão envolvidas ao longo do desenvolvimento da iniciativa;
		Envolva especialistas e cidadãos na definição e aplicação das técnicas de anonimização dos dados;
		Faça um pré-lançamento para um grupo limitado de indivíduos antes de abrir os dados, isso ajudará a fazer uma avaliação de impacto na privacidade.
4. Estabeleça diretrizes concretas e essenciais	Estabeleça as medidas internas de identificação, revisão e liberação de dados;	
	Defina seus objetivos, mesmo que para projetos específicos de abertura, pois isso apoiará a decisão sobre a medida da anonimização e manutenção da utilidade dos dados;	
	Estabeleça medidas internas e externas relativas à privacidade, de modo a garantir que as informações pessoais não sejam divulgadas, estabelecendo medidas de mitigação e impacto, inclusive para os padrões de anonimização;	
	Determine as abordagens de anonimização e licenciamento de dados e direitos e reutilização;	
	Faça um pré-teste como medida de avaliação dos parâmetros de anonimização.	

5. Realize uma auditoria interna de dados	A auditoria é o processo de inventariamento e catalogação dos dados que estão sendo criados e mantidos na organização. A auditoria é importante para adequar o compartilhamento interno de dados e a publicização como dados abertos. O inventário de dados pode ser disponibilizado publicamente, assim como seus progressos.	As auditorias devem ser regulares e seguir as diretrizes de orientação de abertura e publicação de dados;
		O inventário deve identificar o conjunto de dados que devem ser publicados como dados abertos;
		O inventário deve identificar o conjunto de dados que deve ser priorizado;
		O inventário deve identificar o conjunto de dados que deve ser gerenciado num ambiente controlado, como no caso dos dados de categorias especiais, sujeitos às avaliações de impacto.
6. Crie um roteiro de publicação de dados	O roteiro de publicação de dados apoia a definição de quais conjuntos de dados devem ser priorizados a partir do inventário de dados. O editor e publicador de dados pode definir um cronograma de publicação.	Estabeleça um cronograma de revisão dos padrões de coleta, armazenamento, processamento e anonimização, compartilhamento de dados;
		O cronograma de publicação é a primeira etapa de um roteiro de publicação de dados abertos, que permite estabelecer a revisão e atualização regular, estabelecendo metas de publicação;
		O cronograma deve incluir as etapas de pré-teste dos processamentos de anonimização, revisão dos padrões e manutenção da metodologia.

7. Realizar um estudo de avaliação de impacto, determinando as medidas de intervenção	Com o objetivo de garantir a redução de riscos da abertura de dados que possam conter informações sensíveis, o editor e publicador de dados pode realizar um estudo com o apoio da Comissão de Governança de Dados. Sugere-se que um estudo de impacto deve ser composto de determinadas medidas:	Agrupamento de dados sensíveis ou confidenciais através de categorias;
		As categorias devem ser gerenciais e baseadas no nível de gravidade e sensibilidade;
		Tomar as medidas adequadas relativas aos dados sinalizados em nível alto de gravidade e sensibilidade;
		Identificar quais as características do conjunto de dados podem ser usadas para identificação e quais representam uma ameaça em potencial, como pseudoidentificadores ou inferências;
		Rotular as ameaças e definir o grau dos riscos, isso será a base para avaliação de impacto da privacidade;
		Produzir um relatório sobre os procedimentos e a metodologia para mascarar os dados e as diretrizes de suporte a serem adotados pelas partes interessadas e Comissão.
8. Promova a transparência como regra em todas as ações	Todas as ações internas e externas devem ser transparentes, de modo que os processos possam ser revisados continuamente, seja com base no feedback das partes, seja nas lições aprendidas;	
	Disponibilize a metodologia de anonimização e um cronograma de revisão dos parâmetros de anonimização;	
	Promova consultas públicas, formulários e enquetes;	
	Disponibilize dicionários de dados, glossários, relatórios de avaliação de impacto.	

9. Apoie o estabelecimento de uma Comissão de Governança de Dados Sustentável	A criação da Comissão de Governança de Dados Sustentável, formada por servidores públicos e partes interessadas, deve apoiar a abertura de dados, principalmente de dados que possam conter informações pessoais, e também o compartilhamento de dados pessoais, de forma justa, segura e transparente.	A Comissão pode:
		Apoiar o setor público na adequação à legislação;
		Apoiar o setor público na fundamentação sobre o compartilhamento de dados e processamento de dados pessoais;
		Identificar as informações realmente necessárias para o objetivo do compartilhamento;
		Identificar potenciais riscos que o compartilhamento possa representar;
		Analisar e consolidar os parâmetros de anonimização dos dados pessoais;
		Debater e consolidar as medidas de segurança e mitigação de riscos;
		Garantir a transparência, publicização e participação social em todo o processo de abertura de dados, incluindo processamentos e compartilhamentos;
		Apoiar às atividades do Escritório de Dados.

Parte II
A proteção de dados pessoais no Brasil

Resumo em tópicos

Esta parte analisa a proteção de dados pessoais no Brasil abordando os seguintes assuntos:

- Estabelecimento da Lei Geral de Proteção de Dados (LGPD) para harmonizar o regime de proteção de dados pessoais no Brasil;
- Estados brasileiros, especialmente após a LGPD, têm produzido normas que organizam a governança de dados pessoais, criando corpos de governança novos e/ou se aproveitam dos já existentes;
- Há sobreposição entre competências de estruturas institucionais pré-existentes no eixo acesso à informação — dados pessoais — segurança cibernética, de modo que um esforço de harmonização é necessário para tirar proveito de possíveis sinergias;
- A organização do papel do Encarregado é um ponto de considerável variação nas estruturas criadas nos estados. O papel do Encarregado deve estar cercado de garantias de independência e dotado dos recursos e acesso necessários;
- Já há uma extensa produção de guias e recomendações, inclusive oficiais, sobre boas práticas em se tratando de proteção de dados pessoais. Emprega-se, aqui, uma divisão esquemática baseada em uma visão do ciclo de vida do dado pessoal, que agrupa ações em oito chaves temáticas apresentadas de forma resumida.[75]

75 Desenvolvida pelos autores com base em busca documental detalhada na própria ferramenta. Disponível em: https://is.gd/XcagcD.

Introdução

A proteção de dados pessoais no Brasil foi tratada de forma fragmentada por algum tempo, com disposições relevantes contidas em leis como o Marco Civil da Internet e o Código de Defesa do Consumidor. Com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), no entanto, erigiu-se referência unívoca e paradigmática sobre o tema no ordenamento jurídico nacional. Assim, falar em cuidados relacionados à proteção de dados pessoais no Brasil passa necessariamente por compreender os ditames da LGPD e sua forma de aplicação.

Esta aplicação, no entanto, passa pela pormenorização dos modos de implementação da lei — em outras palavras, pela transformação do regime geral da LGPD em rotinas, instituições e estruturas — bem como em uma cultura de proteção de dados pessoais. Em se tratando especificamente de entidades públicas que decidem a respeito do acesso a dados de interesse público, como é o ponto de convergência sob análise neste trabalho, isto se traduz em atos normativos e em estruturas de governança que dão concretude às determinações da lei, recomendações de boas práticas alinhadas com a lei e representam a sua incorporação às rotinas destas entidades.

Assim, esta seção enfoca dois esforços distintos, porém relacionados, de mapeamento e análise. Primeiro, um mapeamento das normativas estaduais que pretendem estruturar os sistemas de proteção de dados, respondendo ao ímpeto inaugurado pela LGPD. Em segundo lugar, uma sistematização de boas práticas derivadas de extensa documentação — com particular destaque a publicações oficiais da Autoridade Nacional de Proteção de Dados (ANPD) e órgãos governamentais relacionados à segurança da informação, digitalização para a adequação à LGPD.

Pretende-se, com estes dois componentes, prover linhas-guia para a reflexão a respeito de processos de abertura de dados que respeitem a proteção de dados pessoais, com enfoque prático e pragmático.

1 A harmonização de um sistema fragmentado de proteção de dados pessoais no Brasil

Em agosto de 2018, o Brasil adotou sua nova Lei Geral de Proteção de Dados nº 13.709/2018, mais conhecida pelo acrônimo "LGPD", que começou

a entrar em vigor em setembro de 2020 e passou a vigorar em agosto de 2021.[76] Antes da adoção da LGPD, o Brasil tinha muitas regulamentações setoriais em nível federal que regulavam direta e indiretamente a proteção de dados pessoais, mas muitas vezes eram confusas, redundantes ou contraditórias.[77]

A proteção de dados era parcial e incoerentemente abordada na legislação esparsa, impulsionada pela lógica da regulação setorial de domínios específicos, em vez de se basear na proteção integral da personalidade através da proteção dos dados pessoais.[78] Por exemplo, a Lei de Habeas Data definiu o procedimento para o exercício do direito fundamental de acesso às informações pessoais armazenadas em banco de dados público previsto no art. 5º da Constituição Federal, enquanto o art. 43 do Código de Defesa do Consumidor estabeleceu o direito de acesso aos dados pessoais dos consumidores, sem definir um procedimento para viabilizar o acesso. A Lei do Cadastro Positivo definiu a capacidade das instituições financeiras de coletar informações do consumidor para fins de pontuação de crédito, enquanto o Marco Civil da Internet (MCI), proibiu a coleta de dados dos usuários da Internet, exceto mediante consentimento expresso, livre e informado do usuário ou conforme previsto em lei.[79]

Entretanto, disposições importantes, como a definição dos fundamentos legais para o processamento de dados, somente seriam definidas na legislação futura. Tal abordagem fragmentada e parcial criou notável incerteza jurídica. A LGPD tem como objetivo substituir ou complementar as regulamentações setoriais enormemente heterogêneas e fragmentadas que o Brasil promulgou nas últimas décadas. De fato, cerca de 40 leis e decretos federais regulamentavam direta e indiretamente a proteção de dados pessoais em diversos setores, antes da entrada em vigor da LGPD.

---

76 Veja 'A Lei Geral de Proteção de Dados – Versão em inglês não oficial' (Projeto CyberBRICS 2020). Disponível em: https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/.

77 Esta seção baseia-se na seção "Brazil: Towards the Harmonisation of a Fragmented System" de BELLI, Luca. New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a post-Western Model of Data Governance. Indian Journal of Law and Technology, 2023.

78 Ver DONEDA, D. Da privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados. 3. Ed. São Paulo: Thomson Reuters Brasil, 2021.

79 Ver art. 7.VII do Marco Civil da Internet (Lei Federal n. 12.965 de 2014). Disponível em: https://observatoriolegislativocele.com/en/brazil-law-12-965-civil-internet-framework-2014/.

Entre as principais leis federais que foram complementadas, atualizadas e esclarecidas pela LGPD se encontram:

- Portaria nº 852 da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos, de 28 de março de 2023, que define em pormenores o Programa de Privacidade e Segurança da Informação a ser adotado em órgãos e entidades da administração pública federal direta, autárquica e fundacional;
- A Lei Geral de Telecomunicações (Lei Federal nº 9.472 de 1997; Art. 3º, IX) que assegura aos consumidores o direito à privacidade nos serviços de telecomunicações;
- A Lei de Habeas Data (Lei nº 9.507/97);
- A Lei de Identificação Criminal (Lei Federal nº 12.037 de 2009);
- A Resolução nº 3/2009 do Comitê Gestor da Internet no Brasil (CGI.br), que estabelece princípios para garantir a privacidade e a proteção de dados sobre o uso da internet no Brasil, principalmente no que se refere às atividades desenvolvidas pelos provedores de serviços de internet;
- A Lei de Livre Acesso à Informação (Lei Federal nº 12.527/2011, especialmente no que se refere ao seu Art. 4 IV e Art. 31);
- O Marco Civil da Internet (Lei nº 12.965, de 2014);
- A Lei do Cadastro Positivo (Lei nº 12.414/2011) em conjunto com o Decreto nº 9.936/19 e a Resolução do Banco Central nº 4/737/19, regulamentando a criação e gestão de bases de dados contendo informações sobre o histórico de pagamentos e registro de transações de pessoas físicas e jurídicas, para a construção de score de crédito.[80]

É importante ressaltar que o processo que trouxe à elaboração da LGPD levou quase uma década, desde a proposta do primeiro Projeto

80 Uma visão detalhada das leis e regulamentos setoriais pode ser encontrada em Sato, L.; Bragium, Guilherme; Powell, Igor B.; Costa, Geórgia. Data Protection Laws and Regulations Brazil 2022-2023. ICLG. Disponível em: https://iclg.com/practice-areas/data-protection-laws-and-regulations/brazil.

de Lei oficial sobre a Proteção de Dados Pessoais e Privacidade.[81] Isso foi baseado em uma proposta de lei-modelo debatida no âmbito do grupo de trabalho do Mercosul (a organização econômica internacional composta por Argentina, Brasil, Paraguai e Uruguai) sobre comércio eletrônico.[82] O Ministério da Justiça abriu a primeira consulta pública sobre um projeto de lei de proteção de dados em 2010.[83]

O Projeto de Lei foi em grande parte moldado com base na Convenção 108 do Conselho da Europa e na Diretiva 95/46/CE da União Europeia (UE), que eram as principais referências legais na época e já incluíam algumas características típicas da legislação brasileira que foram mantidas até o texto final da LGPD, como a referência explícita a elementos centrais do direito do consumidor.

No entanto, durante os oito anos subsequentes que levaram à cristalização da LGPD, as disposições e a estrutura evoluíram enormemente, devido ao número muito elevado de contribuições diversas de stakeholders recebidas durante uma nova fase de consultas públicas. Isso inclui tanto um processo participativo organizado pelo Ministério da Justiça do Brasil quanto várias audiências no Congresso, de 2016 a 2018. Após a aprovação da LGPD, em agosto de 2018, o período de *vacatio legis*[84] anterior à sua entrada em vigor foi posteriormente prorrogado em múltiplas ocasiões, levando a uma situação de considerável incerteza jurídica.[85] A pandemia de COVID-19 trouxe mais confusão e tentativas de atrasar ainda mais a

81 O projeto original submetido a consulta pública em 2010, bem como os contributos recebidos duran te a primeira fase de consulta, podem ser consultados em: http://pensando.mj.gov.br/dadospessoais2011/files/2011/03/PL-Protecao-de-Dados_.pdf.

82 Mercosul, XII Reunião ordinário do subgrupo de trabalho nº13 – Comércio Eletrônico (15 de Junho de 2004) https://documentos.mercosur.int/simfiles/docreuniones/23116_SGT13_2004_ACTA02_ES.pdf. Acesso em: 8 out. 2021.

83 O material de consulta contido nos arquivos do Ministério da Justiça do Brasil ainda está disponível no site pessoal do brasileiro que foi pioneiro em proteção de dados, professor Danilo Doneda: http://www.doneda.net/2020/03/08/consultas-publicas-protecao-de-dados/.

84 Nos sistemas de direito civil, *vacatio legis* refere-se ao período de transição compreendido entre o anúncio do ato jurídico e o seu momento de entrada em vigor. O propósito dessa fase é oferecer um período de adaptação em que o cumprimento da nova lei possa ser devidamente organizado antes que a lei possa ser aplicada.

85 Belli L. e Zingales N. Brazilian Data Protection under Covid-19: Legal Certainty is the Main Casualty. CyberBRICS. (24 de agosto de 2020). Disponível em: https://cyberbrics.info/brazilian-data-protection-under-covid-19-legal-certainty-is-the-main-casualty/.

entrada em vigor da Lei. Por fim, a LGPD entrou em vigor em setembro de 2020, com exceção das disposições específicas que tratam de sanções administrativas por descumprimento da LGPD, que entraram em vigor em agosto de 2021, por meio da Lei nº 14.010/2020.

O Brasil também estabeleceu uma nova Autoridade Nacional de Proteção de Dados, mais conhecida como "ANPD",[86] em novembro de 2020, e um novo Conselho Nacional de Privacidade e Proteção de Dados que atua como um órgão multissetorial consultivo da ANPD. Embora a ANPD tenha um quadro de pessoal muito limitado, o órgão atualmente está em pleno funcionamento, e responsável por fazer cumprir a LGPD em face de pessoas físicas, jurídicas e governamentais. Em janeiro de 2021, a ANPD publicou sua agenda regulatória inicial, por meio da Portaria nº 11/2021.[87] O documento definiu objetivos educacionais e prioridades regulatórias. Entre as tarefas mais urgentes identificadas pela ANPD, contam-se a definição de procedimentos especiais para as pequenas e médias empresas (PMEs) e para *start-ups*, regras para a aplicação de sanções, relatórios e notificações de vazamentos e violação de dados, bem como avaliações de impacto sobre a proteção de dados. Num momento subsequente, o regulador prevê tratar dos procedimentos relativos ao acesso aos direitos dos titulares de dados e às tarefas dos encarregados — *Data Protection Officers* — e transferências internacionais de dados.

Infelizmente, a ANPD não incluiu nas suas prioridades regulatórias — deixando assim, substancialmente por definir — outras questões prementes, como os critérios de segurança e anonimização dos dados ou a definição de normas de interoperabilidade, que são essenciais para permitir o gozo do direito à portabilidade dos dados. Além disso, no momento da redação deste relatório, a maioria das tarefas regulatórias mencionadas acima permanece não realizada,[88] devido à capacidade notavelmente limitada da ANPD, o que torna quase impossível operar efetivamente.

---

86 O site oficial da nova Agência Brasileira de Proteção de Dados está disponível em: https://www.gov.br/anpd/pt-br.

87 BRASIL, Portaria ANPD nº 11 de 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313.

88 Os avanços em relação à regulamentação da ANPD podem ser monitorados em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes.

Cabe destacar que, de fato, com um orçamento escasso e um quadro inicial de apenas 36 servidores públicos — que foi ampliado apenas recentemente, para atingir um total de 75 membros — a ANPD parece ter sido estruturada pelo governo federal para ser incapaz de regular e fiscalizar a proteção de dados de forma eficaz, oferecendo um exemplo do que podemos definir como "ineficácia por design" (Belli, 2023).

Por último, mas não menos importante, o Congresso brasileiro aprovou uma emenda constitucional criando o direito fundamental à proteção de dados na Constituição Brasileira, que foi promulgada em fevereiro de 2022.[89] Ao conceder à proteção de dados pessoais o posto de direito fundamental, o Congresso brasileiro deu um passo histórico em direção ao reconhecimento da importância dos dados pessoais e sua proteção para o povo brasileiro, especialmente considerando a tecnologia recente. No entanto, é importante ressaltar que o Congresso brasileiro não aproveitou a oportunidade para definir quais são os elementos essenciais de tal direito — por exemplo, o princípio do consentimento, a legalidade, a equidade, a transparência, a visão geral independente etc. — que foram incluídos em outras experiências de direito fundamental à proteção de dados, como no art. 8 da Carta dos Direitos Fundamentais da União Europeia ou no art. 6 da Constituição mexicana. Além disso, embora o país tenha feito avanços consideráveis, a conformidade com a proteção de dados e uma cultura de proteção de dados ainda estão muito longe de serem alcançadas.

2 Mapeamento de normas estaduais de proteção de dados pessoais nos estados e municípios

Dez estados e o Distrito Federal possuem normas gerais de proteção de dados, ou seja, normas que regulam a implementação da LGPD e dão provimentos abrangentes sobre aspectos estruturais/institucionais e aspectos substantivos do direito à proteção de dados.[90] Todas as normas tomam a forma de Decretos, sendo o mais antigo o Decreto nº 49.265, de 6 de agosto

89 Em maio de 2020, o Supremo Tribunal Federal reconheceu um direito fundamental à proteção de dados na Constituição Brasileira de 1988, derivado, mas não coincidente com o direito à privacidade e o mandado de "habeas data".

90 Não há obrigatoriedade de normatização nos estados. De forma geral, os decretos encontrados tratam da organização administrativa da proteção de dados no estado. Quando vão além disto, enunciando direitos, tendem a repetir o texto da LGPD.

de 2020, do governo de Pernambuco, e o mais recente o Decreto nº 41.006, de 5 de outubro de 2021, do governo do Sergipe.

Dentre os Decretos encontrados, a maioria adota um modelo de indicação de Encarregado por cada órgão ou entidade da Administração Pública direta e das entidades da Administração Pública indireta. Alguns mencionam explicitamente a necessidade de indicação direta pelo Dirigente Máximo do órgão ou entidade, outros, não.

Um modelo alternativo foi encontrado no Espírito Santo e no Sergipe, em que se realizou uma divisão do papel do Encarregado entre dois níveis de organização. No Espírito Santo, o papel de Encarregado é centralizado pelo Comitê Encarregado Central, sendo seus membros indicados pela Autoridade Máxima de cada órgão ou entidade da Administração Pública Estadual. Paralelamente, cada órgão ou entidade deve também indicar um Encarregado Interno, que servirá como ponto de contato entre o Comitê Central e o órgão ou entidade. Além disso, o Decreto do Espírito Santo também determina que os operadores devem indicar encarregados próprios, que estarão sujeitos à fiscalização do Comitê Encarregado Central e dos Encarregados Internos.

As competências atribuídas ao Comitê Encarregado Central são extensas, ultrapassando aquelas três explicitamente citadas nos incisos I, II e III do §2º do art. 41 da LGPD. As dos Encarregados Internos, por outro lado, limitam-se a "atuar como canal de comunicação entre o Comitê Encarregado Central e os titulares dos dados, bem como exercer as funções previstas no art. 41 da Lei Geral de Proteção de Dados, no âmbito de cada órgão ou entidade" (art. 14, Decreto nº 4.922/21). Assim, enquanto os Encarregados Internos parecem ter uma função ocupada com o dia a dia do órgão ou entidade em que estão lotados, o Comitê Central, além de poder assumir essas atribuições (inclusive com poder de dispensar a indicação de Encarregado Interno), tem papéis relativos à coordenação, orientação, capacitação e auditoria de Encarregados Internos e dos órgãos e entidades.

No Sergipe, cada órgão ou entidade da estrutura administrativa estadual deve indicar um Encarregado Setorial, que atuará como Encarregado para aquele órgão ou entidade. Em paralelo, cabe à Secretaria de Estado da Transparência e Controle velar pelo papel de Encarregado Central. O cenário é semelhante àquele estruturado no Espírito Santo, com alguma sobreposição de atribuições relativas às funções típicas do Encarregado segundo a LGPD, mas com um papel de coordenação e assessoria técnica

da atuação de Encarregados Setoriais e seus respectivos órgãos e entidades por parte do Encarregado Central. Aqui, no entanto, há ainda mais um corpo de governança envolvido na arquitetura de supervisão e controle de proteção de dados: o Comitê Executivo da Política de Proteção de Dados Pessoais (CEPDP), que deverá ser formado em cada órgão e entidade e que apoia a atuação do Encarregado Setorial, além de elaborar o Programa de Governança em Privacidade e realizar o processo de adequação.

Finalmente, outro arranjo estadual que foge ao padrão observado é aquele encontrado no estado de São Paulo. Lá, o papel de Encarregado é totalmente centralizado, exercido pelo Ouvidor Geral do Estado. Destaca-se que o Ouvidor Geral, como encarregado pela proteção de dados, deverá atuar em coordenação com o Arquivo Público do Estado, designado pelo Decreto nº 58.052 de 2012 como responsável pela política estadual de arquivos e gestão de documentos, e os Serviços de Informação ao Cidadão. As exceções a esta centralização do papel do encarregado são os entes da Administração Pública indireta, que devem indicar Encarregados próprios.

3 A possível sobreposição entre órgãos responsáveis para segurança da informação, acesso a dados públicos e proteção de dados pessoais

Afora estes comentários específicos a respeito da estruturação da figura do Encarregado nestas três jurisdições, cabem alguns comentários gerais, por interessantes. Primeiro, é digno de nota que muitos dos estados estudados criaram estruturas de governança de dados pessoais, conforme exposto na figura a seguir:

	Corpos de governança	
Paraíba	Conselho Gestor de Proteção de Dados Pessoais	Comitê Executivo de Proteção de Dados Pessoais
Minas Gerais	Comitê Estadual de Proteção de Dados Pessoais	
Pernambuco	–	

Rondônia	Comitê Gestor de Privacidade e Proteção de Dados Pessoais	
Santa Catarina	Comitê Gestor de Proteção de Dados	
São Paulo	Comitê Gestor de Governança de Dados e Informações	
Espírito Santo	Comitê Encarregado Central	
Mato Grosso do Sul	–	
Paraná	Comitê Gestor de Proteção de Dados Pessoais	
Sergipe	Comitês Executivos de Proteção de Dados Pessoais	Conselho de Governança da Política Estadual de Proteção de Dados Pessoais

Elaboração dos autores.

Além dos novos corpos de governança criados, muitas normas citam entidades pré-existentes como componentes ou relacionadas à governança de proteção de dados pessoais, como Controladorias estaduais e Conselhos, Superintendências e Comissões ocupados com temas correlatos, como segurança da informação, sigilo de dados e acesso à informação. Este é um ponto de grande relevo para os objetivos deste trabalho, pois indica a sobreposição de sistemas pré-existentes relacionados à segurança da informação e ao acesso a dados públicos com as dinâmicas estaduais nascentes em proteção de dados pessoais.

Em muitos casos, aquelas entidades são citadas em referência à necessidade de diálogo entre estes três sistemas, enquanto em outros casos assumem responsabilidades relacionadas ao próprio sistema de proteção de dados pessoais — como é o caso do Decreto paulista, que dispõe:

> Decreto n. 65.347/2020, art. 6º, §2º: O disposto no "caput" deste artigo não impede que os órgãos da Administração Pública indiquem, em seus respectivos âmbitos, para desempenhar, em interlocução com o encarregado, as atividades a que aludem os incisos I e III do § 2º do artigo 41 da Lei federal nº 13.709, de 14 de agosto de 2018, respectivamente: 1. os Serviços de Informações ao Cidadão — SIC, criados pelo artigo 7º do Decreto nº 58.052, de 16 de maio de 2012; 2. as Comissões de Avaliação de Documentos e Acesso — CADA, de que trata a Seção III do Capítulo II do Decreto nº 58.052, de 16 de maio de 2012 (Assembleia Legislativa do Estado de São Paulo, 2020).

Cabe ressaltar a importância de se considerar conjuntamente a abertura, a proteção e a segurança de dados, a fim de maximizar a sinergia e reduzir redundâncias e potenciais sobreposições e fricções entres os profissionais implicados. Assim, como destacamos desde o início deste relatório, idealmente, cada órgão público deveria estabelecer um Escritório de dados no âmbito do qual profissionais formados na abertura, proteção e segurança de dados podem dialogar e trocar informações, organizando-se e cooperando continuamente.

É interessante notar recente Portaria da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), nº 852 de 28 de março de 2023, em que se detalha o Programa de Privacidade e Segurança da Informação, a ser desenvolvido e implementado no âmbito de órgãos e entidades da administração pública federal direta, autárquica e fundacional. O documento institui alguns elementos basilares para o Programa, como o diagnóstico de implementação de controles de privacidade e segurança da informação (art. 4º, §1º, III) e a promoção de "boas práticas por meio de disponibilização de guias, processos, modelos e procedimentos" (art. 4º, §1º, VI), dentre outros. Também reúne controles, metodologias e ferramentas de apoio sob a denominação de um "Framework de Privacidade e Segurança da Informação", sob a égide da LGPD, da Política Nacional de Segurança da Informação, de normativos da ANPD e do Gabinete de Segurança Institucional e recomendações de órgãos de controle interno e externo.

Importante para a discussão ora travada a respeito de estruturas organizacionais que deem concretude às sinergias entre abertura, proteção e segurança de dados e organizem áreas de sobreposição, a Portaria também trata da formação, nos órgãos e entidades, de uma estrutura de governança própria. Assim, estariam reunidos sob essa estrutura o Gestor de TICs, o Gestor de Segurança da Informação, o Encarregado pelo tratamento de dados pessoais e o Responsável pela Unidade de Controle Interno. Estes agentes trabalhariam em uníssono para promover a segurança da informação e a proteção de dados nos órgãos e entidades.

É interessante notar a caracterização do papel de cada um nessa estrutura de governança. Enquanto os Gestores de TICs e Segurança da Informação são caracterizados como "a primeira linha de defesa quando se tratar de controles de privacidade e segurança da informação"

(art. 6º, §1º), o Encarregado tem papel de apoio e orientação à atuação dos demais. Como veremos adiante, normas estaduais têm operado uma ampliação das atribuições do Encarregado e conferido protagonismo a este agente, podendo-se aventar como ponto passível de investigação futura alguma dissonância entre a construção do seu papel naquelas normas e na normativa federal.

Ademais, nota-se que a Portaria trata apenas de segurança da informação e privacidade, não abordando o tópico da abertura de dados. Devido à proximidade dos tópicos, inclusive na necessidade de tomada de decisão a respeito de padrões técnicos para abertura de dados, manutenção ou criação de sistemas para tanto etc., seria importante que integrassem a estrutura de governança, também, gestores da transparência de dados, como fazem algumas das normas estaduais estudadas adiante.

4 Garantias e pré-requisitos para a atuação do Encarregado

Um segundo ponto de interesse é a relação de garantias e pré-requisitos para a atuação do Encarregado. Dos dez estados, sete asseguram apoio dos setores jurídico, tecnológico, de controle interno e outras unidades à atuação do Encarregado; seis mencionam a capacitação permanente do Encarregado, inclusive com apoio à sua formação; cinco mencionam acesso direto à alta administração do órgão ou entidade, a subordinação direta ao Dirigente Máximo do órgão ou entidade e não estar lotado no setor de Tecnologia da Informação ou gerir sistemas de informação.

Apenas quatro fazem menção ao acesso (em alguns casos caracterizado como "motivado", em outros, sem qualquer adjetivação) às operações de tratamento de dados pessoais e apenas um menciona amplo acesso à estrutura organizacional.

5 Atribuições de competência dos Encarregados

Finalmente, o quadro a seguir descreve as categorias de atribuições de competência aos Encarregados e sua respectiva frequência dentre os dez decretos estudados:

Atribuições:	Freq.:
Atendimento a titulares de dados	10
Recebimento de comunicações da ANPD	9
Orientação de servidores, funcionários e contratados	8
Apoio no processo de adequação à LGPD	5
Demais atribuições definidas em normas complementares	5
Emitir recomendação de adequação / mitigação de riscos	5
Mapeamento / inventário de dados	5
Atender a normas complementares pela ANPD	4
Informar / auxiliar na gestão de incidentes	4
Monitoramento regular e sistemático de atividades de tratamento	4
Orientação sobre padrões de boas práticas	4
Publicação de RIPD	4
Apoio técnico	2
Canal de comunicação entre agentes de tratamento, ANPD e titulares	2
Avaliação e aconselhamento sobre segurança de dados	1
Campanhas educativas	1
Capacitação de encarregados internos	1
Coordenação de Política de PD	1
Elaboração de RIPD	1
Informar à ANPD sobre uso compartilhado com entes privados	1
Providenciar análise de conteúdo sigiloso	1
Requisitar informações	1
Sugerir alterações normativas	1

Elaboração dos autores. Células em destaque: atribuições contidas na LGPD.

O rol de atividades do Encarregado, segundo o artigo 41 da LGPD, resume-se a três atividades específicas e duas normas indefinidas para a

sua expansão (em virtude de determinação do controlador ou por norma complementar). A sua expansão nas normas estudadas pode ser fruto do detalhamento do seu papel na dinâmica mais ampla de proteção de dados, ultrapassando a mera função de "canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados" (art. 5º, VII, LGPD) para assumir uma postura proativa na adequação dos órgãos e entidades à lei. É o caso, por exemplo, das previsões em que o Encarregado é responsável por elaborar Relatórios de Impacto à Proteção de Dados e em que participa da realização de mapeamento ou inventário de dados.

6 Boas práticas em proteção de dados pessoais

O enfoque, no tópico anterior, nas estruturas de governança da proteção de dados pessoais se justifica por uma razão: a concretização desse direito depende da composição de políticas e processos internos, de ações concretas inseridas no dia a dia da gestão de dados e do envolvimento ativo dos agentes. Voltamos, agora, à exposição de algumas boas práticas centradas nesta necessidade de concretizar a proteção de dados pessoais nos procedimentos de tratamento de dados da organização.

A seguir são elaboradas algumas considerações construídas a partir de consulta documental composta por guias práticos publicados por especialistas, organizações da sociedade civil e pela Autoridade Nacional de Proteção de Dados. Foi criada também uma versão estendida, na forma de ferramenta interativa,[91] pensada como documento de referência para um passo a passo de adequação à LGPD.

De forma resumida, as ações de adequação podem ser divididas em grandes campos de ação:

I. Preparativos;

II. Mapeamento de dados;

III. Segurança;

91 Desenvolvida pelos autores com base em busca documental detalhada na própria ferramenta. Disponível em: https://is.gd/XcagcD.

IV. Gestão de incidentes;

V. Relações com terceiros;

VI. Informação e direitos dos titulares;

VII. Relatório de impacto;

VIII. Governança.

Cada tópico representa um conjunto temático a ser concretizado por meio de estruturas, processos, instrumentos e treinamento dos agentes envolvidos. Dentre as ações preparatórias (I), destacamos a definição do papel da organização (como Controladora ou Processadora) e a nomeação de Encarregado. Como indicam os atos normativos estudados no tópico anterior, a posição do Encarregado dentro da estrutura de gestão deve estar cercada de algumas garantias, como o necessário apoio, formação continuada, acesso aos processos de tratamento de dados e acesso à alta diretoria, além de cuidados relativos a conflitos de interesse — como reportar-se diretamente à alta administração da organização e não estar lotado no setor de TI. Sobre a definição do papel da organização, há Guia Orientativo publicado pela ANPD[92] que esclarece pontos importantes neste sentido.

O segundo campo, do mapeamento de dados, refere-se à atividade basilar merecedora de um tópico próprio pela sua importância. Compreender os dados pessoais que são coletados e tratados pela organização, classificá-los (em função da sensibilidade, do tipo de titular, das fontes, bases legais, finalidades etc.) e manter os registros adequados, sob uma perspectiva do ciclo de vida do dado pessoal (onde se origina, por onde/quem passa e quando deverá ser extinto ou arquivado) é etapa seminal na construção de uma postura responsável em relação à proteção de dados pessoais.

O terceiro campo, da segurança, será tratado em maiores detalhes na seção seguinte. No entanto, cumpre destacar que o dever de segurança consiste na implementação das medidas técnicas e administrativas aptas a garantir a segurança dos dados — consideradas sob uma lente contextual,

92 ANPD. (2021). Guia orientativo para definições dos agentes de tratamento de dados pessoais (operadores e controladores) e do encarregado. Disponível em: https://is.gd/Yd5JRP.

levando em conta "a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia" (art. 46, §1º, LGPD). Ou seja, deve-se analisar caso a caso (e seguir o direcionamento dado pela Autoridade, quando houver[93]) as medidas adequadas. Além disso, é importante atentar à necessidade de demonstrabilidade da adoção destas medidas e de providências mitigadoras de riscos e danos, em observância ao princípio da responsabilização e prestação de contas (art. 6º, X, LGPD).

A política de gestão de incidentes deve enfrentar o desafio delicado de definir o momento em que um incidente é uma ameaça concreta à segurança de dados pessoais. Verificada a necessidade de comunicação à ANPD,[94] é importante haver um esforço ativo de registro dos detalhes do incidente e de seu enfrentamento. Isso é relevante não apenas para existir um corpo de conhecimentos necessário ao aprimoramento futuro de práticas de segurança, mas também para cumprir o dever de informação à Autoridade e, eventualmente, aos titulares de dados.

Um tratamento cuidadoso das relações com terceiros (V) é importante para determinar o adequado grau de cuidado e as responsabilidades associadas a prestadores de serviço. Para tanto, recomenda-se a celebração de um contrato de processamento de dados, inclusive determinando as condições sob as quais os sub-operadores poderão ser contratados. Também importa para o dever de informação ao titular de dados, que tem o direito de conhecer aqueles com quem seus dados são compartilhados (art. 9º, V, e art. 18, VII, da LGPD).

Os deveres de informação e a garantia dos direitos dos titulares (VI) compõem boa parte da face pública do programa de adequação. Os principais núcleos normativos referentes a esses direitos e deveres se encontram nos artigos 9º e 18 da LGPD, representando elementos das operações de tratamento de dados que devem ser informados ao titular no momento da coleta de dados e disponíveis ao longo da relação de tratamento de dados. Dois exemplos relevantes, por comumente se encontrarem na inter-

93 Ver, por exemplo: ANPD. (2021). Guia orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Disponível em: https://is.gd/NHzGqO.

94 ANPD. (2021, July 21). Comunicação de incidentes de segurança. ANPD.Gov.Br. Disponível em: https://is.gd/U30TW5.

face entre Controlador e Titular, são a Política de Privacidade e a Política de Cookies (que podem estar contidas em documentos separados ou apresentadas conjuntamente). É de suma importância que o controlador demonstre preocupação em comunicar os detalhes do tratamento de dados, bem como os direitos do titular de dados em termos e formato que o titular compreenda. Isto passa por adotar linguagem acessível e encontrar soluções de design aptas a guiar a atenção do leitor de forma eficaz, sem a implementação dos chamados *dark patterns* — padrões de design e linguagem tendentes a levar o leitor a erro.

O Relatório de Impacto sobre Proteção de Dados Pessoais e Privacidade (RIPDP) é um documento que concentra boa parte das preocupações até aqui apresentadas. O relatório descreve a operação de tratamento de dados pretendida, busca identificar riscos e propõe ações de mitigação. Nem sempre será preciso realizar RIPDP, mas fazê-lo é uma boa prática que proporciona uma governança de dados mais efetiva e eficiente, apoiando e facilitando consideravelmente a atividade de adequação, como explicamos na última parte deste relatório.

Finalmente, as ações de governança (VIII) criam a costura prática e organizacional dos pontos discutidos até aqui. Implementar processos de avaliação de riscos de privacidade de dados, criar um programa de governança de dados pessoais e privacidade e definir responsáveis setoriais, fluxos de informações, grupos especiais de resposta a incidentes, comissões de formação de funcionários e outras formas de organização refletem, em essência, a necessidade de criar os corpos organizacionais adequados. Para tanto, não há modelo pré-determinado: cada organização tem necessidades específicas e deve estruturar a governança que se adapte aos seus processos internos.

Os quadros a seguir enumeram mais ações importantes por campo de ação, com base na revisão documental empreendida. As fontes consultadas estão listadas na versão estendida e interativa destas considerações.[95]

95 Desenvolvida pelos autores com base em busca documental detalhada na própria ferramenta. Disponível em: https://is.gd/XcagcD.

Áreas	Ações
Geral	Identificação dos gaps atuais na adequação.
	Engajar os executivos (alta administração) da companhia no processo de adequação.
	Formação de comitê de adequação à LGPD com ao menos uma pessoa de cada área da empresa.
	Nomear um encarregado pelo tratamento de dados pessoais.
	Determinar o papel da companhia como controlador e/ou operador de dados. Analisar responsabilidades e obrigações daí decorrentes.
	Escolher e adotar (ou desenvolver) software de gestão da privacidade.
	Manter registro dos tratamentos de dados realizados.
	Planejar e implementar avaliações periódicas do cumprimento do programa de adequação.
	Realizar treinamentos sobre privacidade, proteção de dados e segurança da informação.
	Implementar princípios de privacidade by design.
Mapeamento de dados	Criar metodologia e agenda de revisão periódica do mapeamento de dados.
	Mapear (identificar, classificar, registrar) dados pessoais.
	Identificar a base legal apropriada para cada categoria de dado tratado.
	Manter registro da finalidade.
	Identificar se há tratamento de dados sensíveis ou de crianças e adolescentes.
	Manter registro do consentimento obtido de titulares.
	Criar uma agenda de retenção dos dados e eliminá-los ou arquivá-los após cumprida a finalidade.
	Minimizar dados (eliminar dados desnecessários, coletar apenas dados necessários).
	Identificar instâncias em que a companhia envia dados para o exterior e para que propósitos.

Governança	Implementar processo de avaliação de riscos de privacidade de dados.
	Criar programa de governança de dados pessoais e privacidade.
	Definir responsáveis pela determinação das bases legais adequadas a cada tipo de dado pessoal tratado.
Segurança	Implementar e documentar medidas de segurança.
	Criar política de segurança da informação.
	Implementar criptografia.
	Adotar anonimização e pseudominimização sempre que possível.
	Controlar ferramentas (software) e dispositivos (hardware) por meio de inventário, criptografia, política de transporte para fora da empresa e política de BYOD.
	Realizar periodicamente testes de intrusão.
	Revisar e documentar a segurança física dos dados.
	Adotar política de backups periódicos dos dados.
	Adotar senhas fortes e trocadas periodicamente, bem como autenticação de acesso em múltiplos fatores.
	Definir política de acesso e controlar acessos.
Incidentes	Criar política de resposta a incidentes.
	Criar plano de comunicação.
	Definir política de notificação de incidentes.
	Padronização de atividades de resposta.
	Definir responsáveis por resposta.
	Documentar resposta a incidentes.
	Documentar incidentes.

Terceiros	Identificar todos os terceiros com quem a companhia compartilha dados pessoais.
	Identificar operadores e sub-operadores de dados pessoais contratados pela empresa.
	Estabelecer obrigações específicas dos envolvidos no tratamento em contratos de tratamento de dados.
	Elaborar contratos específicos sobre responsabilidades e cuidados de prestadores de serviço.
	Exigir testes, evidências e auditorias de terceiros.
	Verificar adequação de serviços de terceiros envolvidos no tratamento de dados.
Informação e direitos dos titulares	Atualizar a política de privacidade e informá-la aos titulares.
	Verificar o uso de cookies e outros mecanismos de rastreamento do site e informá-lo aos usuários.
	Informar previamente a finalidade de tratamento ao titular.
	Comunicar mudanças na finalidade do tratamento.
	Informar aos titulares sobre tratamentos iniciados antes da entrada em vigor da lei, incluindo a sua finalidade.
	Adotar medidas para garantir consentimento válido.
	Explicar ao titular como e por que são aplicadas técnicas de *profiling* e decisão automatizada.
	Treinar pessoal no atendimento ao titular, inclusive em relação aos pedidos de direitos do titular.
	Estabelecer processo de resposta rápida a pedidos dos titulares (e.g., acesso, eliminação, correção, portabilidade de dados).

Relatório de impacto	Avaliar se o tratamento é de alto risco para o titular de dados ou se há obrigatoriedade legal de realização do relatório para o tipo de tratamento em análise.
	Elaborar relatório de impacto à proteção de dados pessoais antes de iniciar o tratamento.
	Implementar medidas de mitigação dos riscos identificados.
	Ao identificar riscos graves que não possam ser mitigados, consultar a ANPD antes de realizar o tratamento.
	Realizar RIPDP sempre que for implementar novos programas, sistemas e processos.
	Realizar previamente Relatório/Avaliação de Legítimo Interesse, baseado no teste de equilíbrio de legítimo interesse, para todo tratamento que tiver o legítimo interesse como base legal.

Parte III
Segurança da informação no Brasil

Resumo em tópicos

No presente capítulo, mapeou-se a normatização da segurança cibernética no Brasil, consideradas relevantes para planos de dados abertos, para além de padrões de segurança da informação, que indicam boas práticas a serem adotadas pelo órgão ou ente público. Neste sentido, destacam-se as seguintes prioridades:

- No caso de entes ou órgãos no âmbito Federal, adotar o arranjo ("*framework*") de privacidade e segurança da informação e envio à Secretaria de Governo Digital, conforme prevê a Portaria SGD/MGI nº 852/2023;
- No caso de entes ou órgãos no âmbito estadual ou municipal, recomenda-se adotar este arranjo como boa prática de segurança cibernética;
- Instituir mecanismos de cooperação de segurança cibernética com outros órgãos e entes, principalmente, com entidades ou órgãos públicos que também acessam e/ou realizam operações com os dados que serão abertos; trocas de experiências em situações de incidentes ou de rotinas de segurança;
- Elaborar política de segurança cibernética de fácil compreensão, acompanhada de documentos complementares, para informar sobre as medidas que são usadas para assegurar os dados pessoais objeto de abertura, e ao mesmo tempo dar transparência sobre eventuais impactos no direito de privacidade, de pessoas que interagem com as plataformas de dados abertos, diante da adoção de medidas de segurança;
- Investir em medidas de informação, comunicação, treinamento e educação em temas de segurança cibernética, estimulando

comportamentos seguros no ambiente digital, e fornecendo transparência sobre quaisquer incidentes com dados pessoais, ou dados anonimizados, em geral, envolvidos na abertura de dados;

- Estimular a participação social na definição dos arranjos de segurança cibernética;
- Empreender esforços para que essas medidas alcancem não só a/os agentes pública/os, mas também fornecedores envolvidos no plano de dados abertos, e pessoas em geral que irão interagir com a plataforma de dados abertos;
- Garantir medidas de auditabilidade sobre a interação com sistemas e infraestruturas necessárias para abertura de dados, que sejam compatíveis com a garantia da privacidade e proteção de dados pessoais;
- Instituir instrumentos de responsabilização por descumprimento de obrigações de segurança cibernética a todas as pessoas jurídicas envolvidas nos processos de abertura de dados;
- Adotar ferramentas de segurança que permitam o acompanhamento contínuo de ameaças, vulnerabilidades e ataques de segurança;
- Sempre que possível, priorizar ferramentas não proprietárias/comerciais, *open source* (código aberto);
- Adotar esforços para incorporar, principalmente, os controles da ISO/IEC 27001:2013, indicados na Tabela II desta seção, para elaboração do sistema de segurança da informação do Plano de Dados Abertos, na medida daquilo que for cabível diante do contexto e realidade concreta da organização que está executando o plano de dados abertos.

Introdução: promoção de segurança em atividades de abertura de dados em plataformas digitais

O campo da segurança cibernética no Brasil é recente e, portanto, sua interação com as políticas de dados abertos e com o sistema de proteção de dados pessoais brasileiro ainda precisa ser aprofundada.

Para a presente análise, que tem como objetivo compreender as medidas necessárias para promoção de segurança em uma atividade específica que se vale de infraestruturas digitais (*i.e.*, a publicação de dados coletados pelo, produzidos por, ou acerca das atividades do Poder Público), não será utilizado o conceito de ciberespaço — que dicotomiza a realidade em duas esferas.[96] Valendo-nos, no entanto, das contribuições de autores que partem do conceito, entendemos que as medidas de segurança cibernética (termo empregado em razão da denominação da E-Ciber) — sejam elas no plano técnico, organizacional (incluindo a revisão de processos) ou cultural — devem ter como centralidade a promoção da segurança das pessoas e coletividades de pessoas, de seus direitos ou, de forma mais ampla, a garantia de direitos humanos.

Nesse sentido, entende-se que a escolha e adoção de técnicas de segurança cibernética para apoiar a abertura de dados pelo Poder Público precisam estar extremamente alinhadas com as preocupações de proteção de dados e abertura apresentadas nos tópicos anteriores.

A fim de compreender requisitos mínimos e boas práticas de segurança, foram mapeados instrumentos normativos que trazem disposições gerais, em nível nacional (*i.e.*, Estratégia Nacional de Segurança Cibernética, Política Nacional de Segurança da Informação, e o Programa de Privacidade e Segurança da Informação). Além disso, apresentar-se-ão, a título exemplificativo, obrigações instituídas no nível estadual (utilizando-se como estudo de caso o estado do Rio de Janeiro e a política de segurança que obriga os entes da administração pública do estado), com o objetivo de

96 Betz e Stevens (2013), ao empreender uma análise do discurso sobre a cibersegurança nos EUA, colocando em questionamento as "racionalidades analógicas" empregadas para atribuir conteúdo ao conceito, pontuam que as ciências sociais se afastaram do uso do termo "ciberespaço" (p. 150). Os autores mobilizam a literatura para sugerir que o termo não é o mais transparente, uma vez que deixa de explicitar toda a infraestrutura física, e as pessoas que são envolvidas nas atividades. (Betez; Stevens, 2013, p. 151).

alertar os agentes públicos acerca da necessidade de observar medidas previstas em normas locais. Esses instrumentos fornecem medidas técnicas e administrativas (utilizando-se do vocabulário da proteção de dados pessoais[97]) previstas nos padrões internacionais de desenvolvimento de tecnologias — a partir de uma abordagem menos "sócio" e mais "técnica".[98] Apresentar-se-ão estes padrões, e principais controles que instituem, após comentários sobre a regulação mapeada.

Entende-se que tais medidas não são as únicas nem são suficientes para proteger pessoas (sujeitos) ou grupos de pessoas (sujeitos coletivos) que podem ser alvos de violências e exploração, com base na divulgação de informações por meio da abertura de dados. Não por outro motivo, acredita-se na relevância de aproveitar o atual cenário para revisar e avançar na agenda regulatória de cibersegurança, principalmente diante da centralidade que é dada à cooperação com setor empresarial no arcabouço regulatório existente, bem como perante o seu caráter individualista, militarizado (não somente por conta da previsão de competências que estão a cargo de órgãos ou atores militares, mas também pela abordagem combativa — inclusive às pessoas, compreendidas como ameaças).[99] Trata-se de um plexo regulatório fragmentado, e que não estabelece o necessário diálogo com disposições de proteção de dados (apresentadas anteriormente).

Enquanto não houver esse avanço na agenda regulatória e abandono do legado militarizado dos últimos anos, sugere-se que, para o cumprimento das obrigações legais e a adoção de boas práticas apresentadas neste documento, haja o enriquecimento das referências oficiais ao elaborar a estratégia de segurança cibernética para processo de abertura de dados. Recomendam-se as cartilhas publicadas na biblioteca[100] da organização

---

97 Conforme visto, a LGPD prevê no artigo 46 que "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." (Brasil, 2018)

98 Discutindo a abordagem sociotécnica proposta por van den Berg (2020).

99 Para críticas preliminares ao atual arcabouço regulatório em segurança cibernética, *cf* Belli et al, 2023.

100 Cf.: SHIRA, F.; JANCZ, C. Barricadas, estratégias e coletividade: Uma cartilha de segurança digital para organizações. São Paulo: MariaLab, dez. 2020. Disponível em: https://www.marialab.org/wp-content/uploads/2020/12/Barricas-estrategias-coletividade.pdf. Acesso em: 2 mar. 2023.; SHIRAKAWA, Fernanda; MONTEIRO, Fernanda; SANTIAGO, Larissa. GUIA

MariaLab para apoiar essa complementação, as quais contemplam orientações de práticas de segurança (e de como lidar com casos de incidentes, como o sequestro de dados) para organizações na defesa de direitos; e comportamentos seguros e cuidados digitais que podem ser adotados, principalmente, por mulheres pretas e trans, como forma de reforçar a proteção de seus direitos.

1 Mapeamento de documentos normativos

Para o mapeamento de instrumentos normativos e resoluções aplicadas a contextos específicos, foram verificados os padrões de segurança instituídos nos seguintes documentos:[101]

> I. O Decreto nº 9.637/2018, que "Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação", voltada para regular as atividades da administração pública federal, para os casos em que houver tratamento de "dados custodiados por entidades públicas" e para assegurar "informação das infraestruturas críticas", dados pessoais e de informações com restrição de acesso (art 4º, VI, a, b, c e d). Tal decreto foi, posteriormente, alterado pelo decreto 10.641/2018, tendo sido mapeada a redação que já traz tais alterações;

PRÁTICA DE ESTRATÉGIAS E TÁTICAS PARA A SEGURANÇA DIGITAL FEMINISTA. CFEMEA e Universidade Livre Feminista, disponível em: https://www.marialab.org/wp-content/uploads/2020/09/guia_pratica_estrategias_taticas_seguranca_digital_feminista.pdf. Outros materiais podem ser encontrados na Biblioteca da MariaLAB: https://www.marialab.org/biblioteca/.

101 Utilizou-se o mesmo grupo de palavras-chave para realizar buscas em diferentes repositórios legislativos. Foram as expressões "segurança digital" e "segurança da informação" que também conduziam a resultados contendo a noção de "segurança cibernética" como aproximação dos termos utilizados para orientar a busca nos sites do Congresso Nacional e, em âmbito estadual - refletindo sobre a elaboração do presente documento - replicou-se a consulta nos sites da Câmara Municipal da cidade do Rio de janeiro - onde não se encontrou nenhum documento relevante e na Assembleia Legislativa do Estado do Rio de Janeiro (ALERJ - Câmara de Deputados Estaduais do Estado). De acordo com os resultados de busca, verificou-se se, de fato, havia previsões normativas instituindo deveres ou regimes de responsabilidade sobre adoção de medidas de segurança para atividades que ocorrem com suporte digital nos documentos achados, caso negativo, buscou-se referências, nestes documentos, a outros textos normativos (ou necessidade de elaborar regulações específicas) que endurece riscos relacionados à segurança da informação - ou cibernética, nos termos da Estratégia Nacional de Segurança Cibernética).

II. O Decreto 10.222 de 2020, que institui a Estratégia Nacional de Segurança Cibernética (E-Ciber), a qual "orienta a sociedade brasileira sobre as principais ações do governo federal em termos nacionais e internacionais, na área de segurança cibernética no quadriênio 2020-2023"[102];

III. A Portaria SGD/MGI nº 852, de 28 de março de 2023, do Ministério da Gestão e da Inovação em Serviços Públicos/Secretaria de Governo Digital, que dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI); e

IV. O Decreto nº 10.748, de 16 de julho de 2021, institui a Rede de Gestão de Incidentes Cibernéticos. Trata-se de regulamentação formal daquilo disposto no art. 15, inciso VII, do Decreto nº 9.637/2018.

No âmbito estadual, tomando por exemplo o Estado do Rio de Janeiro, identificou-se a instrução Normativa 02 do PRODERJ — Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro, vinculado à Secretaria de Estado de Transformação Digital, que regulamenta "os procedimentos a serem adotados pelos órgãos e entidades da Administração Direta e Indireta do Poder Executivo do Estado do Rio de Janeiro quanto à segurança da informação, para aprimorar a segurança da informação no âmbito da Administração Pública Estadual". Alguns elementos incorporados pela instrução normativa serão apontados após a apresentação dos principais achados nos instrumentos normativos de âmbito nacional.

Na Tabela I a seguir, indicam-se obrigações legais ou ações estratégicas estabelecidas pela regulação federal em segurança cibernética. É possível que algumas disposições deixem de ser obrigatórias, no caso de eventual avanço na agenda regulatória de cibersegurança, na direção de maior centralidade para proteção de direitos sociais e fundamentais das pessoas (Belli *et al.*, 2023). Ademais, a amplitude das medidas (que são acompanhadas de custos de diferentes naturezas) evidencia a necessidade de priorizar algumas ações, de acordo com aquilo que é mais urgente adotar a fim de proteger informações pessoais e atender ao interesse público nos planos de

102 Texto de apresentação da E-ciber na plataforma do governo digital, disponível em: https://is.gd/28IHf6.

dados abertos. Após a Tabela, apresentar-se-ão alguns comentários acerca dos documentos normativos utilizados para sua elaboração.

Tabela I: Principais medidas de segurança cibernética na regulação federal			
Medida a ser adotada na abertura de dados/ pontos de atenção	Instrumento normativo	Obrigação legal/ação estratégica	Detalhamento
Elaboração de política de segurança da informação e normas de segurança cibernética em geral	PNSI/E-ciber	art. 15, II	É importante que, no caso de abertura de dados, seja considerada a publicação de política de segurança da informação para pessoas externas ao órgão ou ente público, que acessarão os sistemas e infraestruturas digitais relacionadas. No item 3.2.2.1. e na seção 3.3 apresentaram-se maiores sugestões com relação à política de segurança. A E-ciber fala em desenvolvimento de programas e projetos sobre governança cibernética nas práticas de abertura de dados, os quais devem estar em diálogo com as políticas e normas
Criação de espaços de educação em termos de segurança da informação	PNSI	art. 3º, VII, VIII	É importante que o treinamento seja diferenciado da prática educativa sobre segurança cibernética, que deve ir além da apropriação de técnicas e habilidades
Instituir medidas de treinamento e capacitação em segurança da informação	PNSI	art. 3º, VII, VIII; art. 15, IV	Considerar disponibilizar testes, vídeos, textos de treinamento de segurança cibernética para pessoas que não façam parte do órgão ou ente público

Comunicação interna e externa (sociedade em geral) acerca de assuntos relacionados à segurança da informação	PNSI/E-Ciber	art. 4º, V (PNSI); Ação estratégica relacionada: Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade (E-ciber)	A comunicação pode ser feita por alertas e recomendações, vídeos explicativos, áudios
Comunicar às pessoas (agentes pública/os do órgão ou ente, e a sociedade em geral) sobre vulnerabilidades e incidentes	PNSI/E-ciber/ PPSI	art. 17, IX (PNSI); Ação estratégica relacionada: Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade (E-ciber); art. 15 (PPSI)	É importante que todas as pessoas que acessam, desenvolvem, fazem a manutenção da base sejam alertados sobre incidentes de segurança, e de forma compreensível e acessível. Por isso, recomenda-se que o tom da comunicação seja diferente, de acordo com o público-alvo
Notificar incidentes cibernéticos ao CISC gov.br	PPSI	art. 18	As especificações da ISO 27.001:2013 indicam informações que podem ser apresentadas nessa comunicação do incidente de segurança cibernética. Essas sugestões podem ser acessadas no item 3.3 deste documento
Instituição de controle de acesso, autenticação e gerenciamento de identidade	PNSI	art. 3º, XII; art 3º, XIV	Maiores detalhamentos sobre mecanismos de autenticação podem ser encontrados na seção 3.3 deste documento, onde serão apresentadas boas práticas sugeridas por padrões como ISO 27.001:2013.

Restrição/ minimização de acesso às informações (a partir do controle de acesso, autenticação e gerenciamento de identidade)	PNSI	art. 17, par. 1º, I; art. 3º, XII; art 3º, XIV	Restrição de acesso, a partir dos controles de acesso, de acordo com a "necessidade de conhecer", indicando que o acesso apenas será liberado por ser importante para o desempenho de determinadas funções, e a "necessidade de uso", indicando que só será permitido acessar determinados recursos quando essencial para o desempenho de tarefas atribuídas a si. Sugere-se que sejam adotados recursos criptográficos para assegurar a restrição de acesso às informações (art. 17º, par. 1º, I)
Adoção de medidas de segurança cibernética	PNSI/PPSI	art. 3º, XV, art. 17, VI (PNSI); art. 9º, IV (PPSI)	A seção 3.3 traz maior concretude às medidas que podem ser adotadas, e que devem contemplar a criticidade das informações (e também sensibilidade das informações), sistemas e infraestruturas digitais, buscando aumento da capacidade e maturidade do órgão ou ente em privacidade e segurança da informação.
Adoção de sistemas de segurança da informação que permita o acompanhamento das atividades de segurança	PNSI	art. 17, II e VIII	Sugere-se que sejam priorizados *softwares* livres na escolha de ferramentas de gerenciamento de ameaça — já que o uso de ferramentas comerciais para proteção de informações estratégicas do poder público pode não ser favorável a uma estratégia de segurança cibernética alinhada com os objetivos de soberania digital (evidente que desde que acompanhado de treinamento)

Acompanhamento contínuo e proativo das ameaças e dos ataques cibernéticos	E-ciber	Ação estratégica relacionada: Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade)	O acompanhamento pode ser feito pela adoção de sistemas ou criação de sistemas de gerenciamento de segurança cibernética
Instituição de controles internos de segurança da informação	PNSI	art. 17, VIII	Controles podem ser instituídos conforme padrões de segurança internacional, e considerando aprendizado institucional de acordo com o contexto específico
Alocação de equipe própria para prevenção, gestão e resposta a incidentes; e instituição de medidas de prevenção de incidentes e realização de análise de riscos e ações de contingência	PNSI	art. 3º, IX, art. 7º, III, art. 15, VII	Apesar da PNSI não mencionar a necessidade de elaboração de plano de resposta a incidentes, a alocação da equipe deve ser acompanhada da elaboração deste instrumento institucional, que deverá documentar as estratégias de ação no caso de incidentes cibernéticas nos sistemas, redes, infraestruturas e outros

Estabelecer mecanismos de cooperação multissetorial e poder público	PNSI/E-Ciber	art. 3º, XV; Ação estratégica relacionada: Ampliar a parceria em segurança cibernética, entre setor público, setor privado, academia e sociedade (E-ciber)	A E-ciber também vai falar de estabelecer mecanismos de cooperação multissetorial para **estudo** sobre segurança cibernética, algo que se considera extremamente relevante diante das rápidas transformações em termos de ameaças e ataques cibernéticos. O diálogo com diferentes atores, e a troca de experiência poderá apoiar no fortalecimento das estratégias de segurança cibernética. Além disso, a E-ciber prevê, como ação estratégia do governo federal, a criação de centros de pesquisa em segurança cibernética, reforçando a necessidade de constante atualização e investigação de assuntos relacionados, que podem ser fomentados por órgãos e entes da administração pública, a partir de investimentos com fundos públicos em pesquisa na área de segurança cibernética (outra ação estratégica prevista na E-ciber)
Estabelecer mecanismos de participação da sociedade nas definições de segurança cibernética	E-ciber/E-gov	Ação estratégica relacionada: Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade/ Objetivo 14 — Participação do cidadão na elaboração de políticas públicas	Destaca-se esta ação da E-ciber por conta da sua relação com as recomendações sobre participação social pública no Plano de Dados Abertos elaborado pelo órgão ou ente público. Trazer informações sobre possíveis técnicas de segurança e, por exemplo, interferências na privacidade, para apreciação social, pode ser uma ótima estratégia de elaborar arranjos de segurança contextuais

Indicação de gestor de segurança da informação	PNSI/E-ciber/ PPSI	art. 15, III (PNSI); art. 6º, II (PPSI); ação estratégica relacionada: Fortalecer as ações de Governança Cibernética	Ator/atriz com atribuição de administrar os controles de segurança da informação de ativos de informação
Indicação de gestor de tecnologia da informação e comunicação	PPSI	art. 6º, I	Agente cuja responsabilidade primordial, dentre outras, é administrar os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicação — atividade, portanto, que inclui o planejamento, a implementação e o monitoramento em prol de melhorias contínuas
Indicação de encarregado pelo tratamento de dados pessoais e gestão de controles de privacidade em ativos que tratem dados pessoais	PPSI	art. 6º, III	Conferir itens 2.3, 2.4 e 2.5 deste Documento
Indicação de responsável pela unidade de controle interno	PPSI	art. 6º, IV	Atuação "no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017"

Instituição de comitê de segurança da informação	PNSI	art. 15, IV	É importante que este órgão de deliberação interna seja estabelecido não só para o Plano de Dados Abertos, mas para todo o arranjo de segurança cibernética do órgão ou ente. Assim, se recomenda que haja a criação de grupos de trabalho específicos para abertura de dados, com interlocução com outros órgãos deliberativos internos, como comitês de proteção de dados e privacidade, se existentes, ou órgãos de deliberação de questões políticas/ governança institucional. O comitê terá as atribuições previstas no art. 15, § 3º da PNSI
Destinar orçamento para instituição de medidas de segurança da informação	PNSI	art. 15, V	Previsão nos documentos estratégicos, conforme apresentado ao final da tabela
Realização e registro de auditorias	PNSI	art. 15, IX	A auditoria pode ser realizada tanto para verificação da atividade de usuária/os em nível de administração — verificar se está havendo violação a outros direitos —, como para verificação dos investimentos de verbas dotadas para segurança cibernética e também da efetividade das medidas adotadas
Instituição de mecanismos de responsabilização pelas atividades de segurança	PNSI	art. 17, III e art. 15, X	De acordo com a abordagem institucional, podem ser previstas consequências referentes à violação das políticas e normas de segurança cibernética internas, desde que aprovado pelos órgãos de governança do órgão ou ente

Uso de recursos criptográficos pelo órgão/instituição/ente	PNSI/E-ciber	art. 17, par. 1º, (PNSI); Ação estratégica relacionada: Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade (E-ciber)	É importante que a adoção de técnicas de segurança priorizem a manutenção da criptografia das comunicações, a fim de respeitar a obrigação. A E-ciber fala ainda no papel do governo na promoção do estímulo do uso de criptografia para comunicação de assuntos sensíveis pela sociedade em geral
Garantir mecanismos de interoperabilidade das informações (valorizando acesso por organizações da sociedade civil, movimento sociais, e outros órgãos/ entidades que possam acessar os dados)	PNSI	art. 17, par 1º, IV	Esta obrigação é de responsabilidade da alta gestão dos órgãos entidades da administração pública, e é incorporada nas obrigações de planejamento das ações de segurança cibernética
Integração e compartilhamento de ativos, redes e sistemas do governo (sistema gov.br)	PNSI	art. 17, par 1º, IV, a	Essa obrigação se relaciona com as disposições da E-Gov (objetivo 4), que preveem a unificação de sistemas, e a criação de acesso único para sistemas integrados ao gov.br (nesse caso, entendemos que é um ponto de atenção para Plano de Dados Abertos apenas da administração Pública Federal)
Uniformização e redução da fragmentação das bases de dados	PNSI	art. 17, par 1º, IV, b	Estas são obrigações da alta gestão dos órgãos ou entes, que precisam ser endereçadas no planejamento de segurança cibernética, pontuado no final desta tabela

Esforços de padronização da comunicação entre sistemas	PNSI	art. 17, par 1º, IV, d	Estas são obrigações da alta gestão dos órgãos ou entes, que precisam ser endereçadas no planejamento de segurança cibernética, pontuado no final desta tabela
Estabelecer requisitos mínimos de segurança cibernética nas eventuais contratações para prestação de serviço sobre processos necessários para a abertura de dados	E-ciber	Ações estratégicas relacionadas: Fortalecer as ações de Governança Cibernética, Elevar o nível de proteção do Governo e Elevar nível de proteção do Governo	Entende-se que, junto às disposições contratuais, pode ser interessante elaborar listas detalhadas de normas de segurança mínima a serem seguidas por fornecedores de tecnologia da informação e comunicação (TICs), a fim de facilitar auditorias posteriores, para comprovar cumprimento das medidas
Auditar e acompanhar a atenção dos requisitos mínimos de segurança cibernética instituídos em contratos	E-ciber	Ações estratégicas relacionadas: Fortalecer as ações de Governança Cibernética, Elevar o nível de proteção do Governo e Elevar nível de proteção do Governo	É importante ter atenção a possíveis acessos indevidos ou desvios de finalidade eventualmente praticados por fornecedores contratados (ferramentas comerciais) para serviços ou funcionalidades de segurança cibernética

Realização de fóruns de governança e adoção de outras medidas para a promoção do diálogo entre diferentes atores da sociedade nesses fóruns e outros espaços (a estratégia fala em exercícios de simulação de incidentes cibernéticos)	E-ciber	Ações estratégicas relacionadas: Fortalecer as ações de Governança Cibernética, Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade, Elevar o nível de maturidade da sociedade em segurança cibernética	Esta ação estratégica dialoga com as obrigações de participação social, e estabelecimento de cooperação, e pode ser uma ótima forma de manter uma visão ampla e atualizada sobre ameaças, vulnerabilidades e ataques cibernéticos
Adoção de framework de privacidade e segurança da informação para compatibilização da privacidade e da segurança da informação	PPSI/PNSI	art. 7º, §4º (PPSI); art, 3º, II, art. 4º, I, art. 15, IV (PNSI)	Recomenda-se que o *Framework* de privacidade e segurança da informação do órgão ou entidade teça considerações específicas sobre prática de abertura de dados, que levem em consideração as recomendações apresentadas na seção 1, principalmente as preocupações de Plano de Dados Abertos, e seção 2 deste trabalho, principalmente as boas práticas em proteção de dados
Realizar autoavaliação pelo próprio órgão ou ente público em relação à privacidade e segurança da informação	PPSI	art. 9º, I	A autoavaliação deverá seguir o modelo de avaliação de maturidade e capacidade disponibilizado pela Secretaria de Governo Digital no âmbito do Programa de Privacidade e Segurança da Informação

Realizar análise de lacunas de privacidade e segurança da informação	PPSI	art. 9º, II	Nesta etapa, é importante que seja feita a avaliação das medidas que precisam ser implementadas e aprimoramento das medidas já adotadas (lembrando que há necessidade de compatibilizar a adoção dessas medidas com o direito à privacidade e à proteção de dados pessoais, inclusive das pessoas que acessam as plataformas de dados abertos)
Planejamento de implementação de medidas para reforço de privacidade e segurança da informação nas atividades do órgão ou ente	PPSI	art. 9º, III	Há necessidade de especificação de prazo de implementação das medidas, e indicação dos recursos orçamentários que precisarão ser implementados
Elaboração de plano de trabalho, privacidade e segurança da informação,	PPSI	art. 10	O plano de trabalho deve ser revisado a cada autoavaliação, e integrado a documento institucional como Plano de Transformação Digital, ou similares (art. 10, par. 1º).
Elaboração de plano de transformação digital, plano diretor de tecnologia da informação e comunicação e o referido plano de dados abertos (seção 1)	E-gov.	art. 3º, I, II, III	Os documentos são obrigações instituídas pela Estratégia de Governo Digital (vigente até 2023), e devem prever disposições acerca dos arranjos institucionais sobre segurança cibernética (incluindo preocupações de caráter orçamentário e definições gerais de prioridades)

1.1. Política Nacional de Segurança da Informação — Decreto nº 9.637/2018

A Política Nacional de Segurança da Informação (PNSI) é um texto normativo que se baseia na tríade consolidada de CIA, que é a sigla em

inglês para disponibilidade, integridade e confidencialidade das informações, preocupando-se igualmente com sua autenticidade. As atenções do Decreto são voltadas, essencialmente, para segurança e defesa cibernética (às quais não é dado maior detalhamento conceitual), à segurança das infraestruturas críticas, segurança de informações "sigilosas" e proteção contra vazamento de dados (art. 6º, I à V) organizacionais (art. 2º, III).

O Decreto do PNSI institui a competência dos órgãos envolvidos na realização de atividades necessárias à efetivação da Política de Segurança Nacional. Dentre essas atividades do Gabinete de Segurança Institucional da Presidência (GSI), constam, exemplificativamente, a necessidade de definição de requisitos metodológicos para gestão de riscos de ativos, o estabelecimento de critérios para monitorar e avaliar a execução da Política de Segurança, além de estabelecer os requisitos mínimos de segurança para garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (art. 12, I, VII e IX respectivamente). A auditoria dessas atividades, por sua vez, caberá à Controladoria Geral da União, conforme disposto no artigo 14 do Decreto.

A cooperação entre diferentes entes e atores da sociedade — comunidade científica, atores da sociedade, órgãos e entes da administração pública —, e com a comunidade nacional e internacional, é apontada tanto como princípio (art. 3º, XIV, XV, XVI), quanto como objetivo da Política (art. 4º, II), ao prever o fomento à "pesquisa científica", ao "desenvolvimento técnico" e "inovação" relacionadas ao campo de segurança. A PNSI favorece a cooperação em diferentes momentos do texto normativo, inclusive ao propor que mesmo as atividades de "prevenção, tratamento e resposta a incidentes cibernéticos" deverão acontecer com a interlocução de diferentes órgãos do Poder Executivo (art. 17, § 1º, III).

Há, no entanto, uma aparente centralidade da Presidência da República, expressa não apenas na referida previsão de interlocução dos atores do executivo, mas também diante da centralidade da figura do Gabinete de SI da Presidência da República, pela previsão de obrigatoriedade de "órgãos e as entidades da administração pública federal direta, autárquica e fundacional, nos atos administrativos que envolvam ativos de tecnologia da informação" incorporarem normas do Gabinete de SI (art. 18), bem como na própria composição do Gabinete de SI que, após alterações promovidas

em 2019, passa a concentrar a composição com órgãos vinculados diretamente à Presidência (art. 9º).

Insta salientar que esse texto normativo revoga o Decreto nº 8.135/2013, que determinava que a "comunicação de dados da administração pública federal direta, autárquica e fundacional" deveria ser feita apenas baseada em infraestruturas fornecidas por "órgãos ou entidade da administração pública federal, incluindo empresas públicas e sociedade mistas da União e suas subsidiárias". Já na PNSI, o Gabinete de SI da Presidência tem como uma de suas funções a articulação com "centros nacionais de prevenção, tratamento e resposta a incidentes cibernéticos pertencentes a outros países" (art. 12, X), além de "acompanhar a evolução doutrinária e tecnológica, em âmbito nacional e internacional" (art. 12, IV). Revoga-se também a Política de Segurança da Informação instituída pelo Decreto nº 3.505/2000, que não se limitava a uma abordagem de garantia de direitos individuais – como parece ser o caso do atual Decreto, quando menciona a proteção de pessoas, e não somente sistemas e dados –, e mencionava a garantia de direitos coletivos. Diante do atual cenário em que há possibilidade para avanços na agenda de regulação de cibersegurança no país (Belli *et al*., 2023), é possível que esses encaminhamentos (indesejáveis) de dados pelo governo anterior sejam superados.

1.1.1 Política de Segurança da Informação para abertura de dados

Conforme apresentado na Tabela I, além de ser um instrumento essencial para apoiar a organização dos arranjos institucionais de segurança cibernética, a elaboração das políticas de segurança cibernética é uma obrigação legal. De acordo com a E-ciber, é importante que as políticas, elaboradas de acordo com o contexto específico da instituição, prevejam (sem prejuízo de outros elementos):

- "Métricas, mecanismos de avaliação e revisão periódica" dos sistemas, que envolvam a adoção de mecanismos automatizados para atualização, sempre que disponível, dos "sistemas informacionais, as infraestruturas e os sistemas de comunicação", para realização de "cópias de segurança" "segregadas" (com os mesmo níveis de segurança) das informações disponibilizadas e dos sistemas

necessários para apoiar a abertura de dados (com principais ações estratégicas relacionadas, enumeram-se: elevar os níveis de proteção do Governo e de proteção das infraestruturas críticas nacionais).

- Criação de medidas de controle de acesso às informações, adotar níveis de restrição ao acesso às informações, prever o uso de *endpoints*[103] pelo ente federativo e ampliar o uso do certificado digital pelos atores envolvidos na procedimentalização da abertura de dados — que poderia ser solicitado, no entanto, para acesso a determinados dados, por determinados atores (como principais ações estratégicas relacionadas: fortalecer as ações de Governança Cibernética e elevar o nível de segurança).
- Adoção de técnicas nacionais de criptografia das informações disponibilizadas e da base de dados principal, observando a legislação, caso existente (a principal ação estratégica relacionada é: fortalecer as ações de Governança Cibernética).
- Adoção de medidas que possibilitem a interoperabilidade das "informações em diferentes níveis", inclusive entre os diferentes órgãos do ente federativo que pretende abrir dados acerca de suas atividades, ou de usuários de serviços públicos, incentivando o "uso dos dispositivos de comunicação segura" (as principais ações estratégicas relacionadas são: promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade e elevar o nível de proteção do Governo).
- Observar os padrões de segurança internacionais para o desenvolvimento dos sistemas necessários para disponibilização dos dados — padrões dos quais serão explorados mais adiante (são as principais ações estratégicas relacionadas: fortalecer as ações de Governança Cibernética e elevar o nível de proteção do Governo)[104].

103 O termo "*endpoints*", em uma tradução literal, significa "ponto de extremidade" ou "ponto final". São dispositivos conectados em redes privadas ou corporativas para transmissão de dados (TEIXEIRA, Álvaro. O que é um *endpoint* em TI? Disponível em: https://tecnoblog.net/responde/o-que-e-um-endpoint-em-ti/).

104 É possível que existam regulações locais que tragam outros elementos essenciais nas políticas de segurança da informação dos órgãos vinculados ao ente federativo emissor da regulamentação. É o caso do art. 10º, da IN 2 do PRODRJ, do Estado do Rio de Janeiro.

Apesar da relevância desse documento, é importante ressaltar que se trata de texto com linguagem técnica e que, pela necessidade de prever uma série de medidas, conceitos, métricas, obrigações, é invariavelmente longo. Ante o exposto, considera-se de suma importância que a elaboração e a publicação deste instrumento venham acompanhadas de outros meios e suportes de comunicação acerca das principais disposições da respectiva Política de Segurança do órgão, ente ou instituição do Poder Público, no intuito de possibilitar a compreensão efetiva do seu conteúdo.

- Outro exemplo, apresentado enquanto ação estratégica pela própria E-ciber, é o incentivo na adoção de comportamentos seguros por meio de campanhas (preferencialmente institucionalizadas em políticas públicas) de conscientização, não somente dos agentes do poder público envolvidos nas atividades de abertura de dados, mas da sociedade como um todo. A estratégia fala igualmente da inclusão do tema de segurança na educação básica e criação de programas e eventos de capacitação no tema (como principal ação estratégica relacionada: elevar o nível de maturidade da sociedade em segurança cibernética). É importante que esta inclusão seja feita de forma crítica, e que seja acompanhada de práticas educativas que ensinam a programação para crianças e adolescentes (Belli *et al*. 2023).
- Por fim, deve-se incentivar a criação de tecnologias de segurança cibernética — tecnologias emergentes —, que permitam a interoperabilidade dos dados, com uso de técnicas de criptografia da informação nacionais, conforme proposição da E-ciber (como principais ações estratégicas relacionadas: incentivar a concepção de soluções inovadoras em segurança cibernética e elevar o nível de maturidade da sociedade em segurança cibernética). Entende-se que programação e cocriação de técnicas de segurança pela própria população representa uma forma de fomentar a adoção de técnicas mais apropriadas às verdadeiras ameaças e prioridades do contexto brasileiro.

1.1.2. Estratégia Nacional de Segurança Cibernética (E-Ciber) — 2020-2023

A Estratégia Nacional de Segurança Cibernética (E-Ciber) foi instituída pelo Decreto nº 10.222/2020 para atender à determinação da PNSI, que prevê que a Política deverá valer-se de uma Estratégia de Segurança da Informação enquanto instrumento para sua procedimentalização – refere-se ao primeiro dos cinco módulos a que a PNSI faz referência (*i.e.*, a segurança cibernética). Uma vez que tem sua validade para o final de 2023, defende-se que não há urgência na adequação ao documento normativo, para fins de abertura de dados pelo Poder Público, haja vista que os requisitos impostos perderão vigência neste ano. Portanto, na Tabela I, selecionaram-se as disposições da E-Ciber que, na opinião das autoras, apoiam na compreensão de boas práticas de promoção de segurança nas atividades de abertura de dados[105].

A partir da realização do que é chamado de um diagnóstico do "estágio de maturidade" e das "necessidades do país em segurança cibernética e os aspectos relativos ao ecossistema digital, no âmbito nacional e internacional", o texto da E-Ciber propõe 10 eixos de ações estratégicas que devem ser observadas pelos órgãos do poder público e do "setor privado", para que possam operacionalizar os objetivos da estratégia:

> 1. Tornar o Brasil mais próspero e confiável no ambiente digital;
>
> 2. Aumentar a resiliência brasileira às ameaças cibernéticas; e
>
> 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional. (Brasil, 2020)

105 Foram suprimidas as ações relativas à centralização das competências de segurança na figura do Gabinete de Segurança Institucional da Presidência da República (tendo em vista que, diante da atual mudança de governo, há expectativa de que tal concentração de competências seja minimizada). Outras ações estratégicas suprimidas foram aquelas que fazem referência à adoção de medidas de proteção de dados pessoais (como desenvolvimento de técnicas observando padrões de *privacy by design*) - por serem preocupações pertinentes à proteção de dados pessoais - bem como aquelas que falam de Centros de resposta a incidentes vinculados ao Governo Federal (já que, não necessariamente, o órgão de abertura será um ator em nível federal). Também pela impressão de que não se deve seguir a mesma postura militarizada nas ações de segurança sobre a abertura de dados em meio digital, não destacamos medidas de combate a crimes cibernéticos.

A E-Ciber reforça a ampliação de uma cooperação multissetorial para estudo sobre segurança em atividades com meios digitais, parcerias para investimento e desenvolvimento de medidas de segurança cibernética e para "implantação de programas, projetos e ações em segurança cibernética, que alcancem toda a sociedade", para além de grupos de trabalho e reuniões (principal ação estratégica relacionada: ampliar a parceria em segurança cibernética, entre setor público, setor privado, academia e sociedade). No entanto, submetida à PNSI, acaba por replicar a mesma centralidade dada por esta política às parcerias com o setor empresarial. Este tipo de abordagem pode enfraquecer pressupostos à segurança cibernética, como a soberania digital, que pode ser fortalecida pela ampliação do uso de ferramentas de software livre, diálogo com os diversos setores e com a própria sociedade, entre outros (Belli *et al.*, 2023).

Por outro lado, há recomendação de ações voltada para cooperação internacional — com destaque à cooperação com países da América Latina — e para proteção de infraestruturas críticas, as quais poderiam ser aproveitadas também para as infraestruturas digitais que apoiam a abertura de dados, principalmente a depender da natureza das informações que sejam disponibilizadas — seja pelo alto interesse público em sua disponibilização, seja pela sensibilidade dos dados pessoais eventualmente divulgados (elencam-se como principais ações estratégicas relacionadas: elevar o nível de proteção das infraestruturas críticas nacionais e ampliar a cooperação internacional do Brasil em segurança cibernética).

1.1.3 Estratégia de Governo Digital — 2020-2023

Assim como a E-Ciber, a Estratégia de Governo Digital encerra sua vigência este ano (2023). Nada obstante, uma série de críticas aos objetivos previstos podem abrir margem para centralidade da atuação do setor privado, e consequente priorização de interesses mercadológicos, na digitalização governamental (alguns exemplos são os objetivos 1.2., 7.2. e 15) também para coleta massiva de dados que permitem rastreabilidade das pessoas (objetivo 12).

No entanto, apresenta-se o decreto devido à previsão da obrigatoriedade de dos órgãos da Administração Pública federal elaborarem documentos institucionais, como os Planos de TIC e de Inovação, nos quais deverão

constar planejamentos relativos à segurança cibernética. Reforça-se que, ainda que estes instrumentos normativos não sejam cogentes aos órgãos das esferas estaduais ou municipais, suas disposições eventualmente serão refletidas em instrumentos normativos emitidos pelos respectivos entes normativos. Isso justifica a relevância de dedicar atenção às obrigações instituídas pelo arcabouço regulatório federal.

1.1.4. Programa de Privacidade e Segurança da Informação — Portaria SGD/MGI nº 852/2023

O objetivo do Programa de Privacidade e Segurança da Informação (PPSI) é aumentar a maturidade e a resiliência relativa à privacidade e à segurança da informação desses atores (art. 3º). A respectiva meta é prescrita como dois dos valores do PPSI, ao lado da efetividade, da colaboração e da inteligência (art. 4º, §2º).

A PPSI institui o "Framework de Privacidade e Segurança da Informação", formado pelo conjunto de controles, metodologias e instrumentos de suporte (art. 7º, *caput*). O arranjo deverá conformar a Lei Geral de Proteção de Dados (LGPD), a Política Nacional de Segurança da Informação (PNSI), e atender às normativas emitidas como, por exemplo, pela Autoridade Nacional de Proteção de Dados Pessoais (art. 7º, §4º). O texto prevê que todos os controles que integrarão o *Framework* estarão disponíveis no portal da Secretaria do Governo Digital (art. 7º, §2º).

Os órgãos e entidades alcançados pela Portaria deverão implementar esse *Framework*, podendo esquivar-se de medidas obrigatórias apenas na hipótese de justificativa adequada e fundamentada em análise de risco (art.8º). A etapa de planejamento indicada na Tabela I deverá contemplar os prazos e as necessidades de recursos orçamentários e de pessoas — esse "plano de trabalho" deverá ser enviado à Secretaria de Governo Digital (que poderá realizar alterações (art. 10, *caput*, e 12), e deve ser revisado a cada 12 meses (art. 10, §5º). A portaria recomenda que o documento seja considerado sigiloso pelo órgão ou ente público (art. 10º, § 4º). As três primeiras fases de adoção do *Framework* (*i.e.*, autoavaliação, análise e planejamento) deverão ser executadas no prazo de 180 dias, a contar de 03 de

abril de 2023 (data de início da vigência da Portaria), com possibilidade de prorrogação por igual período, mediante motivação (art. 9º, §2º).

Criou-se também, pelo PPSI, o Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br, art. 13) e o Centro de Excelência em Privacidade e Segurança da Informação (art. 19). O "CISC Gov.br", é uma "unidade de coordenação operacional das equipes de prevenção, tratamento e resposta a incidentes cibernéticos" dos órgãos e entidades do SISP, aos quais deverão ser notificados eventuais incidentes em relação aos sistemas e infraestruturas digitais que sustentam a abertura de dados. Os órgãos ou entes podem recorrer aos serviços de apoio em relação aos incidentes cibernéticos ao CISC, bem como realização de testes de penetração, além de outros testes "estáticos e dinâmicos de segurança" em outros serviços estão no escopo do órgão, conforme artigo 16.

O segundo, trata-se de unidade incumbida de promover a cultura de privacidade e segurança da informação nesses órgãos e entidades por meio de, dentre outras ações: *i)* busca por parcerias; *ii)* ações de sensibilização, conscientização, capacitação e especialização de profissionais, bem como de disseminação de conhecimentos de boas-práticas; *iii)* apoio na implementação dos controles de privacidade e segurança da informação e na promoção do engajamento voltado à mudança cultural; e *iv)* organização de fóruns especializados para facilitar o intercâmbio de conhecimentos e vislumbre de oportunidades, e de "exercícios conjuntos de simulação cibernética" (art. 20).

A PPSI prevê que as omissões do texto normativo serão solucionadas pela Secretaria de Governo Digital (art. 21).

1.1.5. Rede de Gestão de Incidentes Cibernéticos — Decreto nº 10.748, de 16 de julho de 2021

O Decreto nº 10.748/2021, que institui a Rede de Gestão de Incidentes Cibernéticos, regulamenta a obrigação imposta no art. 15, inciso VII, da PNSI, em instituir equipe de prevenção, tratamento e resposta a incidentes. Atribui-se à Rede de Gestão de Incidentes de Cibernéticos a função de coordenar a prevenção, o tratamento e a resposta a incidentes cibernéticos entre órgãos e entidades da administração pública direta, autárquica e fun-

dacional (art. 2º), no intuito de aprimorar os níveis de segurança cibernética dos ativos informacionais sob custódia. Enquanto há obrigatoriedade de órgãos e entidades da administração pública direta, autárquica e fundacional integrarem a rede, a adesão de empresas públicas e sociedades de economia mista e subsidiárias é voluntária.

Pela leitura de seus objetivos (art. 3º), identifica-se um comprometimento com *i)* a conscientização, devido à pretensão de divulgar medidas protetivas, avisos relativos às vulnerabilidades e aos ataques cibernéticos; e com *ii)* o apoio na promoção da cooperação entre os participantes da Rede e da celeridade na resposta de incidentes cibernéticos.

O Decreto, no artigo 15, dispõe que todas as informações específicas relativas aos incidentes cibernéticos, bem como sobre as configurações e características técnicas de ativos de informação de cada órgão ou entidade da administração pública federal direta, autárquica e fundacional, são "imprescindíveis" à segurança da sociedade e do estado. Portanto, os respectivos dados informacionais apenas serão acessados por profissionais autorizados pelos responsáveis pelos ativos (controle de acesso privilegiado). Somente dados estatísticos de interesse público serão publicizados em sítio eletrônico pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

1.1.6. IN nº 2/2022 PRODERJ — Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Com ênfase à proteção de ativos e à segurança individual, a IN 2/2022 considera a informação um ativo do Estado e estabelece o PDCA (*Plan-Do-Check-Act*) como principal metodologia para implementação, na prática interna de cada órgão, das atividades de segurança (art. 10, parágrafo único). O documento dispõe de medidas mais práticas,[106] de ordem mais específica em comparação com o PNSI, que deveriam ser implementadas no prazo de 120 dias para a sua implementação por cada órgão, a partir de

106 Alguns exemplos de obrigações que trazem maior concretude às boas práticas de segurança cibernética são: instituição de cópias de segurança (backup), armazenadas em base lógica separada ("local protegido") (art. 6º); descarte seguro - sem, no entanto, trazer maiores complementações sobre tal eliminação (art. 7º); segurança de senhas (art. 8º) - sem necessariamente remeter à necessidade de adoção de senhas complexas; a necessidade de

28 de abril de 2022. Reforça-se que, embora seja improvável que esta Instrução Normativa proponha práticas de segurança cibernética que atribuam necessária centralidade na garantia de direitos,[107] trata-se de um exemplo para alertar sobre a necessidade de verificar obrigações normativas em termos de segurança cibernética, instituídas em âmbito local.

A abrangência anunciada da Instrução Normativa nº 2 do PRODERJ é bastante similar àquela disposta no texto da Política Nacional de Segurança da Informação. Contudo, na Instrução Normativa de 2022, nota-se a influência da Lei Geral de Proteção de Dados nos princípios e alcance daquilo que se busca assegurar através daquela (IN nº 2). Contempla ainda mais centralidade à proteção das pessoas, na medida em que a dignidade da pessoa humana e a garantia de direitos fundamentais previstos no art. 5º da CRFB são incorporadas enquanto princípios norteadores da segurança cibernética de órgãos e entidades vinculadas à Administração Pública do Estado do Rio de Janeiro.

Na IN nº 2, do Estado do Rio de Janeiro, intitula-se novo ator de governança, para além daqueles já identificados (encarregado de tratamento de dados, gestor de segurança da informação, e gestor de TIC), qual seja, a figura específica responsável pelo Tratamento e Resposta a Incidentes (art. 11, VI, b), função que, na Política Nacional de Segurança da Informação, era uma das atribuições do gestor de segurança da informação. Este/a ator/atriz de governança tem como responsabilidades:

- inventariar os recursos de TICs, exigidos para o monitoramento previsto no artigo 18, I;
- detectar e analisar incidentes de segurança, além de comunicar incidentes que envolvam dados pessoais ao encarregado pelo tratamento de dados pessoais (art. 18, I e II);

atualização das políticas - além de determinar com que periodicidade os documentos serão revisados, para determinar novos atores e normas de segurança (art. 10º caput e art. 11, VIII); obrigação de assinatura de Termo de Responsabilidade para todas as pessoas que atuem no órgão (art. 14); divulgação aberta das normas de segurança(art. 13), em respeito ao princípio da publicidade (art. 2º).

107 Para além da adoção de uma linguagem de ameaças de segurança (com medidas de "defesa cibernética"), a IN 2 indica militares enquanto agentes responsáveis por gerir a segurança da informação e pelo tratamento e resposta de incidentes (Art. 17, parágrafo único, e 18, parágrafo único, respectivamente). Sobre análise de discurso da cibersegurança (enquanto aproximação da segurança cibernética, conceito do qual nos valemos), e as relações analógicas que caracterizam tais discursos, cf Betz; Stevens, 2013.

- identificar as vulnerabilidades nos sistemas de TIC (art. 18, III);
- criar canal de comunicação para notificações de incidentes — para os quais o responsável pelo tratamento e resposta de incidentes deverá propor respostas (art. 18, IV).

A necessidade de uma abordagem contextualizada para definição dos controles de segurança na prática é anunciada não somente na obrigação de diferentes órgãos emitirem suas próprias normas de segurança, mas também na afirmação da IN de que "os procedimentos de segurança", adotados por todas as pessoas envolvidas nas operações com informações, devem ser alinhados com a "natureza, finalidade e ao planejamento estratégico" (art. 12) da atuação de cada órgão específico. Essa contextualização, no entendimento das autoras, é desejável, ao abrir espaço para que sejam centralizadas preocupações com coletividades específicas, que poderiam ser mais afetadas diante de determinados contextos concretos de tratamento.

1.1.7. Boas práticas sociotécnicas de segurança da informação

No âmbito das relações públicas e privadas, as organizações têm buscado outros mecanismos, além da legislação e regulação, para orientar suas atividades digitais com maior segurança. Para isso, empenham-se (ou deveriam se empenhar) para *i)* seguir guias relativas às boas práticas referentes a questões plurais administrativas como, por exemplo, continuidade do negócio, gestão da qualidade e da segurança da informação, sejam essas diretrizes gerais ou setorizadas, locais ou globais; *ii)* obter certificações ao seguir modelos de sistemas e estruturas destas guias, seja para as organizações como um todo, seja para áreas específicas, projetos (como abertura de dados) ou profissionais, agregando, dessa maneira, valor e confiança às atividades prestadas;[108] *iii)* aderir a códigos de conduta produzidos por

108 Como exemplo, cita-se a *Certified in Risk and Information Systems Control* (CRISC), guia de base para a certificação de profissionais com atuação em gestão na área da tecnologia da informação e outros. Nesta, exigem-se conhecimentos correlatos à governança corporativa; tratamento de riscos relativos à tecnologia da informação; respostas e reporte de ameaças e vulnerabilidades; e,

elas próprias (internamente) ou, preferencialmente, por grupos multissetoriais e, portanto, que possibilitem uma visão plural e interdisciplinar sobre a matéria; *iv)* assinalar contratos com cláusulas-tipo (padronizadas); e *v)* adotar regras corporativas vinculativas.

De forma geral, essas soluções são relativamente objetivas, exceto quanto aos respectivos conteúdos e instrumentos de implementação — à substância dos controles propostos como boas práticas. Tais soluções, portanto, serão definidas de maneira contextualizada, de acordo com as urgências e dores institucionais. Conquanto, justamente em face dessa subjetividade secundária, a escolha da melhor opção pode demandar esforços hercúleos. Até mesmo porque a infinidade de controles de segurança da informação previstos nas guias e padrões demandam um conhecimento técnico e institucional,[109] haja vista linguagem pouco acessível e acesso aos conteúdos de parte dessas normas não serem gratuitos.

Ante o exposto, portanto, apresentar-se-á, ainda que sucintamente, alguns modelos de padronização internacional. Para tal, cabe, por amostragem, a partir do modelo da ISO 27.001, padrão de sistema de gerenciamento da segurança da informação, tecer comentários sobre as suas recomendações primordiais, costurando com outro referencial largamente utilizado por diversas instituições: o NIST[110] Cybersecurity Framework (CSF), estrutura que se dedica ao aperfeiçoamento da gestão de riscos de

questões relacionadas ao alinhamento das práticas e visões organizacionais à gestão da tecnologia e segurança da informação. Precisamente sobre a segurança da informação, elencam-se como eixos centrais *i)* conceitos, estruturas e padrões de segurança da informação; *ii)* treinamentos para conscientização; *iii)* gestão da continuidade de negócios; e *iv)* princípios de privacidade e proteção de dados. Haja vista a menção à gestão de risco, resgata-se o ciclo necessário de, primeiro, definir o contexto para, assim identificar, analisar, avaliar, tratar, comunicar e monitorar os riscos. Disponível em: https://www.isaca.org/credentialing/crisc

109 A título ilustrativo, van den Berg (2020), que defende uma abordagem de cibersegurança focada na promoção de atividades seguras no meio digital, elenca como exemplos de comportamentos seguros para atingir esse objetivo. São eles: "nunca clicar num URL em um e-mail; minimizar ou descontinuar o uso de USB drives; sempre escolher senhas fortes; proteger e armazenar senhas adequadamente; limitar ou interromper a realização de downloads de arquivos diretamente da internet; realização de backups regulares; proteger dispositivos eletrônicos adequadamente; e monitorar cuidadosamente transações, abastecimentos, produções e processos de entrega; e atividades na *dark web*, entre outros" (van den Berg, 2020, p. 31, tradução nossa).

110 *National Institute of Standards and Technology* (NIST).

segurança cibernética em infraestruturas críticas,[111] igualmente utilizado por organizações de outros setores ou pela sociedade.

Nesta esteira, apenas em 2005, a ISO/IEC 27001, dedicada ao gerenciamento da segurança da informação, é criada, tornando-se, hodiernamente, uma das normas ISO mais populares[112] — o que evidencia sua relevância atual, haja vista contar com 167 países-membros, incluindo o Brasil — passível de certificação. Trata-se de documento que alcança todos os tipos de organizações[113] e que, embasada em riscos, traz requisitos para implementação de controles que podem ser aplicados tanto nas empresas, de modo integral, quanto em segmentos específicos dessas.[114]

Embora se entenda que a visão gerencial em riscos não seja necessariamente desejável no contexto do Poder Público, por reproduzir uma lógica mercadológica, a ISO/IEC 27001:2005 poderá apoiar a abertura de dados por órgãos ou entes públicos, na medida em que contempla o uso nas organizações *i)* para formular requisitos e objetivos de segurança; *ii*) para garantir a conformidade com leis e regulamentos, bem como uma gestão de risco que seja econômica; *iii)* como uma estrutura de processo para a implementação e gerenciamento de controles para garantir que os objetivos de segurança específicos de uma organização sejam atendidos; *iv)* para identificação e compreensão de processos de gestão de segurança

111 Conforme definição do *US Patriot Act*, de 2001, infraestruturas críticas são "sistemas e ativos, sejam eles físicos ou virtuais, tão vitais para os Estados Unidos que a incapacidade ou destruição de tais sistemas e ativos teria um impacto debilitante sobre a segurança econômica nacional, saúde e segurança pública nacional, ou na combinação de qualquer uma dessas áreas" (42 U.S.C § 5195c(e)). Os EEUU identificam 16 setores como de infraestrutura crítica: setor químico; instalações comerciais; comunicações; manufatura crítica; presas/barragens; base industrial de defesa; serviços de emergência; energia; serviços financeiros; comida e agricultura; instalações governamentais; saúde e saúde pública; tecnologia da informação; reatores nucleares, materiais e resíduos; sistemas de transporte; sistemas de água e águas residuais. *Homeland Security, Setores de infraestructura crítica*. Disponível em: https://www.dhs.gov/cisa/critical-infrastructure-sectors.

112 Disponível em: https://is.gd/ZvnRSU.

113 Exemplificativamente, citam-se as organizações comerciais, as sem fins lucrativos e as governamentais.

114 Embora se reconheça a relevância de outros padrões técnicos como, por exemplo, o "NIST Cybersecurity Framework", cuja primeira versão foi publicada em 2014, pelo "National Institute of Standards and Technology", dos Estados Unidos da América, o presente trabalho se ampara na documentação ISO/IEC 27000, tendo em vista seu alcance - contando com 167 países-membros, incluindo-se o Brasil.

da informação já existentes ou novos; *v)* para fornecer informações relevantes sobre políticas, diretivas, padrões e procedimentos de segurança da informação para parceiros comerciais e outras organizações com as quais se mantém qualquer interação operacional ou comercial; *vi)* como instrumento de avaliação do grau de aderência e *status* das atividades de gerenciamento de segurança da informação na organização.[115] Portanto, apesar dessas normas não proporcionarem a centralidade necessária à proteção de direitos de todas as pessoas — e afunilar as preocupações na proteção de ativos e atividades institucionais —, o conhecimento prévio delas é útil aos órgãos e entes públicos, para terem um ponto de partida de segurança cibernética na abertura de dados (mas não é suficiente).

A ISO/IEC 27001:2013, tratando-se de diretriz geral, determina a necessidade de *i)* compreender a organização e o seu contexto,[116] bem como as respectivas necessidades e expectativas – identificando-se as partes interessadas e relevantes para a segurança da informação; e *ii)* determinar o escopo do sistema de gestão da segurança da informação para, assim, elaborar, implementar, manter e continuamente adequar (melhorar) o respectivo programa. Frisam-se o papel de liderança e a demanda de comprometimento da Alta Direção.[117]

Pela norma, entende-se que a elaboração do sistema de segurança da informação, conforme Figura 1, deve seguir as fases de *i)* planejamento, determinando e avaliando os riscos e as oportunidades que merecem atenção; *ii)* tratamento de riscos de segurança da informação; *iii)* estabelecimento de objetivos de segurança da informação e de como alcançá-los; *iv)* determinação e provimento de recursos de apoio necessários (o que inclui a definição de competência de pessoas, os processos de conscientização, comunicação, documentação e respectivo controle); *v)* operação, avaliando e tratando os riscos em períodos predeterminados ou após a proposição de modificações, e o desempenho da segurança da informação e da eficácia do sistema de gestão implementado, bem como realizando auditorias internas e submetendo à análise crítica da

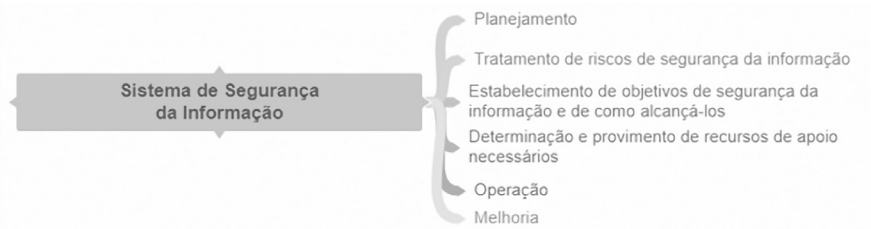
115 Disponível em: https://is.gd/ZvnRSU

116 Para determinação de contexto convém acessar o item 5.3 da ABNT NBR ISO 31000:2009, Gestão de Riscos - Princípios e diretrizes.

117 ISO/IEC 27.001:2013, p. 1-3.

Alta Direção; e *vi)* melhoria (contínua), atentando a não conformidade e à promoção de ações corretivas.[118] Para abertura de dados, este fluxo pode ser incorporado à adoção do *Framework* de privacidade (arranjo instituído pela PPSI) – tornando-o mais robusto quanto às etapas de elaboração do plano de trabalho.

Figura 1: Representação gráfica das fases de um Sistema de Segurança da Informação.



Essa organização sistêmica e cíclica é similar em todos os sistemas e estruturas padrão com enfoque no risco. O NIST CSF, por exemplo, sugere como funções simultâneas e contínuas ("estruturas básicas") de alto nível para abranger todos os objetivos de cibersegurança de uma organização: *i)* identificar e, portanto, desenvolver um entendimento organizacional para a administração dos riscos de cibersegurança de recursos como sistemas, pessoas e dados, *ii)* proteger com a implementação de medidas de segurança, *iii)* detectar e, dessa forma, definir as atividades necessárias para identificar o risco, *iv)* responder ao risco identificado e obter capacidade de contenção, e *v)* recuperar e, assim, restaurar eventuais danos provenientes de incidente de segurança e manter planos de resiliência.

De visão holística, a ISO/IEC 27001:2013 apoia-se em 14 categorias de controles: *i)* "política de segurança da informação"; *ii)* "organização da segurança da informação"*; iii)* "segurança em recursos humanos"; *iv)* "gestão de ativos"; *v)* "controle de acessos"; *vi)* "criptografia"; *vii)* "segurança física e do ambiente"; *viii)* "segurança nas operações"; *ix)* "segurança nas comunicações"; *x)* "aquisição, desenvolvimento e manutenção de sistemas"; *xi)* "relacionamento na cadeia de suprimento"; *xii)* "gestão de incidente de segurança da informação"; *xiii)* "aspectos de segurança da informação na

118 ISO/IEC 27.001:2013, p. 3-11.

gestão da continuidade de negócio"; e *xiv)* "*compliance*". Muitos desses controles podem ser identificados na Tabela II, que apresenta quais deles foram incorporados pelas políticas de cibersegurança brasileiras.

A "Política de Segurança da Informação" é o pilar estrutural do Sistema de Gestão de Segurança da Informação (SGSI). Devido à relevância, é cogente que este documento (ou o conjunto de normas que irão compor as diretrizes organizacionais sobre a matéria) seja aprovado pelo corpo diretivo do órgão ou ente público, publicado e comunicado amplamente para colaboradores, parceiros e demais terceiros com os quais se mantenham relações. Essa comunicação pode ser acompanhada dos cuidados apontados anteriormente.

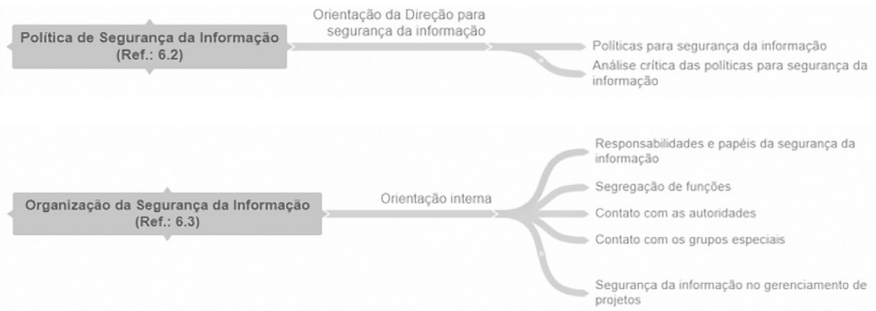
Seu desenho macro deverá pautar-se nas estratégias da organização, nas regras aplicáveis (sejam elas públicas — como, por exemplo, leis — ou privadas e, portanto, pela celebração de contratos, conforme refletido na PNSI), e na compreensão do ambiente de ameaças à segurança da informação. Deverá contemplar definições relevantes, objetivos, princípios, definição de papéis e responsabilidades,[119] contato de autoridades e grupos especiais, bem como processos de tratamento de adversidades. Acrescenta-se um necessário contato com a sociedade, principalmente nos casos de abertura de dados — já que, pautando-se no interesse público, a abertura deverá estar a serviço das pessoas (principais interessadas na divulgação de informações).

Frisa-se que o método de gerenciamento de projetos seja orientado desde o início, e por padrão, pela análise de riscos à segurança da informação (*by design*, ou seja, desde o desenvolvimento de sistemas e infraestruturas digitais, e *by default*, ou, em outras palavras, por padrão nas atividades digitais). Nos pormenores, convém que a política se ampare em alguns documentos temáticos que se adequem às especificidades da organização como, por exemplo, controle de acessos, *backup*, classificação da informação, transferência da informação, proteção contra *malware*, e outros. Os

119 Na atribuição de responsabilidades e papéis, recomenda-se que haja segregação de funções conflitantes, evitando conluio ou que uma única pessoa obtenha acesso ou detenha poder de modificação sem autorização específica ou possibilidade de monitoramento (ISO/IEC 27.001:2013, item 6.3.1.2, e ISO/IEC 27.002:2013, item 6.1.2).

documentos normativos deverão ser analisados crítica e periodicamente, com datas programadas e quando houver mudanças relevantes.[120]

Figura 2: Representação gráfica de categorias e subcategorias da ISO/IEC 27.001:2013, itens 6.2 e 6.3.

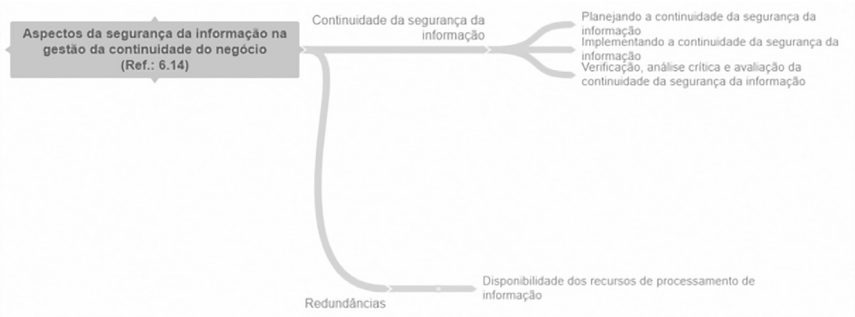


É importante haver preocupação com a continuidade da segurança da informação. Isso impõe a formalização do procedimento que deverá envolver análises críticas e testes. Como recomendação de garantia da disponibilidade, da integridade, da autenticidade e da confidencialidade dos recursos de processamentos da informação, menciona-se a importância de implementação com redundância (ou seja, a duplicação dos ativos digitais).[121] No entanto, frisa-se que, diferente do setor privado, a preocupação não deve ser centrada na "continuidade de negócio", conforme "Figura 3" (no caso, na continuidade da abertura de dados), mas na proteção das pessoas cujas informações são disponibilizadas (ainda que agregadas) – titulares –, e na manutenção de políticas sociais e serviços públicos que dependem destas informações.

120 ISO/IEC 27.001:2013, item 6.2, e ISO/IEC 27.002:2013, item 5.

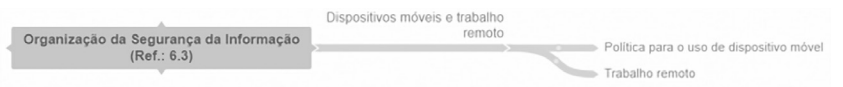
121 ISO/IEC 27.001:2013, item 6.14, e ISO/IEC 27.002:2013, item 17.

Figura 3: Representação gráfica de categorias e subcategorias da ISO/IEC 27.001:2013, item 6.14.



Atento ao "trabalho remoto", bem como à "utilização de dispositivos móveis", conforme "Figura 4", o padrão prescreve objetivamente a necessidade de elaborar uma política e implementar controles de apoio à segurança da informação. Elenca assuntos que deverão ser estudados no momento da redação do material. É evidente que alguns dos elementos previstos na ISO podem ser de difícil implementação no Brasil, devido às desigualdades socioeconômicas como, por exemplo, ao acesso a dispositivos físicos (celulares, computadores, tablets).[122] Por isso, a realidade local deve ser considerada no momento de definição dos controles, para que sejam efetivos.

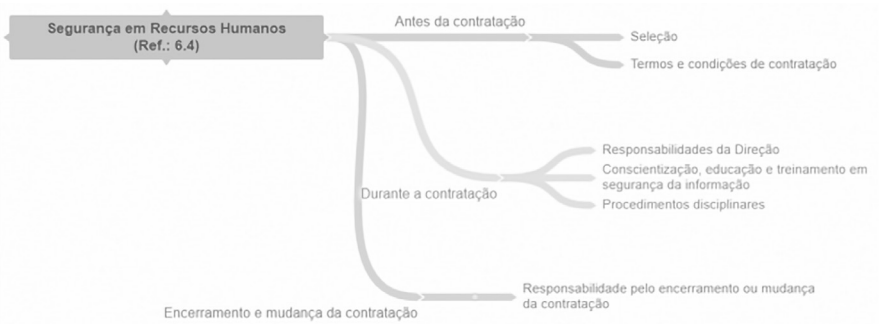
Figura 4: Representação gráfica de categorias e subcategorias da ISO/IEC 27.001:2013, item 6.3 (continuação).



122 Dentre eles, citam-se *i)* a importância de se manter registro dos dispositivos móveis; *ii)* quais serão os requisitos de proteção física; *iii)* limitações correlatas à instalação de *softwares* - atribuindo destaque aos seus versionamentos -, ao acesso em ambientes desprotegidos e requisitos de *firewall*; *iv)* implementação de proteção contra *malwares,* acessos indevidos (considerando-se, inclusive, familiares e amigos), bem como de sistema de desativação, bloqueios e exclusão remota; *v)* orientações sobre navegação em sites e utilização de sistemas; *vi)* uso de técnicas de autenticação e criptografia; *vii)* alerta e conscientização acerca de restringirem-se o uso de aparelhos e sistemas para fins profissionais; e outros (ISO/IEC 27.001:2013, item 6.3.2, e ISO/IEC 27.002:2013, item 6.2).

Sobre a "segurança em recursos humanos", a ISO 27001:2013 discrimina três momentos ilustrados na Figura 5: antes da contratação, durante a contratação e após o encerramento ou modificações da contratação. Frisam-se os objetivos de garantir que todos — colaboradores e terceiros — compreendam suas funções e responsabilidades, bem como de proteger interesses organizacionais. A norma novamente elenca uma série de controles, listados na "Figura 5" — os quais, reforça-se: devem ser implementados de acordo com as necessidades organizacionais e a realidade material local. Por exemplo: mais do que exigir determinados conhecimentos em processos seletivos[123] para contratação ou nomeação de profissional dedicado às atividades digitais de abertura de dados, é fundamental que o órgão ou ente público forneça as informações e condições necessárias para formação e preparação daquele, após o processo de contratação, ou investidura na função e antes do início de suas atividades com dados públicos.

Figura 5: Representação gráfica de categorias e subcategorias da ISO/IEC 27.001:2013, item 6.4.



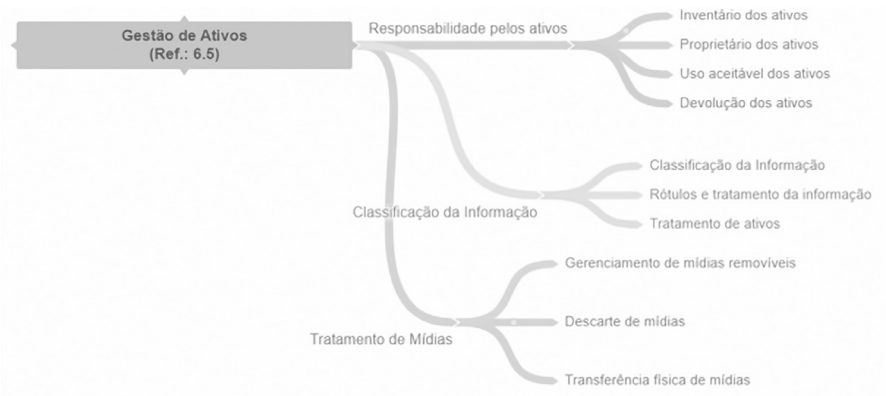
Para a "gestão de ativos", representada na "Figura 6", a norma sobreleva a importância da realização e manutenção de um inventário que contemple todos os ativos envolvidos no ciclo de vida das informações, com a devida classificação de relevância para a organização, indicação de proprietário (com designação de responsabilidades como as de registro, proteção, classificação e tratamento para destruição) e documentação referente ao seu

123 ISO/IEC 27.001:2013, item 6.4, e ISO/IEC 27.002:2013, item 7.

uso aceitável[124]. Reitera-se: são controles que podem ajudar a concretizar as obrigações instituídas pela regulação aplicável ao órgão ou ente público.

Com relação à classificação, especificamente às informações, é importante que esteja alinhada com as previsões do Capítulo IV, da Lei de Acesso à Informação, que define as hipóteses de restrição de acesso às informações mantidas pelo poder público (e objeto de abertura de dados).

Figura 6: Representação gráfica de categorias e subcategorias da ISO/IEC 27.001:2013, item 6.5.



O "controle de acesso", além de se tratar de uma obrigação legal (ao menos em âmbito federal), trata-se de uma boa prática prevista na ISO que contempla não somente a restrição de acesso às informações, mas igualmente aos recursos de processamento.

Para tal, conforme se verifica na "Figura 7", recomenda-se que seja elaborada uma política própria, analisada criticamente, envolvendo o gerenciamento de acessos lógicos e físicos, direitos e limitações conforme papéis e responsabilidades (segregação de funções e privilégios) — bem como respectivas remoções de acesso —, e regras para manutenção e gestão de registros de eventos relevantes acerca das identidades dos usuários e das autenticações secretas.

Para o gerenciamento de acesso do usuário, especificamente nas ações de registro e cancelamento de usuário, cabe garantir *i)* que cada usuário

124 ISO/IEC 27.001:2013, item 6.5.1, e ISO/IEC 27.002:2013, item 8.

possua um ID único; *ii)* que a remoção ou desabilitação do ID de usuário que tenha deixado a organização seja imediata; e *iii)* que os ID de usuários redundantes não sejam transmitidos para terceiros.[125]

Os materiais de boas práticas[126] também indicam a necessidade de criação de senhas complexas e, portanto, que tenham no mínimo oito caracteres, que incluam números, símbolos e letras, maiúsculas e minúsculas, sem sequências lógicas ou associações a datas ou nomes familiares, a serem alteradas periodicamente, não reproduzidas em outros ambientes (como, por exemplo, não usar a mesma senha para acesso em sistemas diferentes). A eventual implementação de autenticação multifator é igualmente desejável.

Em que pese a omissão no texto, as autoras sugerem a assinatura de termos de confidencialidade da informação, a autenticação secreta e a obrigação de alteração de senha temporária (que devem ser complexas e fornecidas de forma segura) logo no primeiro uso[127].

Sobre o procedimento seguro de entradas no sistema (*log-on*), é interessante destacar a orientação de uso de métodos alternativos de autenticação por senhas, como a criptografia, os *tokens* ou biometria e *smart cards*[128].

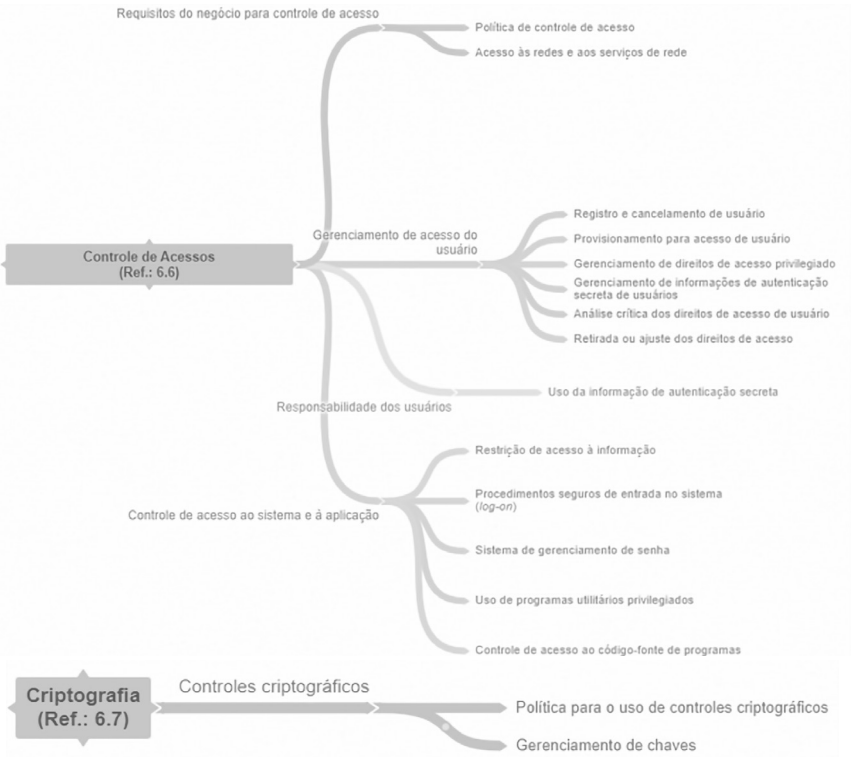
125 ISO/IEC 27.002:2013, item 9.2.1, p. 25-26.

126 As já mencionadas guias elaboradas pela MaraLAB, por exemplo, trazem indicações sobre como criar **e manter** senhas seguras Cf.: SHIRAKAWA, Fernanda; MONTEIRO, Fernanda; SANTIAGO, Larissa. GUIA PRÁTICA DE ESTRATÉGIAS E TÁTICAS PARA A SEGURANÇA DIGITAL FEMINISTA. CFEMEA e Universidade Livre Feminista, página 75.

127 ISO/IEC 27.002:2013, item 9.2.4, p. 28.

128 ISO/IEC 27.002:2013, item 9.4.2, p. 31.

Figura 7: Representação gráfica de categorias e subcategorias da ISO/IEC 27.001:2013, itens 6.6 e 6.7.



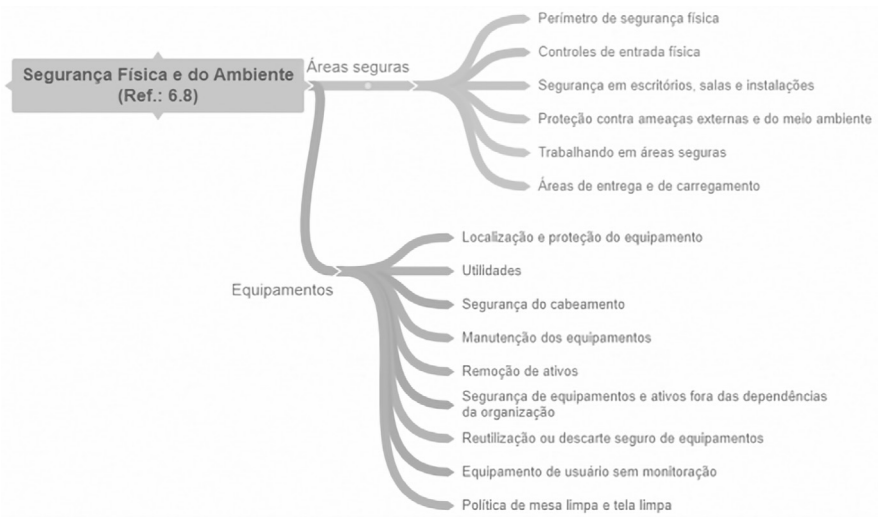
Como a ISO 27001:2013 reconhece que as informações não estão somente nos meios digitais, bem como que aparelhos e ambientes merecem proteção, ao abordar a "segurança física e do ambiente" ("Figura 8"), em "áreas seguras", identifica-se como objetivo a prevenção de acesso físico não autorizado, danos e interferências com os ativos de processamento da e na informação tratada pela organização.[129-130] Há ainda recomendações

129 Dentre as diretrizes prescritas para a implementação de perímetros físicos e demais cuidados, citam-se *i)* definição clara e precisa baseada na análise de risco; *ii)* que ambientes que contenham as instalações de processamento das informações sejam "fisicamente sólidos", portanto, com construções robustas e portas externas e janelas protegidas contra acessos não autorizados e sob monitoramento - projetadas igualmente contra desastres naturais, ataques maliciosos ou acidentes (ISO/IEC 27.002:2013, item 11.1.3, p. 40); *iii)* inclusão de recepção, onde convém que sejam registradas data e hora de entrada de visitantes, que o acesso a determinados ambientes sejam restritos e associados às necessidades e finalidades específicas de colaboradores que, inclusive, devem circular portando respectiva

práticas de proteção dos equipamentos contra perdas, danos e furtos, e contra a falta de energia elétrica e demais interrupções por falha de utilidades, remoções ou utilização externa (fora das dependências da organização), reutilização ou descarte seguro.[131]

Outra orientação relevante é a "política de mesa limpa e tela limpa", que sugere que papéis, mídias de armazenamento removíveis e recursos de processamento de informações sejam guardados em locais seguros, e que telas de dispositivos e/ou teclados sejam bloqueadas quando a pessoa que utiliza o equipamento se afastar (por exemplo, para ir ao banheiro, ir almoçar, beber água e outros).[132]

Figura 8: Representação gráfica de categorias e subcategorias da ISO/IEC 27.001:2013, item 6.8.



identificação pessoal visível; *iv)* incorporação de barreiras físicas e portas corta-fogo dotadas de monitoramento e alarme, conforme legislação nacional e local (ISO/IEC 27.002:2013, itens 11.1.1 e 11.1.2, p. 38-39); e *v)* discrição na identificação de lugares de processamento de informações ou de trabalho em áreas seguras (ISO/IEC 27.002:2013, item 11.1.5, p. 40-41).

130 ISO/IEC 27.001:2013, item 6.8, e ISO/IEC 27.002:2013, item 11 e 11.1.

131 ISO/IEC 27.001:2013, item 6.8, e ISO/IEC 27.002:2013, item 11.2.

132 ISO/IEC 27.002:2013, item 11.2.9, p. 47.

A ISO 27.001:2013 também endereça preocupações com relação à "segurança nas operações", em capítulo apartado no documento[133] ("Figura 9"). A recomendação primária é que as operações sejam documentadas e publicizadas aos usuários que dela necessitem. É fundamental que o órgão ou ente público que pretenda abrir dados realize *i)* o controle e a gestão dos processos de mudanças da organização, atentando-se aos requisitos de segurança da informação, garantindo respectivo registro, planejamento, teste e comunicação aos envolvidos;[134] e *ii)* implemente mecanismos céleres na identificação de problemas.[135] Conforme as normas de boas práticas, é aconselhável que a manutenção dos ambientes de desenvolvimento, teste e produção sejam mantidos apartados dos demais, a fim de minorar os riscos de acessos ou alterações não autorizadas; bem como que os eventos sejam registrados (*logs*).[136]

Nessa linha relativa à proteção contra invasões — acessos ou modificações sem autorização —, sobreleva-se o "controle contra *malware*". Consoante o relatório "2022 SonicWall Cyber Threat Report", somente no terceiro trimestre daquele ano, o volume global de ameaças de ataques de *malware* ultrapassou a marca de 4 bilhões de tentativas.[137] Por *malware*, expressão genérica, entende-se qualquer aplicação maliciosa (fusão das palavras *malicious* + *software*) realizada com a intenção de gerar prejuízos — como interceptação e/ou sequestro de dados, danificação de sistemas e outros — atingindo computadores, aparelhos *mobile* e, eventualmente, redes inteiras (para taxonomia de ameaças, ataques e vulnerabilidades cibernéticas, cf Belli *et al.*, 2023).

Face à pluralidade e aos elevados reportes de ocorrência, recomenda-se que controles de detecção, prevenção e recuperação sejam implementados para assegurar a organização. A fim de atingir um nível mínimo e adequado de segurança, destacam-se as medidas desejáveis em diferentes contextos, como *i)* a implementação de um programa de conscientização coeso (acompanhado pelos treinamentos e práticas educativas); *ii)* que se

133 ISO/IEC 27.001:2013, item 6.9, e ISO/IEC 27.002:2013, item 12.

134 ISO/IEC 27.002:2013, item 12.1.2, p. 49.

135 ISO/IEC 27.002:2013, item 12.1.3, p. 49-50.

136 ISO/IEC 27.002:2013, itens 12.1.4 e 12.4, p. 50-51 e 54-56.

137 Disponível em: https://is.gd/Qkh4Pa.

proíba o uso de *softwares* não autorizados, com a utilização, por exemplo, de uma lista de sistemas e aplicações permitidos (*whitelisting*); *iii*) implementar controles de prevenção de acesso aos sites maliciosos, suspeitos ou conhecidos*; iv)* instalar e atualizar os *softwares* de proteção e detecção de incidentes regularmente; *v)* elaborar e circular boletins informativos fomentando processo de conscientização de agentes públicos envolvidos na abertura de dados; *vi)* isolar ambientes danificados; e outros.[138]

Haja vista a complexidade e os riscos referentes aos *softwares* nos sistemas operacionais, alerta-se para a elaboração e a implementação de procedimento para o controle da sua instalação (com restrições), sob responsabilidade de corpo técnico autorizado, garantindo-se a manutenção das versões anteriores como medida de contingência e de registros de auditoria.[139] É necessária a elaboração e a implementação de políticas e diretrizes correlatas "à aquisição, ao desenvolvimento e à manutenção de sistemas" de forma que atendam aos requisitos de segurança da informação estabelecidos pela organização[140] ("Figura 9"). É de igual importância alocar a equipe interna para realização de testes de segurança em sistemas legados e sistemas novos, envolvidos na abertura de dados (como testes de penetração), e para sanitização de bases de dados operacionais (limpeza de dados que não são necessários), acompanhada da remoção ou modificação daqueles dados que sejam pessoais ou pessoais sensíveis.[141]

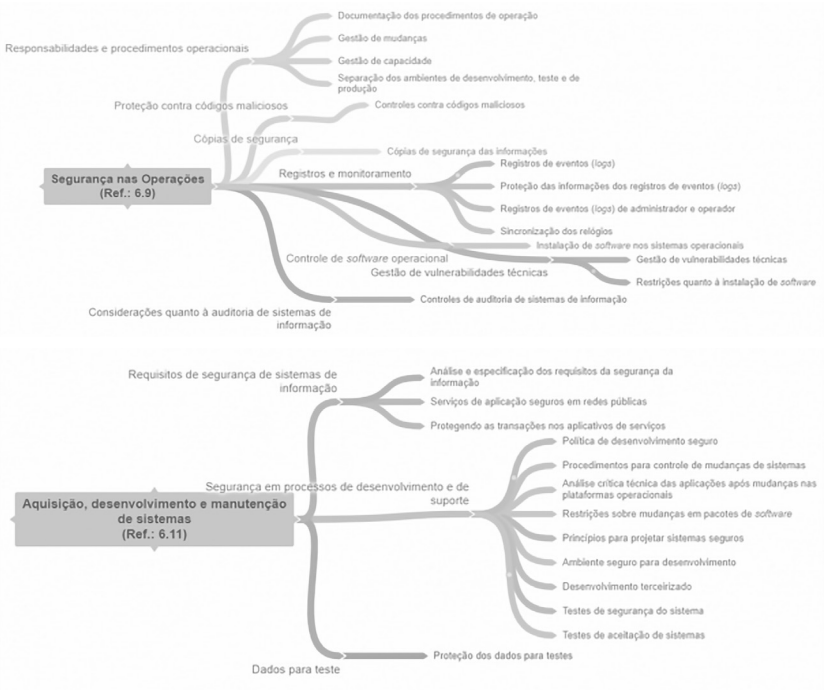
138 ISO/IEC 27.002:2013, item 12.2, p. 51-53.

139 ISO/IEC 27.002:2013, itens 12.5, 12.6 e 12.7, p. 57-60.

140 ISO/IEC 27.001:2013, item 6.11, e ISO/IEC 27.002:2013, item 14.

141 Para recomendações nesse âmbito, convém acessar a ISO/IEC 29.101, *Information technology - Security techniques - Privacy architecture framework* (ISO/IEC 27.002:2013, item 14.3, p. 76-77.).

Figura 9: Representação gráfica de categorias e subcategorias da ISO/IEC 27.001:2013, itens 6.9 e 6.11.



Dentre as orientações elencadas na ISO/IEC 27.002/2013,[142] destacamos a segregação de rede ("Figura 10"), ou seja, sua divisão em diferentes domínios, por exemplo, com base no nível de confiança (como de acesso público e de trabalho), em todas as áreas do órgão ou ente público envolvido na abertura de dados, com a utilização de diferentes redes físicas ou lógicas — e dedicar especial atenção às redes *wireless*.

Figura 10: Representação gráfica de categorias e subcategorias da ISO/IEC 27.001:2013, item 6.10.

142 ISO/IEC 27.002:2013, item 13.1.3, p. 62-63.

Cientes da impossibilidade de ecossistemas de "risco zero", apesar da implementação de programas coesos e eficientes de segurança da informação, é necessário gerenciar de modo consistente os incidentes correlatos, de forma que se incluam diretrizes associadas às responsabilidades e papéis — assegurando-se que todos entendam as prioridades —, aos registros e às notificações de eventos e fragilidades, garantindo-se que os respectivos objetivos sejam acordados com a direção[143] ("Figura 11"). Na comunicação de incidentes, elencam-se denominação de eventos considerados como:

a) controle de segurança ineficaz;

b) violação da disponibilidade, confidencialidade e integridade da informação;

c) erros humanos;

d) não conformidade com políticas ou diretrizes;

e) violações de procedimentos de segurança física;

f) mudanças descontroladas de sistemas;

g) mau funcionamento de *softwares* ou *hardware*;

h) violação de acesso.[144]

Os relatórios de incidentes de segurança devem seguir um procedimento formal (documentado). Recomenda-se que essa trilha contempla *i)* a identificação do ponto de contato; *ii)* a coleta tempestiva (logo após o infortúnio) de evidências; *iii)* a realização de análise forense de segurança da informação; *iv)* o registro de todas as ações realizadas — inclusive escalação; *v)* a comunicação interna e externa; *vi)* o tratamento das vulnerabilidades identificadas; *vii)* o roteiro de encerramento após o tratamento "bem-sucedido" do incidente; e *viii)* a garantia de que sejam efetuadas análises posteriores.[145] Adicionalmente, as autoras sugerem que sejam acompanhados de um documento dotado de linguagem mais simples e didática (poupando termos excessivamente técnicos) no intuito de promover uma

143 ISO/IEC 27.001:2013, item 6.13, e ISO/IEC 27.002:2013, item 16.

144 ISO/IEC 27.002:2013, item 16.1.2, p. 85.

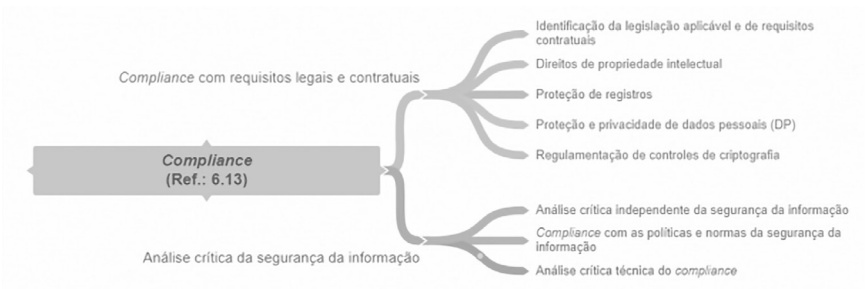
145 ISO/IEC 27.002:2013, itens 16.1.5 e 16.1.6, p. 86-87.

comunicação de amplo alcance sobre o evento adverso — garantindo que sua compreensão seja acessível por todos e todas.

Figura 11: Representação gráfica de categorias e subcategorias da ISO/IEC 27.001:2013, item 6.13.

Por fim, a organização deve garantir a "conformidade" ("Figura 12") com os requisitos legais, estatutários, regulamentares — internos e externos — e contratuais naquilo que é relativo à segurança da informação. Destarte, os respectivos elementos devem ser identificados, documentados e analisados criticamente, assegurando-se a manutenção dos registros atualizados.[146]

Figura 12: Representação gráfica de categorias e subcategorias da ISO/IEC 27.001:2013, item 6.15.



A seguir, apresentamos uma tabela que lista 23 categorias relevantes para arranjo de segurança cibernética (além de outras 108 subcategorias, não transcritas), conforme funções previstas no NIST CSF e na ISO, com indicação dos controles, para que possam ser consultados na íntegra de acordo com a necessidade. Vejam-se a seguir:

146 ISO/IEC 27.001:2013, item 6.15, e ISO/IEC 27.002:2013, item 18.

Tabela II comparativa: ISO/IEC 27001:2013 e NIST SP 800-53 Rev. 4[147]		
Função	**Categoria**	**Referência**
IDENTIFICAR (ID)	**Gerenciamento de Ativos (ID.AM)**	· **ISO/IEC 27001:2013** A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6, A.12.5.1, A.13.2.1, A.13.2.2
		· **NIST SP 800-53 Rev. 4** AC-4, AC-20, CA-3, CA-9, CM-8, CP-2, PL-8, PM-5, PM-11, PS-7, RA-2, SA-9, SA-14, SC-6
	Ambiente Organizacional (ID.BE)	· **ISO/IEC 27001:2013** Clause 4.1, A.11.1.4, A.11.2.2, A.11.2.3, A.12.1.3, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.17.1.1, A.17.1.2, A.17.2.1
		· **NIST SP 800-53 Rev. 4** CP-2, CP-8, CP-11, PE-9, PE-11, PM-8, PM-11, SA-12, SA-13, SA-14
	Governança (ID.GV)	· **ISO/IEC 27001:2013** Clause 6, A.5.1.1, A.6.1.1, A.7.2.1, A.15.1.1, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5
		· **NIST SP 800-53 Rev. 4** -1 controls from all security control families, PS-7, PM-1, PM-2, PM-3, PM-7, PM-9, PM-10, PM-11, SA-2
	Avaliação de Risco (ID.RA)	· **ISO/IEC 27001:2013** Clause 6.1.2 e 6.1.3, A.6.1.4, A.12.6.1, A.16.1.6, A.18.2.3
		· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, PM-4, PM-9, PM-11, PM-12, PM-15, PM-16, RA-2, RA-3, RA-5, SA-5, SA-11, SA-14, SI-2, SI-4, SI-5
	Estratégia de Gestão de Risco (ID.RM)	· **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3
		· **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	Gestão de Riscos da Cadeia de Suprimentos (ID.SC)	· **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.17.1.3
		· **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9, RA-2, RA-3, SA-9, SA- 11, SA-12, SA-14, SA-15, PM-9, PS-7

147 Tabela adaptada. Tradução livre (National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. April 16, 2018, p. 24 - 44. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf).

PROTEGER (PR)	**Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC)**	· **ISO/IEC 27001:2013** A.6.1.2, A.6.2.1, A.6.2.2, A7.1.1, A9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A9.4.1, A.9.4.2, A.9.4.3, A9.4.4, A9.4.5, A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3, A.18.1.4
		· **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9, AC-10, AC-11, AC-12, AC-14, AC-16, AC-17, AC-19, AC-20, AC-24, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, SC-7, SC-15
	Conscientização e Treinamentos (PR.AT)	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2, A.12.2.1
		· **NIST SP 800-53 Rev. 4** AT-2, AT-3, IR-2, PM-13, PS-7, SA-9, SA-16
	Segurança de Dados (PR.DS)	· **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.11.2.4, A.11.2.5, A.11.2.7, A.12.1.3, A.12.1.4, A.12.2.1, A.12.5.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3, A.14.2.4, A.17.2.1
		NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, AU-4, CM-2, CM-8, CP-2, MP-6, MP-8, PE-16, PE-19, PS-3, PS-6, SA-10, SC-5, SC-7, SC-8, SC-11, SC-12, SC-13, SC-16, SC-28, SC-31, SI-4, SI-7
	Processos e Procedimentos de Proteção da Informação (PR.IP)	· **ISO/IEC 27001:2013** Clause 9, Clause 10, A.6.1.5, A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 , A.8.2.3, A.8.3.1, A.8.3.2, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.7, A.12.1.2, A.12.3.1, A.12.5.1, A.12.6.1, A.12.6.2, A.14.1.1, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.5, A.16.1.1, A.16.1.3, A.16.1.6, A.17.1.1, A.17.1.2, A.17.1.3, A.18.1.3, A.18.2.2, A.18.2.3
		· **NIST SP 800-53 Rev. 4** AC-21, CA-2, CA-7, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, CP-2, CP-4, CP-6, CP-7, CP-9, CP-12, CP-13, IR-3, IR-7, IR-8, IR-9, MP-6, RA-3, PE-10, PE-12, PE-13, PE-14, PE-15, PE-17, PE-18, PL-2, PL-8, PM-6, PM-14, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, RA-5, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SA-21, SI-2, SI-4, SI-12, SI-13, SI-14, SI-16, SI-17
	Manutenção (PR.MA)	· **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6, A.15.1.1, A.15.2.1
		· **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-4, MA-5, MA-6
	Tecnologia de Proteção (PR.PT)	· **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.1.2, A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.9, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.15.1.1, A.15.2.1, A.13.1.1, A.13.2.1, A.14.1.3, A.17.1.2, A.17.2.1
		· **NIST SP 800-53 Rev. 4** AU Family, AC-3, AC-4, AC-17, AC-18, CM-7, CP-7, CP-8, CP-11, CP-13, MA-2, MA-3, MA-4, MA-5, MA-6, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, PL-8, SA-14, SC-6, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43

DETECTAR (DE)	**Anomalias e Eventos (DE.AE)**	· **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.12.4.1, A.13.1.1, A.13.1.2, A.16.1.1, A.16.1.4, A.16.1.7
		· **NIST SP 800-53 Rev. 4** AC-4, AU-6, CA-3, CA-7, CM-2, CP-2, IR-4, IR-5, IR-8, RA-3, SI-4
	Monitoramento Contínuo de Segurança (DE.CM)	· **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.12.2.1, A.12.4.1, A.12.4.3, A.12.5.1, A.12.6.1, A.12.6.2, A.14.2.7, A.15.2.1
		· **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM10, CM-11, PE-3, PE-6, PE-20, PS-7, SA-4, SA-9, SC-5, SC-7, SC-18, SC-44, SI-3, SI-4, SI-8, RA-5
	Processo de Detecção (DE.DP)	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.14.2.8, A.16.1.2, A.16.1.3, A.16.1.6, A.18.1.4, A.18.2.2, A.18.2.3
		· **NIST SP 800-53 Rev. 4** AC-25, AU-6, CA-2, CA-7, PE-3, PL-2, PM-14, RA-5, SA-18, SI-3, SI-4, PM-14
RESPONDER (RS)	**Plano de Resposta (RS.RP)**	· **ISO/IEC 27001:2013** A.16.1.5
		· **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Comunicações (RS.CO)	· **ISO/IEC 27001:2013** Clause 7.4, Clause 16.1.2, A.6.1.1, A.6.1.3, A.6.1.4, A.7.2.2, A.16.1.1, A.16.1.2, A.16.1.5
		· **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, CP-2, CP-10, IR-4, IR-6, IR-8, PE-6, RA-5, SI-4, SI-5, PM-15
	Análises (RS.AN)	· **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
		· **NIST SP 800-53 Rev. 4** AU-6, AU-7, CA-7, CP-2, IR-4, IR-5, IR-8, PE-6, SI-4, SI-5, PM-15
	Mitigação (RS.MI)	· **ISO/IEC 27001:2013** A.12.2.1, A.12.6.1, A.16.1.5
		· **NIST SP 800-53 Rev. 4** CA-7, IR-4, RA-3, RA-5
	Melhorias (RS.IM)	· **ISO/IEC 27001:2013** A.16.1.6, Clause 10
		· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECUPERAR (RC)	**Plano de Recuperação (RC.RP)**	· **ISO/IEC 27001:2013** A.16.1.5
		· **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Melhorias (RC.IM)	· **ISO/IEC 27001:2013** A.16.1.6, Clause 10
		· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Comunicações (RC.CO)	· **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		· **NIST SP 800-53 Rev. 4** CP-2, IR-4

Embora se tenha traçado um "modelo ideal" a ser implementado nas organizações, sinaliza-se que nem todos esses controles serão, de fato, necessários. A abrangência poderá variar devido: "1) ao tamanho da organização, e seu tipo de atividades, processos, produtos e serviços; 2) à complexidade dos processos e suas interações; e 3) à competência das pessoas".[148-149]

Muito além disso, a realidade material do local, disponibilidade de dispositivos, sistemas e infraestrutura, bem como as prioridades de atuação do órgão ou ente impactarão diretamente na definição do arranjo de segurança cibernética. As práticas propostas pelas normas não são estruturadas contextualmente, no que diz respeito aos impactos e aos possíveis prejuízos às coletividades ou grupos de coletividades. Sendo assim, a consulta à tecnologistas, profissionais com *expertise* na área de segurança da informação, e da população local é indispensável para compreender as prioridades de segurança para abertura de dados.

148 ISO/IEC 27.001:2013, p. 7.

149 Como exemplo, cita-se a "Guia de Segurança da Informação para Agentes de Pequeno Porte", publicada em outubro de 2021, pela ANPD. Disponível em: https://is.gd/d0bPJk.

Parte IV
Proposições finais: recomendações, DatagovGPT e modelo de avaliação de impacto sobre abertura, proteção e segurança de dados[150]

Resumo em tópicos

Esta parte conclusiva oferece algumas recomendações para os tomadores de decisões e apresenta um modelo detalhado para administradores públicos, com intuito de especificar os elementos técnicos e normativos apresentados ao longo do estudo em sugestões operacionais que possam permitir uma melhor governança de dados no setor público. Os seguintes assuntos serão abordados:

- Visão geral do tratamento e caracterização dos dados tratados;
- Descrição e controle das operações de tratamento e dos instrumentos de suporte com enfoque especial nas operações de tratamento, abertura dos dados e garantia de direitos do titular de dados;
- Estudo dos riscos de segurança de dados, com enfoque nos controles implementados para tratar os riscos relacionados à segurança de dados, na descrição e avaliação dos controles gerais de segurança e dos controles organizacionais (governança);
- Avaliação de risco com particular enfoque nas possíveis violações da privacidade;

150 Baseado em Belli, L (2020). Como implementar a LGPD por meio da Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED). Em Mendes L. *et al*. Tratado de Proteção de Dados.

- Validação do modelo proposto, no que diz respeito às informações relativas ao compartilhamento de dados com terceiros, a avaliação de conformidade conforme princípios fundamentais, de cumprimento das boas práticas de segurança de dados, de proporcionalidade e necessidade do tratamento, e de controles para proteger os direitos dos titulares dos dados;
- Avaliação das ações de mitigação de riscos e elaboração de plano de ação;
- Documentação do modelo proposto com enfoque no resumo das respostas à tomada de subsídios, validação formal do encarregado pelo tratamento de dados pessoais e validação formal do controlador.

Introdução

Nas três primeiras partes deste relatório foram apresentadas as principais questões da governança e regulação de dados no setor público, estimulando uma visão sistêmica capaz de conectar as exigências da abertura de dados, da proteção de dados pessoais e da segurança da informação. Assim, o objetivo geral deste trabalho é interconectar estas dimensões fundamentais da governança de dados, destacando a necessidade de tal interconexão para uma transformação digital sustentável. É importante reiterar que este trabalho tem três objetivos específicos complementares que esperamos que possam se fortalecer reciprocamente.

Primeiramente, traçar um diagnóstico detalhado do arcabouço regulatório em vigor no Brasil, em segundo lugar, identificar as boas práticas que deveriam ser adotadas por administradores públicos a fim de favorecer uma transformação digital sustentável, e por fim, consolidar o arcabouço normativo e as boas práticas, em uma série de recomendações para tomadores de decisões e um Modelo de avaliação de impacto sobre abertura, proteção e segurança de dados.

Cabe frisar que, além das recomendações e do modelo que detalharemos nesta parte conclusiva, os elementos das recomendações e do Modelo serão embutidos numa ferramenta interativa disponibilizada em acesso livre para suportar administradores públicos em suas atividades de abertura, proteção e segurança de dados.

As recomendações e o modelo são baseados no diagnóstico técnico e regulatório traçado ao longo deste relatório, e nas melhores práticas internacionais. O modelo é direcionado aos administradores e inclui instruções sobre como implementar os dispostos normativos em vigor e as melhores práticas de governança de dados.

As recomendações são direcionadas aos tomadores de decisões e, junto com os elementos normativos e boas práticas destacados acima, incluem algumas sugestões operacionais que, a nosso ver, seriam particularmente úteis não somente para suportar uma correta implementação do arcabouço normativo brasileiro, mas, também, para facilitar uma governança suave e promover a experimentação baseada em dados num ambiente controlado.

Neste sentido, duas propostas nos parecem particularmente valiosas. Primeiramente, o estabelecimento de um Escritório de Governança de

Dados em cada administração pública, para combinar as competências e facilitar a constante interação dos profissionais responsáveis pela abertura, proteção e segurança de dados. Como destacamos, a criação de um (escritório) responsável pela abertura de dados já é boa prática na administração pública, a identificação de um encarregado ou DPO é uma obrigação definida ela LGPD, enquanto ainda não existe — por enquanto — uma obrigação de definir um chefe de segurança de informação ou CISO.

Nos parece que para favorecer uma transformação digital sustentável, não somente estas figuras são essenciais, mas é absolutamente fundamental que elas interajam e se coordenem da maneira mais eficiente, efetiva e suave possível. Assim, nos parece que a criação de um Escritório de Governança de Dados que possa reunir os profissionais com background técnico e jurídico seja uma opção altamente desejável. Para facilitar o trabalho de tais Escritórios ou das unidades atualmente responsáveis pela abertura, proteção e segurança de dados, esta última parte oferece um modelo de avaliação de impacto sobre abertura, proteção e segurança de dados.

Em segundo lugar, sugerimos que é altamente pertinente explorar o estabelecimento de Ambientes de Pesquisa Confiáveis ou *sandboxes* de pesquisa, baseados no modelo britânico dos *Trusted Research Environments* (TREs) (UK Health Data Research Alliance; NHSX, 2021). No Reino Unido, estes ambientes de pesquisa confiáveis são utilizados para operar o equilíbrio entre dois desenvolvimentos divergentes, mas interconectados: de um lado, um apetite crescente por tecnologias baseada em processamento maciço de dados abertos e/ou pessoais, apoiado por um setor de pesquisa, um ecossistema tecnológico e políticas públicas orientadas à promoção da inovação. De outro lado, o entendimento dos enormes riscos que o processamento de dados em escala pode trazer e, portanto, o aumento da conscientização sobre a importância das salvaguardas legais e éticas para orientar essas inovações, garantindo o pleno respeito de direitos e obrigações legais, no âmbito de uma colaboração contínua entre setor público, setor acadêmico e setor privado (Kerasidou *et al*. 2023).

Os Ambientes de Pesquisa Confiáveis, também conhecidos como "enclaves de dados" ou "portos seguros de dados", são ambientes analíticos físicos ou virtuais que podem conter vários conjuntos de dados (censo e dados demográficos, dados de saúde etc.). Sujeito a monitoramento e controles de acesso, o usuário dos Ambientes de Pesquisa Confiável pode ter

permissão para trabalhar com esses dados, mas é impedido de liberar suas análises sem permissão.

O objetivo é, portanto, atuar como uma *sandbox* voltada à pesquisa com dados, fornecendo um espaço seguro para os pesquisadores analisarem dados, especialmente dados pessoais, permitindo uma pesquisa colaborativa e transparente, protegendo a confidencialidade e privacidade dos dados, e estimulando a inovação. Embora os TREs tenham recebido relativamente pouca atenção na literatura acadêmica, eles estão em operação no Reino Unido há quase 20 anos e, recentemente, se destacaram como um serviço essencial para os dados do Serviço Nacional de Saúde britânico, pois podem gerar confiança pública ao facilitar a intensificação da demanda por dados confidenciais para fins de pesquisa, garantindo privacidade, confidencialidade e acesso seguro.

Em uma *sandbox* de pesquisa, os dados não são liberados externamente aos usuários de dados para análise em seus próprios computadores, mas colocados em um servidor dentro de um ambiente informático restrito, onde o usuário aprovado recebe acesso seguro para realizar sua análise de projeto. Nenhum dado em nível de linha sai dos Ambientes de Pesquisa Confiáveis. Tradicionalmente, apenas resultados de nível agregado (por exemplo, tabelas de resumo, gráficos, modelos estatísticos) são liberados no final do projeto baseado na *sandbox* de pesquisa, e somente após uma série de controles automáticos e manuais serem aplicados para garantir que todos os resultados correspondam aos mais altos padrões éticos e, particularmente, não divulguem nenhum dado pessoal.

Como destacam Kerasidou e colegas (2023), a maioria dos TREs são estruturados com base no modelo chamado dos "cinco cofres" baseado em cinco pilares fundamentais, que foi reconhecido internacionalmente e introduzido pelo Escritório Nacional de Estatísticas do Reino Unido em 2003. Tal estrutura é utilizada para enquadrar, em vez de prescrever, as discussões cruciais sobre governança e gerenciamento de dados confidenciais envolvendo provedores de dados, usuários e reguladores, compartimentando as decisões em torno do acesso e uso de dados em cinco dimensões relacionadas (Jefferson *et al*. 2021).

Nos parece que os cinco pilares definidos ao nível britânico deveriam ser considerados como boas práticas a ser reproduzida ao nível brasileiro. Tais pilares da estrutura são:

1) Pessoas seguras: a equipe administrativa do Ambiente de Pesquisa Confiável e os pesquisadores que acessam os dados por meio dele são treinados e autorizados a usar os dados com segurança, seguindo as diretrizes e relatando problemas de segurança de dados, se houver;

2) Projetos seguros: por meio de um processo inicial de aprovação ética e de governança de dados, os Ambientes de Pesquisa Confiáveis garantem que os projetos de pesquisa sejam aprovados pelos controladores de dados e que os dados sejam usados adequadamente e para benefício público;

3) Saídas seguras: as *Sandbox* de Pesquisa incluem a obrigação de analisar todos os resultados minuciosamente e aprovação da liberação somente depois de garantir que não há dados pessoais incluídos;

4) Dados seguros: os dados são anonimizados ou pseudoanonimizados antes que o acesso seja concedido aos pesquisadores. É garantido que os pesquisadores vejam apenas os dados de que precisam;

5) Configuração segura: as *Sandbox* de Pesquisa fornecem um ambiente seguro para acessar dados pessoais e impedir qualquer uso não autorizado.

1 Recomendações para tomadores de decisões

As seguintes recomendações são direcionadas aos tomadores de decisões e visam assistir o planejamento de políticas e mecanismos de governança de dados ao nível municipal. Neste sentido, as administrações locais deveriam:

1) Promover a cooperação e participação multissetorial;

2) Garantir a transparência significativa da governança de dados;

3) Estabelecer um Escritório de Governança de Dados que inclua responsáveis de abertura de dados, encarregados de proteção de dados e chefes de segurança de informação;

4) Criar uma estrutura de governança de dados composta por conselho ou comitê capaz de envolver e representar os interesses relativos à governança de dados sustentável, incluindo servidores, e partes interessadas e especialistas;

5) Estabelecer "Ambientes de Pesquisa Confiáveis" ou "Sandboxes de Pesquisa" para permitir a pesquisa e desenvolvimento baseada em processamento de dados abertos e/ou pessoais no pleno respeito de direitos e obrigações legais;

6) Estabelecer um processo de consulta pública multissetorial para viabilizar a participação social, e receber comentários sobre as iniciativas propostas em termos de governança de dados;

7) Adotar uma política abrangente de abertura de dados que incentive diferentes esferas do governo a abrir os dados;

8) Adotar normas que forneçam orientações claras sobre a coleta, armazenamento, compartilhamento e anonimização, garantindo que dados pessoais sejam protegidos e seguros;

9) Estabelecer um processo de governança de dados, incluindo requisitos de qualidade de dados enquanto insumo para as tecnologias emergentes e modelos de tomada de decisão;

10) Estabelecer padrões técnicos para metadados, consumo de dados, licenciamento de dados e anonimização, nos casos de abertura de dados que envolvem de dados pessoais e eventos relativos à cibersegurança;

11) Estabelecer padrões de revisão e transparência para os casos de abertura de dados a partir de dados pessoais, e em casos de incidentes e ameaças cibernéticas;

12) Determinar a realização de estudo de avaliação de impacto e medidas de intervenção relativas aos riscos de abertura de dados;

13) Realizar auditorias sobre os dados que estão sendo abertos, criados, mantidos e gerenciados em ambiente controlado;

14) Promover treinamentos e educação para servidores públicos sobre como implementar as melhores práticas de proteção de dados e cibersegurança;

15) Realizar campanhas de conscientização pública sobre governança de dados nas suas diferentes dimensões (abertura, proteção e segurança);

16) Estabelecer parcerias a fim de compartilhar práticas e experiências para governança de dados;

17) Incentivar o uso de sandbox de pesquisa para elaboração de tecnologia de gestão de dados;

18) Promover avaliação de impacto de processamento de dados, com enfoque especial nos controles implementados para mitigar os riscos relacionados à segurança de dados, à privacidade e proteção de dados pessoais, e à discriminação;

19) Promover a avaliação das ações de mitigação de riscos;

20) Promover a documentação detalhada dos processos de governança de dados.

2 DatagovGPT

Como parte do nosso projeto, criamos uma ferramenta chamada DatagovGPT. A ferramenta tem o objetivo de facilitar a obtenção de sugestões na implementação de esquemas de governança de dados sustentável no nível local, a partir dos requisitos impostos pela legislação aplicável, recomendações e modelos elaborados neste estudo.

Para isso, oferecemos uma ferramenta de chatbot desenvolvida sobre a interface do ChatGPT, como um modelo de técnicas de processamento de linguagem natural e algoritmos de aprendizado de máquina baseado no ChatBase suportado pela empresa OpenAI. O ChatGPT pode oferecer respostas rápidas e explicações detalhadas de conceitos complexos, assim, criar um artefato nesta pesquisa é mais um instrumento desta pesquisa para facilitar a adoção da governança de dados no nível local.

O *chatbot* foi construído através da metodologia de Design Science Research, cujo foco é o desenvolvimento e projeção de soluções através de sistemas para resolver problemas e criar soluções, através do conhecimento científico aplicado (Hevner, 2009). Portanto, é um conjunto científico de métodos orientados à prática cotidiana. O processo de criação do artefato foi operacionalizado em três ciclos. No ciclo de relevância, avaliamos outras ferramentas e chatbots disponíveis, determinando quais seriam os requisitos principais do artefato. No ciclo do design, a equipe de pesquisadores apresentou um protótipo da ferramenta, e foram utilizados algumas regulamentações e casos para testar as funcionalidades. No ciclo de rigor, garantimos que a ferramenta estivesse sendo construída com base em abordagens teóricas e éticas, dado seu propósito de facilitar a adequação de casos ao framework de proteção de dados pessoais.

O artefato é alimentado com este estudo e as regulamentações relacionadas. Mas também é possível acessar as instruções e material utilizado através de cyberbrics.info/DataGov/. Dessa forma, além de testar a ferramenta, tornamos possível sua cópia e adaptação por qualquer interessado.

Destacamos que a ferramenta não tem como objetivo prestar consultoria jurídica concreta, mas fornecer instrumentos para reflexão sobre potenciais desafios que possam ser relevantes no processo de governança de dados públicos. Além disso, informações de caráter sigiloso ou protegido não devem ser adicionadas nesta ferramenta, uma vez que a empresa que

utilizamos para prover o modelo contém sua própria política de processamento e armazenamento de dados adicionados na interface.

Considerando a dificuldade de se analisar cada etapa do processo, a ferramenta pode permitir aos interessados em realizar a abertura avançar com procedimentos e já levar uma proposta de estrutura de governança mais elaborada, que atenda a normas e boas práticas do processo.

Na interação com o DatagovGPT é possível formular perguntas sobre o conteúdo que foi apresentado aqui, assim como sobre as normas estabelecidas em lei. Além disso, com a descrição de um caso formulado, ele poderá oferecer sugestões contextualizadas para o problema apresentado a partir da tecnologia de geração de textos fornecidos pelos modelos de linguagem.


DatagovGPT
Quais as legislações existentes no Brasil sobre proteção de dados?
No Brasil, a principal legislação sobre proteção de dados é a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em setembro de 2020. A LGPD estabelece diretrizes e regras para o tratamento de dados pessoais por parte de empresas e organizações, visando proteger a privacidade e os direitos dos cidadãos.
Além da LGPD, existem outras leis e regulamentos relacionados à proteção de dados no país, como:
1. Marco Civil da Internet (Lei nº 12.965/2014): Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, incluindo disposições sobre privacidade e proteção de dados.
2. Lei de Acesso à Informação (Lei nº 12.527/2011): Regula o acesso a informações públicas e estabelece diretrizes para a divulgação de dados governamentais.
3. Lei do Cadastro Positivo (Lei nº 12.414/2011): Regulamenta a criação e gestão de bases de dados contendo informações sobre o histórico de pagamentos e registro de transações de pessoas físicas e jurídicas, para a construção de score de crédito.
É importante ressaltar que a LGPD é a legislação mais abrangente e específica sobre proteção de dados no Brasil, estabelecendo diretrizes e sanções para o tratamento inadequado de dados pessoais.
DatagovGPT
Que tipos de dados são considerados sensíveis?
Dados sensíveis são informações que, quando associadas a uma pessoa, podem gerar riscos significativos à sua privacidade e segurança. Esses dados são considerados especialmente protegidos de acordo com a Lei Geral de Proteção de Dados (LGPD) no Brasil. Alguns exemplos de dados sensíveis incluem:
1. Dados de saúde: Informações relacionadas à condição física ou mental de uma pessoa, histórico médico, tratamentos, exames, entre outros.
2. Dados biométricos: Características físicas ou comportamentais únicas de uma pessoa, como impressões digitais, reconhecimento facial, voz, entre outros.
3. Dados genéticos: Informações sobre o DNA de uma pessoa, incluindo sequências genéticas, predisposições a doenças, ancestralidade, entre outros.
4. Dados de orientação sexual: Informações sobre a orientação sexual de uma pessoa, como heterossexualidade, homossexualidade, bissexualidade, entre outros.
5. Dados étnicos ou raciais: Informações sobre a origem étnica ou racial de uma pessoa, como raça, cor da pele, ascendência, entre outros.
Esses são apenas alguns exemplos de dados sensíveis, e é importante ressaltar que a definição exata pode variar de acordo com a legislação e regulamentação específicas de cada país. A proteção adequada desses dados é fundamental para garantir a privacidade e a segurança dos indivíduos.
Powered By Chatbase.co

3 Modelo de avaliação de impacto sobre abertura, proteção e segurança de dados

1) Visão geral do tratamento

Breve descrição do tratamento (natureza, escopo, contexto etc.)	
Finalidade do tratamento	Nome, endereço e endereço eletrônico do(s) operador(es) — se houver
Nome, endereço e endereço eletrônico do controlador	Nome, endereço e endereço eletrônico do Encarregado do operador
Nome, endereço e endereço eletrônico do Encarregado do controlador	Normas setoriais aplicáveis

2) Caracterização dos dados

1) Tipo de dados (natureza)
2) Tipos de titulares de dados
3) Destinatários / beneficiários
4) Tempo de retenção
   a) Duração do armazenamento
      i) Justificativa da duração
   b) Mecanismo de apagamento no final da duração do armazenamento

3) Descrição e controle das operações de tratamento e dos instrumentos de suporte

a) Operações de tratamento em geral

1) Operação de tratamento
   a) Descrição detalhada da operação
   b) Base legal
      i) SE consentimento:
         (1) Forma de coleta — controles[151]:
            (a) Consentimento expresso durante o registro
            (b) Consentimento segmentado por categoria de dados ou tipo de processamento
            (c) Consentimento expresso antes de compartilhar dados com outros usuários
            (d) Consentimento apresentado de forma inteligível e facilmente acessível, usando linguagem simples e clara, adaptada ao usuário-alvo (principalmente para crianças)
            (e) Obtenção do consentimento dos pais ou outro responsável legal para menores de 12 anos
            (f) Para um novo tratamento, é necessário obter novamente o consentimento

151 Em "Controles", sempre avaliar entre "Aceitável" ou "Pode ser melhorado" e justificar o atual estado de implementação.

(g) Após um longo período sem uso, o usuário deve ser solicitado a confirmar seu consentimento
(h) Nos casos em que o usuário consentiu o tratamento processamento de dados especiais (por exemplo, sua localização), a interface indica claramente que o processamento ocorre (ícone, luz)
(i) Quando o usuário altera o dispositivo, smartphone ou computador, reinstalar o aplicativo móvel ou excluir seus cookies, as configurações associadas ao seu consentimento são mantidas

ii) SE obrigação legal ou regulatória:
(1) Fonte de obrigação
iii) SE legítimo interesse:
(1) Avaliação de legítimo interesse aprovada pelo Encarregado (anexar)

c) Instrumentos de suporte utilizados (aplicativos de nuvem, e-mail, serviços de e-mail marketing etc.)
d) Informações sobre compartilhamento dos dados
i) SE destinatário interno
(1) Finalidade
(2) Meio / ferramenta
(3) Nacional / Internacional
ii) SE destinatário externo
(1) Finalidade
(2) Meio / ferramenta
(3) Nacional / Internacional
(4) Contrato / *due diligence* aprovado (anexar)
e) Justificativa da necessidade e relevância dos dados
i) Controles de minimização de dados
f) Controles de qualidade dos dados

b) Operações de tratamento: abertura dos dados

1) Exposição de propósitos da abertura de dados
2) Justificativa legal da abertura
3) Consideração das expectativas dos titulares de dados
a) Direitos relativos à proteção de dados e liberdades individuais

b) Contexto / razoabilidade / legítimas expectativas
4) Explicação e justificativa da anonimização dos dados
a) Detalhes sobre a técnica de anonimização dos dados
b) Categorias de dados anonimizados
c) Justificativa da necessidade e relevância da anonimização
d) Controles de anonimização
5) Explicação e justificativa da pseudoanonimização dos dados
a) Detalhes sobre a técnica de pseudoanonimização
b) Pseudoidentificadores[152] utilizados
c) Categorias de dados pseudoanonimizados
d) Dados inferidos por vinculação nos registros dos bancos de dados
e) Impacto sobre titulares de dados
6) Possibilidades de dados por inferências
a) Avaliação de risco de cruzamento de dados
i) Dados cruzados
ii) Dados inferidos
iii) Impacto sobre titulares de dados
7) Decisão sobre abertura — considerar pontos 1-6 anteriores.[153]
a) Abrir;
b) Abrir parcialmente;
c) Não abrir;
d) Suspender para revisão.

c) Garantia de direitos do titular de dados

1) Controles para o direito à informação:
a) Apresentação dos termos e condições de uso/confidencialidade
b) Possibilidade de acessar os termos e condições de uso/confidencialidade
c) Termos legíveis e fáceis de entender
d) Existência de cláusulas específicas para o dispositivo

152 São duplas no conjunto de dados, ou seja, é uma lista ou sequência de dados imutável que pode permitir a identificação de um sujeito no conjunto dos dados.

153 Ao final deste formulário, segue em anexo sugestão para avaliação quantitativa e qualitativa do risco, e para consequente impacto na decisão pela abertura ou não de dados.

e) Apresentação detalhada dos objetivos do tratamento de dados (objetivos especificados, correspondência de dados, quando aplicável etc.)
f) Apresentação da metodologia do processamento de dados pessoais (técnicas e procedimentos de anonimização)
g) Cronograma com a revisão da metodologia de processamento de dados pessoais
h) Apresentação detalhada dos dados pessoais coletados
i) Apresentação de qualquer acesso aos identificadores do dispositivo, smartphone/tablet ou computador, especificando se esses identificadores são comunicados a terceiros
j) Apresentação dos direitos do usuário (retirada de consentimento, apagamento de dados etc.)
k) Informações sobre o método seguro de armazenamento de dados, particularmente no caso de fornecimento
l) Arranjos para entrar em contato com a empresa (identidade e detalhes de contato) sobre questões de confidencialidade
m) Onde aplicável, informações para o usuário sobre qualquer alteração relativa aos dados coletados, os objetivos e as cláusulas de confidencialidade

2) Controles para o direito à informação em relação à transmissão de dados a terceiros
a) Apresentação detalhada dos objetivos da transmissão a terceiros
b) Apresentação detalhada dos dados pessoais transmitidos
c) Indicação da identidade de organismos terceiros e informações de contato

3) Controles para o direito de acesso a dados pessoais
a) Possibilidade de acessar todos os dados pessoais do usuário, através das interfaces comuns
b) Possibilidade de consultar com segurança os rastros de uso associados ao usuário
c) Possibilidade de baixar um arquivo com todos os dados pessoais associados ao usuário
d) Em caso de exceção ao direito de acesso:
i) Justificativa
ii) Planejamento de resposta ao titular

4) Controles para o direito de portabilidade de dados pessoais
   a) Possibilidade de recuperar dados pessoais fornecidos pelo usuário, para transferi-los para outro serviço
   b) Modo de portabilidade (API, arquivo interoperável etc.)
5) Controles para os direitos de correção e eliminação
   a) Possibilidade de corrigir dados pessoais
   b) Possibilidade de apagar dados pessoais
      i) Indicação dos dados pessoais que, mesmo assim, serão armazenados (requisitos técnicos, obrigações legais etc.)
   c) Indicações claras e etapas simples para apagar dados antes de eliminar o dispositivo
   d) Conselhos sobre como redefinir o dispositivo antes de vendê-lo
   e) Possibilidade de apagar remotamente os dados no caso de roubo ou perda do dispositivo
6) Em caso de exceção aos direitos de correção e eliminação:
   a) Justificativa
   b) Planejamento de resposta ao titular
7) Controles dos direitos à restrição e à objeção ao tratamento de dados
   a) Existência de configurações de "Privacidade"
   b) Convite para alterar as configurações padrão
   c) Configurações de "privacidade" acessíveis durante o registro
   d) Configurações de "privacidade" acessíveis após o registro
   e) Existência de um sistema de controle pelos responsáveis legais para crianças menores de 12 anos
   f) Conformidade em termos de rastreamento (cookies, publicidade etc.)
   g) Exclusão de crianças com menos de 12 anos de idade de perfilamento automatizado
   h) Exclusão efetiva do processamento dos dados do usuário no caso de o consentimento ser retirado
   i) Em caso de exceção aos direitos à restrição ao tratamento e à objeção
      i) Justificativa
      ii) Planejamento de resposta ao titular

4) Estudo dos riscos de segurança de dados

a) Controles implementados para tratar os riscos relacionados à segurança de dados

Controles relacionados especificamente aos dados que estão sendo processados	**Implementação ou justificativa de não implementação**
Criptografia	[Descreva aqui os meios implementados para garantir a confidencialidade dos dados armazenados (no banco de dados, em arquivos simples, backups etc.), bem como o procedimento para gerenciar chaves de criptografia (criação, armazenamento, alteração no caso de suspeita de casos de comprometimento de dados etc.). Descreva os meios de criptografia empregados para os fluxos de dados (VPN, TLS etc.) implementados no tratamento.
Anonimização ou pseudominimização	[Indique aqui se os mecanismos de anonimato são implementados, quais e com que finalidade.]
Isolamento de dados (em relação ao restante do sistema de informação)	[Indique aqui se o isolamento de tratamento é planejado e como isso é realizado.]
Controle de acesso lógico	[Indique aqui se os perfis dos usuários são definidos e atribuídos. Especifique os meios de autenticação implementados. Onde aplicável, especifique as regras aplicáveis às senhas (comprimento mínimo, caracteres necessários, duração da validade, número de tentativas com falha antes do bloqueio do acesso à conta etc.).]

Rastreabilidade (registro)	[Indique aqui se os eventos são registrados e por quanto tempo esses rastreamentos são armazenados.]
Monitoramento de integridade	[Indique aqui se os mecanismos são implementados para monitorar a integridade dos dados armazenados, quais e com qual finalidade. Especifique quais mecanismos de controle de integridade são implementados nos fluxos de dados.]
Arquivamento	[Descreva aqui os processos de gerenciamento de arquivos (entrega, armazenamento, consulta etc.) sob sua responsabilidade. Especifique as funções de arquivamento (escritórios de origem, agências de transferência etc.) e a política de arquivamento. Declare se os dados podem estar no escopo de arquivos públicos.]
Gestão de incidente de segurança	[Descreva as indicações de papéis, responsabilidades e procedimentos; forma e fluxo de notificação de eventos e fragilidades/vulnerabilidades; resposta aos incidentes de segurança; lições aprendidas e coleta de evidências.]
Segurança de documentos em papel	[Onde documentos em papel que contêm dados são usados durante o processamento, indique aqui como eles são impressos, armazenados, destruídos e trocados.]

b) Descrição e avaliação dos controles gerais de segurança

Controles gerais de segurança do sistema em que o tratamento é realizado	**Implementação ou justificativa de não implementação**
Gestão de ativos	[Descreva aqui as responsabilidades relativas ao inventário de ativos, sua propriedade e uso aceitável; classificação da informação e rotulagem; e tratamento de mídias (contemplando informações sobre gerenciamento, transferência e descarte).]

Segurança operacional	[Descreva aqui como as atualizações de software (sistemas operacionais, aplicativos etc.) e a aplicação dos controles corretivos de segurança são realizadas.]
Repressão de software malicioso	[Indique aqui se um software antivírus está instalado e atualizado em intervalos regulares nas estações de trabalho.]
Gerenciamento de estações de trabalho	[Descreva aqui os controles implementados nas estações de trabalho (bloqueio automático, firewall etc.).]
Segurança do site	[Indique aqui se as "recomendações para proteção de sites" da ANSSI foram implementadas.]
Backups	[Indique aqui como os backups são gerenciados. Esclareça se eles estão armazenados em um local seguro.]
Manutenção	[Descreva aqui como a manutenção física do hardware é gerenciada e indique se isso foi contratado. Indique se a manutenção remota de aplicativos está autorizada e de acordo com as disposições. Especifique se o equipamento defeituoso é gerenciado de uma maneira específica.]
Segurança de canais de computador (redes)	[Indique aqui o tipo de rede na qual o processamento é realizado (isolado, privado ou Internet). Especifique qual sistema de firewall, sistemas de detecção de intrusão ou outros dispositivos ativos ou passivos são responsáveis por garantir a segurança da rede.]
Monitoramento	[Indique aqui se o monitoramento em tempo real da rede local está implementado e com que meios. Indique se o monitoramento das configurações de hardware e software é realizado e por quais meios.]

Controle de acesso físico	[Indique aqui como é realizado o controle de acesso físico em relação às instalações que acomodam o processamento (zoneamento, escolta de visitantes, uso de passes, portas trancadas etc.). Indique se existem procedimentos de aviso em vigor no caso de uma invasão.]
Segurança de hardware	[Indique aqui os controles relacionados à segurança física dos servidores e estações de trabalho pertencentes aos clientes (armazenamento seguro, cabos de segurança, filtros de confidencialidade, apagamento seguro antes do scrapping etc.).]
Evitando fontes de risco	[Indique aqui se a área de implantação está sujeita a desastres ambientais (zona de inundação, proximidade de indústrias químicas, terremoto ou zona vulcânica, etc.). Especifique se produtos perigosos estão armazenados na mesma área.]
Proteção contra fontes não humanas de riscos	[Descreva aqui os meios de prevenção, detecção e combate a incêndios. Onde aplicável, indique os meios de prevenção de danos causados pela água. Especifique também os meios de monitoramento e alívio da fonte de alimentação.]

c) Descrição e avaliação dos controles organizacionais (governança)

Controles organizacionais (governança)	**Implementação ou justificativa de não implementação**
Organização	[Indique se as funções e responsabilidades da proteção de dados estão definidas. Especifique se uma pessoa é responsável pela aplicação das leis e regulamentos de privacidade. Especifique se existe um comitê de monitoramento (ou equivalente) responsável pela orientação e acompanhamento das ações relacionadas à proteção da privacidade.]

Política (gerenciamento de regras)	[Indique se existe uma carta de TI (ou equivalente) sobre proteção de dados e o uso correto dos recursos de TI.]
Gerenciamento de riscos	[Indique aqui se os riscos de privacidade apresentados por novos tratamentos sobre os titulares de dados são avaliados, se é sistemático ou não e, se aplicável, de acordo com qual método. Especifique se um mapeamento de riscos à privacidade no nível da organização é estabelecido.]
Gerenciamento de Projetos	[Indique aqui se os testes do dispositivo são executados em dados não reais/anônimos.]
Gerenciamento de incidentes e violações de dados	[Indique aqui se os incidentes de TI estão sujeitos a um procedimento de gerenciamento documentado — com resposta a incidentes — e testado.]
Auditoria de sistemas	[Descreva o programa de gestão e os controles de auditoria de sistemas e coleta de evidências]
Gestão de pessoal	[Indique aqui quais controles de conscientização são realizados em relação a um novo recruta. Indique quais controles são executados quando as pessoas que acessam dados deixam o emprego.]
Relações com terceiros	[Indique aqui, para processadores que exigem acesso a dados, os controles e disposições de segurança executados com relação a esse acesso.]
Supervisão	[Indique aqui se a eficácia e a adequação dos controles de privacidade são monitoradas.]

d) Avaliação de risco: possíveis violações da privacidade

Análise e avaliação de riscos

Risco	Fontes de risco	Ameaças	Impactos potenciais	Controles que reduzem gravidade e probabilidade	Gravidade	Probabilidade	Priorização (mapa de calor)
Acesso ilegítimo aos dados							
Alteração indesejada de dados							
Desaparecimento de dados							
Indisponibilidade de dados							
Outro (qual?)							

5) Validação do Modelo

a) Informações relativas a compartilhamento de dados com terceiros

Natureza e categoria do dado	Destinatário/beneficiário	Finalidade (justificativa)	Assinatura de termo compromisso e MTO (medidas técnicas e organizacionais) (anexar)

b) Avaliação de conformidade a princípios fundamentais

Controles selecionados para garantir a conformidade com os princípios fundamentais	**Avaliação**	**Controles corretivos**	**Responsável pela correção**	**Prazo para saneamento**	**Aprovação pelo Encarregado (data)**
Controles que garantem a proporcionalidade e a necessidade do tratamento					
Finalidade(s): específica, expressa e legítima	Choose an item.				☐ Data de aprovação.
Base: legalidade do processamento, proibição de uso indevido	Choose an item.				☐ Data de aprovação.
Necessidade de dados: adequada, relevante e limitada	Choose an item.				☐ Data de aprovação.
Qualidade dos dados: precisos e atualizados	Choose an item.				☐ Data de aprovação.
Durações de armazenamento: limitadas	Choose an item.				☐ Data de aprovação.
Controles para proteger os direitos pessoais dos titulares dos dados					
Informações para os titulares dos dados (tratamento justo e transparente)	Choose an item.				☐ Data de aprovação.
Obtenção de consentimento	Choose an item.				☐ Data de aprovação.

Exercício do direito de acesso e do direito à portabilidade de dados	Choose an item.				☐ Data de aprovação.
Exercício dos direitos de correção e eliminação	Choose an item.				☐ Data de aprovação.
Exercício dos direitos de restrição ao processamento e à objeção	Choose an item.				☐ Data de aprovação.
Processadores: identificados e regidos por um contrato	Choose an item.				☐ Data de aprovação.
Transferências: cumprimento das obrigações decorrentes da transferência de dados para fora do território brasileiro	Choose an item.				☐ Data de aprovação.

c)Avaliação de cumprimento das boas práticas de segurança de dados

Controles implementados para tratar os riscos relacionados à segurança de dados	**Avaliação**	**Controles corretivos**	**Responsável pela correção**	**Prazo para saneamento**	**Aprovação pelo Encarregado (data)**
Controles relacionados especificamente aos dados que estão sendo tratados					
Criptografia	Choose an item.				
Anonimização ou pseudo minimização	Choose an item.				

Isolamento de dados (em relação ao restante do sistema de informação)	Choose an item.				
Controle de acesso lógico	Choose an item.				
Rastreabilidade (registro)	Choose an item.				
Monitoramento de integridade	Choose an item.				
Arquivamento	Choose an item.				
Segurança de documentos em papel	Choose an item.				
Controles gerais de segurança do sistema em que o tratamento é realizado					
Gestão de ativos	Choose an item.				
Segurança operacional	Choose an item.				
Repressão de software malicioso	Choose an item.				
Gerenciando estações de trabalho	Choose an item.				
Segurança do site	Choose an item.				
Backups	Choose an item.				
Manutenção	Choose an item.				
Segurança de canais de computador (redes)	Choose an item.				
Monitoramento	Choose an item.				
Controle de acesso físico	Choose an item.				
Segurança de hardware	Choose an item.				

Evitando fontes de risco	Choose an item.				
Proteção contra fontes não humanas de riscos	Choose an item.				
Controles organizacionais (governança)					
Organização	Choose an item.				
Política (gerenciamento de regras)	Choose an item.				
Gerenciamento de riscos	Choose an item.				
Gerenciamento de Projetos	Choose an item.				
Gerenciamento de incidentes e violações de dados	Choose an item.				
Auditoria de sistemas	Choose an item.				
Gestão de pessoal	Choose an item.				
Relações com terceiros	Choose an item.				
Supervisão	Choose an item.				

d) Avaliação de proporcionalidade e necessidade do tratamento

Controles que garantem a proporcionalidade e a necessidade do tratamento	**Avaliação**	**Controles corretivos**	**Responsável pela correção**	**Prazo para saneamento**	**Aprovação pelo Encarregado (data)**
Objetivos: específicos, explícitos e legítimos	Choose an item.				

Base: legalidade do processamento, proibição de uso indevido	Choose an item.				
Minimização de dados: adequada, relevante e limitada	Choose an item.				
Qualidade dos dados: precisa e atualizada	Choose an item.				
Durações de armazenamento: limitadas	Choose an item.				

e) Avaliação de controles para proteger os direitos dos titulares dos dados

Controles para proteger os direitos dos titulares dos dados	**Avaliação**	**Controles corretivos**	**Responsável pela correção**	**Prazo para saneamento**	**Aprovação pelo Encarregado (data)**
Informações para os titulares dos dados (tratamento justo e transparente)	Choose an item.				
Obtenção de consentimento	Choose an item.				
Exercício dos direitos de acesso e portabilidade de dados	Choose an item.				

Exercício dos direitos de correção e eliminação	Choose an item.				
Exercício dos direitos de restrição ao processamento e à objeção	Choose an item.				
Processadores: identificados e regidos por um contrato	Choose an item.				
Transferências: cumprimento das obrigações decorrentes da transferência de dados para fora da União Europeia	Choose an item.				

f) Avaliação de ações de mitigação de riscos

Riscos	**Avaliação**	**Controles corretivos**
Acesso ilegítimo aos dados	[O avaliador deve determinar se os controles existentes ou planejados (já realizados) reduzem suficientemente esse risco para que seja considerado aceitável.]	[Onde aplicável, ele deve indicar aqui quaisquer controles adicionais que se mostrem necessários.]

Alteração indesejada de dados	[O avaliador deve determinar se os controles existentes ou planejados (já realizados) reduzem suficientemente esse risco para que seja considerado aceitável.]	[Onde aplicável, ele deve indicar aqui quaisquer controles adicionais que se mostrem necessários.]
Desaparecimento de dados	[O avaliador deve determinar se os controles existentes ou planejados (já realizados) reduzem suficientemente esse risco para que seja considerado aceitável.]	[Onde aplicável, ele deve indicar aqui quaisquer controles adicionais que se mostrem necessários.]
Indisponibilidade de dados	[O avaliador deve determinar se os controles existentes ou planejados (já realizados) reduzem suficientemente esse risco para que seja considerado aceitável.]	[Onde aplicável, ele deve indicar aqui quaisquer controles adicionais que se mostrem necessários.]
Outro (qual?)	[O avaliador deve determinar se os controles existentes ou planejados (já realizados) reduzem suficientemente esse risco para que seja considerado aceitável.]	[Onde aplicável, ele deve indicar aqui quaisquer controles adicionais que se mostrem necessários.]

g) Elaboração de plano de ação

Controles adicionais solicitados	**Responsável**	**Frequência**	**Dificuldade**	**Custo**	**Progresso**

6) Documentação do Modelo

a) Resumo das respostas à tomada de subsídios

Em Click or tap to enter a date. encerrou-se o prazo para tomada de subsídios (edital anexo). Sintetizam-se abaixo as contribuições sobre a conformidade do estudo de tratamento e relatório de impacto à proteção de dados pessoais realizado, já sujeitas a objeção pública dos participantes (30 dias):

Click or tap here to enter text.

X _____

Assinatura do responsável pelo texto aprovado

b) Validação formal do Encarregado pelo Tratamento de Dados Pessoais

Em Click or tap to enter a date., o Encarregado pelo Tratamento de Dados Pessoais de Click or tap here to enter text. emitiu o seguinte parecer sobre a conformidade do estudo de tratamento e relatório de impacto à proteção de dados pessoais realizado:

X _____

Encarregado pelo Tratamento de Dados Pessoais

c) Validação formal do Controlador

Em Click or tap to enter a date., o Controlador de Click or tap here to enter text. valida a AIPED para o processamento de dados nos termos descritos nesse formulário, em sua capacidade de controlador de dados.

X_____

Assinatura do representante do Controlador

Anexo
Análise quantitativa e qualitativa do risco

O estudo dos riscos e dos benefícios de eventual abertura de dados contempla possibilidades plurais de análise. Pelo presente ensaio, sugerem-se, ilustrativamente, algumas balizas qualitativas e quantitativas. Os respectivos valores serão dedicados à avaliação do risco à privacidade e à possibilidade de sua ocorrência. Por fim, propor-se-á um quadro conclusivo, ou seja, incentivando ou não a abertura de dados. Segue:

- Referência para avaliação quantitativa e qualitativa do risco à privacidade pela abertura de dados:

Qualitativo	Quantitativo	Descrição
Muito Alto	5	A abertura de dados provavelmente ocasionará diversos efeitos danosos aos indivíduos, a determinados grupos ou a outras organizações (Públicas ou privadas).
Alto	4	A abertura de dados provavelmente ocasionará algum de prejuízo aos indivíduos, a determinados grupos ou a outras organizações (Públicas ou privadas).
Moderado	3	A abertura de dados poderá, eventualmente, ocasionar prejuízos leves aos indivíduos, a determinados grupos ou a outras organizações (Públicas ou privadas).
Baixo	2	A abertura de dados ocasionará efeitos insignificantes aos indivíduos, a determinados grupos ou a outras organizações (públicas ou privadas).
Muito Baixo	1	Apenas dados anonimizados serão abertos.

- Referência para avaliação da possibilidade de ocorrência do risco:

Qualitativo	Quantitativo	Descrição
Muito Alto	5	O risco certamente ocorrerá.
Alto	4	O risco muito provavelmente ocorrerá.
Moderado	3	O risco poderá ocorrer.
Baixo	2	Existe uma possibilidade remota de o risco ocorrer.
Muito Baixo	1	O risco muito provavelmente não ocorrerá.

- Cruzamento das avaliações para análise de eventual proposição de abertura de dados, desde que sejam identificados benefícios aos indivíduos, a determinados grupos ou a outras organizações (públicas ou privadas):

Possibilidade de ocorrência do risco	Impacto do Risco				
	Muito Baixo	Baixo	Moderado	Alto	Muito Alto
Muito Baixo	Abrir	Abrir	Abrir com limitações de acesso	Abrir com limitações e acompanhamento periódico	Não abrir
Baixo	Abrir	Abrir	Abrir com limitações e acompanhamento periódico	Abrir com limitações e acompanhamento periódico	Não abrir
Moderado	Abrir	Abrir com limitações de acesso	Abrir com limitações e acompanhamento periódico	Não abrir	Não abrir
Alto	Abrir com limitações de acesso	Abrir com limitações de acesso	Não abrir	Não abrir	Não abrir
Muito Alto	Abrir com limitações de acesso	Abrir com limitações e acompanhamento periódico	Não abrir	Não abrir	Não abrir

São as proposições:

- Abrir: a recomendação pela abertura dos dados remonta em riscos à privacidade baixo ou baixo com a possibilidade de ocorrência igualmente remota (moderada, baixa ou muito baixa), quando acrescido de benefícios substanciais previstos aos indivíduos, a determinados grupos ou organizações (públicas ou privadas).
- Abrir com limitações de acesso: face aos benefícios substanciais previstos aos indivíduos, a determinados grupos ou organizações (públicas ou privadas) provenientes da abertura de dados, e aos riscos à privacidade serem moderado, baixo ou muito baixo, embora com possibilidade de ocorrência alta ou muito alta, recomenda-se a abertura dos dados com restrições. Nesse sentido, convém abrir para determinados grupos, sujeito à avaliação da conformidade às leis e normas aplicáveis e à celebração de contratos/termos de compromisso, vedando-se tratamentos de

reidentificação de titulares.

- Abrir com limitações de acesso e acompanhamento periódico: ainda que haja a previsão de benefícios aos indivíduos, a determinados grupos ou organizações (públicas ou privadas), o risco de impacto à privacidade é baixo, moderado e alto. Nesse sentido, para que a abertura seja viável, convém que seja restrita a determinados grupos, sujeito à avaliação da conformidade às leis e normas aplicáveis e à celebração de contratos/termos de compromisso, vedando-se tratamentos de reidentificação de titulares. Ademais, o responsável pela abertura dos dados deverá prover de estrutura e meios para acompanhamento e realização de auditorias.
- Não abrir: os riscos de impacto à privacidade e a respectiva possibilidade de ocorrência superam eventuais benefícios aos indivíduos, a determinados grupos ou organizações (públicas ou privadas) e, portanto, não se recomenda a abertura de dados.

Atenção: este material é meramente informativo e, por ele, pretende-se auxiliar nos projetos de abertura de dados. Não representa qualquer documento vinculativo. Por esse documento, não são assimiladas quaisquer responsabilidades jurídicas relativas aos tratamentos de dados pessoais. Recomenda-se a consulta de profissionais técnicos e jurídicos para a condução da conformidade legal.

Referências

AIRTON, José. História da ISO. **Cirius Quality**: Consultoria e Treinamento em Qualidade, 7 mar. 2023. Disponível em: https://ciriusquality.com.br/historia-da-iso/. Acesso em: 27 jan. 2023.

ASSEMBLEIA LEGISLATIVA DE PERNAMBUCO. Lei nº 14.804 de 14 de outubro de 2012. Regula o acesso a informações, no âmbito do Poder Executivo Estadual, e dá outras providências. **Diário Oficial do Estado** — Poder Executivo, 30 out. 2012, p. 4. Disponível em: https://legis.alepe.pe.gov.br/dadosReferenciais.aspx?id=1605.

ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO. Decreto nº 58.052 de 16 de maio de 201. Regulamenta a Lei federal nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações, e dá providências correlatas. **Casa Civil**, 16 maio 2012. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2012/decreto-58052-16.05.2012.html. Acesso em: 26 jan. 2023.

_____. Decreto nº 65.347, de 09 de dezembro de 2020. Dispõe sobre a aplicação da Lei federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), no âmbito do Estado de São Paulo João Doria, Governador do Estado de São Paulo, no uso de suas atribuições legais. **Diário Oficial**, São Paulo, 10 dez. 2020.

ASSEMBLEIA LEGISLATIVA DO ESTADO DO RIO GRANDE DO SUL. Decreto nº 53.523 de 3 de maio de 2017 [Institui Política de Dados Abertos do Poder Executivo Estadual]. **Diário Oficial do Estado**, n. 83, 4 mai. 2017. Disponível em: http://www.al.rs.gov.br/filerepository/repLegis/arquivos/DEC%2053.523.pdf.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Comunicação de incidente de segurança**. [s. l.], 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 27 jan. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**: Versão 1.0. Brasília, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf. Acesso em: 27 jan. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**: Versão 2.0. Brasília, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 27 jan. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Home**. [S. l.], 2023. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 27 jan. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Publicações da ANPD**. [s. l.], 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em: 27 jan. 2023.

BELLI, Luca; GUGLIELMI, Gilles J. L'Etat Digital: Numérisation de l'administration publique et administration publique du numérique. **Berger-Levrault**, Paris, 2022.

BELLI, Luca; BARROS, Marina; REIA, Jess. Les enjeux de l'encadrement et de la gouvernance de l'ouverture des données publiques au Brésil. **Revue française d'administration publique**, v. 3, n. 167, p 585-600, 2018.

BELLI, Luca. Como implementar a LGPD por meio da Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED). *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz. **Tratado de Proteção de Dados Pessoais**. Barueri: Editora Forense, 2020. p. 393-422.

BELLI, Luca. New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a post-Western Model of Data Governance. **Indian Journal of Law and Technology**. 2023.

_____. CyberBRICS: A Multidimensional Approach to Cybersecurity for the BRICS. In BELLI, Luca (Ed) CyberBRICS: **Cybersecurity Regulations in the BRICS Countries**. Springer: [s.n.], 2021.

BELLI, Luca; LORENZON, Laila; FERGUS, Luã; BRITTO, Walter. **The Brazilian Data Protection Law (LGPD)**: Unofficial English version. [s. l.], 2020. Disponível em: https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/. Acesso em: 26 jan. 2023.

BELLI, Luca; ZINGALES, Nicolo. Brazilian Data Protection Under Covid-19: Legal Certainty Is the Main Casualty. **CyberBRICS**, [s. l.], 2020. Disponível em: https://cyberbrics.info/brazilian-data-protection-under-covid-19-legal-certainty-is-the-main-casualty/. Acesso em: 26 jan. 2023.

BRASIL. Ministério do Planejamento, Orçamento e Gestão (Comitê Executivo do Governo Eletrônico). Oficinas de Planejamento Estratégico: Relatório Consolidado. Brasília: DF, 2004b, p.10. Disponível em: https://is.gd/pudufa

BRASIL. Subchefia para Assuntos Jurídicos. Decreto de 15 de setembro de 2011. Institui o Plano de Ação Nacional sobre Governo Aberto e dá outras providências. **Diário Oficial da União**, 16 set. 2011, p. 9. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Dsn/Dsn13117.htm.

_____. Subchefia para Assuntos Jurídicos. Decreto nº 8.777 de 11 de maio de 2015 [Institui a Política de Dados Abertos do Poder Executivo federal. **Diário Oficial da União**, 12 mai. 2015, p. 21. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8777.htm.

_____. Subchefia para Assuntos Jurídicos. Decreto nº 9.319 de 21 de março de 2018. Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. **Diário Oficial da União**, 22 mar. 2018, p. 2. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9319.htm.

_____. Subchefia para Assuntos Jurídicos. Decreto nº 9.903 de 8 de julho de 2019. Altera o Decreto nº 8.777, de 11 de maio de 2016, que institui a Política de Dados Abertos do Poder Executivo federal, para dispor sobre a gestão e os direitos de uso de dados abertos. **Diário Oficial da União**, 9 jul.

2019, p. 7. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9903.htm.

_____. Subchefia para Assuntos Jurídicos. Lei nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, 24 abr. 2014, p. 1. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

_____. Subchefia para Assuntos Jurídicos. Lei nº 14.129 de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. **Diário Oficial da União**, 30 mar. 2021, p. 3. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm.

CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS. **Ministério da Ciência, Tecnologia e Inovações. Estratégia Brasileira para a Transformação Digital (E-Digital):** Ciclo 2022-2026. Brasília, 2022. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf. Acesso em: 26 jan. 2023.

CERQUEIRA, C. M.; FERREIRA, J. P. S. Dados abertos para o fortalecimento da democracia em Goiás. **Diário da Manhã**, Goiânia, 15 dez. 2022. Disponível em: https://www.dm.com.br/opiniao-publica/dados-abertos-para-o-fortalecimento-da-democracia-em-goias-117587?_=amp. Acesso em: 26 jan. 2023.

CLOWDSTRIKE. **Global threat report 2022**. [s. l.], 2022. Disponível em: https://is.gd/Qkh4Pa. Acesso em: 27 jan. 2023.

COMISSÃO EUROPEIA. Comunicação, COM (2020) 66 final. **Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social europeu e ao Comitê das Regiões**, Bruxelas, 19 fev. 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020DC0066&from=EN. Acesso em: 26 jan. 2023.

CONTROLADORIA-GERAL DA UNIÃO. **Base de conhecimento da CGU**. [s. l.], [s. d.]. Disponível em: https://repositorio.cgu.gov.br/. Acesso em: 26 jan. 2023.

CONTROLADORIA-GERAL DA UNIÃO. **O que é a iniciativa**. [s. l.], 2022. Disponível em: https://www.gov.br/cgu/pt-br/governo-aberto/a-ogp/o-que-e-a-iniciativa#:~:text=A%20OGP%20foi%20lan%C3%A7ada%20em,apresentaram%20seus%20Planos%20de%20A%C3%A7%C3%A3o. Acesso em: 26 jan. 2023.

CONTROLADORIA-GERAL DA UNIÃO. **Time Brasil**. [s. l.], 2023. Disponível em: https://www.gov.br/cgu/pt-br/governo-aberto/time-brasil. Acesso em: 26 jan. 2023.

CONTROLADORIA-GERAL DO ESTADO DE MINAS GERAIS. Resolução CGE nº 020 de 6 de agosto de 2014. Estabelece conceitos e diretrizes, no âmbito da Administração direta, autárquica e fundacional do Poder Executivo Estadual, em matéria de dados abertos governamentais. **Diário do Executivo de Minas Gerais**, 7 ago. 2014, p. 63. Disponível em: http://pesquisalegislativa.mg.gov.br/LegislacaoCompleta.aspx?cod=171158

DEIRDRE LEE, Derilinx. Open Data Publishing Guidelines. Version: 1.1 (July 2021); Open Data Unit, Department of Public Expenditure and Reform. Disponível em: https://data.gov.ie/guidelines/index.html.

DEMING, D. Balancing Privacy with Data Sharing for the Public Good. **The New York Times**, Nova York, 19 fev. 2021. Disponível em: https://www.nytimes.com/2021/02/19/business/privacy-open-data-public.html. Acesso em: 26 jan. 2023.

DONEDA, Danilo. **Consultas públicas — Proteção de dados. 2020**. Disponível em: http://www.doneda.net/2020/03/08/consultas-publicas-protecao-de-dados/. Acesso em: 26 jan. 2023.

DONEDA, Danilo. **Da privacidade à Proteção de Dados Pessoais**: fundamentos da lei geral de proteção de dados. 3. ed. [s. L.]: Thomson Reuters Brasil, 2021.

EMPRESA MATO-GROSSENSE DE TECNOLOGIA DA INFORMAÇÃO. **Plano de Dados Abertos**: Ações — Dezembro de 2022 a Dezembro de 2024. Cuiabá, 2022. Disponível em: http://www.mt.gov.br/documents/2458894/0/PDA+PARA+PUBLICA%C3%87%C3%83O.pdf/a77ba2c9-b46e-96dd-0925-1780d847f3e9. Acesso em: 26 jan. 2023.

E-PING: **Padrões de Interoperabilidade de Governo Eletrônico**, versão 2018. Disponível em: https://eping.governoeletronico.gov.br/

EUROPEAN COMMISSION. **A European strategy for data**. COM, 66 final. Brussels, 19.2. 2020. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066.

FICHTNER, L. What kind of cyber security? Theorising cyber security and mapping approaches. **Internet Policy Review**, v. 7, n. 2, p. 1-19, 2018. Disponível https://doi.org/DOI:10.14763/2018.2.788

GARRETT, Filipe. O que é malware? Veja significado, tipos e saiba remover. **Techtudo**, 27 mar. 2021. Disponível em: https://www.techtudo.com.br/listas/2021/03/o-que-e-malware-veja-significado-tipos-e-saiba-remover.ghtml. Acesso em 27 jan. 2023.

GOVERNO DO ESTADO DE RONDÔNIA. Decreto nº 26.236 de 19 de julho de 2021. Institui Política de Dados Abertos do Poder Executivo Estadual. **Diário Oficial do Estado de Rondônia**, ed. 145, p. 4, 20 jul. 2021. Disponível em: https://rondonia.ro.gov.br/wp-content/uploads/2021/07/DECRETO-26236-DE-20-07-2021.pdf.

GOVERNO DO ESTADO DO ESPÍRITO SANTO. Decreto nº 5139-R de 13 de maio de 2022. Institui a Política de Dados Abertos da Administração Pública direta, autárquica e fundacional do Governo do Estado do Espírito Santo. **Diário Oficial dos Poderes do Estado**, ed. N25.736, 16 mai. 2022, p. 1. Disponível em: https://is.gd/PW72hv.

GOVERNO DO DISTRITO FEDERAL. Decreto nº 38.354 de 24 de julho de 2017. Institui a Política de Dados Abertos da Administração Pública direta, autárquica e fundacional do Distrito Federal. **Diário Oficial do Distrito Federal**, n. 141, 25 jul. 2017. Disponível em: https://www.sinj.df.gov.br/sinj/Norma/2a90db6875624a65936a47e18e1c337b/Decreto_38354_24_07_2017.html.

GOVERNO DO ESTADO DO MATO GROSSO DO SUL. **Legislação sobre dados abertos.** [s. l.], [s. d.]. Disponível em: http://www.dados.ms.gov.br/dataset/04d8c42b-a831-431a-beff-bcae94e2148c/resource/8a952515-29f5-4c03-a456-da2a25e0c824/download/legislacao-dados-abertos.pdf. Acesso em: 26 jan. 2023.

GOVERNO DO ESTADO DO PARÁ. **Portal da Transparência**: Legislações. [s. l.], 2010. Disponível em: http://www.transparencia.pa.gov.br/?q=node/21. Acesso em: 26 jan. 2023.

GOVERNO DO ESTADO DO RIO DE JANEIRO. Decreto nº 46.475 de 25 de outubro de 2001. Dispõe sobre o acesso a informações previsto no inciso XXXIII, do caput do Artigo 5º, no inciso II, do §3º do artigo 37, e no §2º, do artigo 216, todos da Constituição da República, e dá outras providências. Disponível em: http://www.cge.rj.gov.br/wp-content/uploads/2020/06/DECRETO-N%C2%BA-46.475-LAI-Consolidado.pdf.

GOVERNO DO MARANHÃO. Lei ordinária nº 10.204 de 23 de fevereiro de 2015. Cria a Secretaria de Transparência e Controle, altera as Leis nº 6.895, de 26 de dezembro de 1996, nº 9.571, de 28 de março de 2012 e a Lei nº 6.107, de 27 de julho de 1994, e dá outras providências. Disponível em: https://www3.stc.ma.gov.br/legisla-documento/?id=3803.

GRENN, et al. Open Data Privacy. **Berkman Klein Center for Internet & Society Research Publication**, 2017.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA. **Opinion 05/2014 on Anonymisation Techniques**. Bruxelas, 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 26 jan. 2023.

HAJE, L. Acesso à informação não pode ser prejudicado por conta de Lei de Proteção de Dados, dizem especialistas. **Agência Câmara de Notícias**, Brasília, 18 nov. 2021. Disponível em: https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de-protecao-de-dados-dizem-especialistas/. Acesso em: 20 dez. 2022.

HEVNER, A. R. A Three Cycle View of Design Science Research. **Scandinavian Journal of Information Systems**, v. 19, n. 2, p. 87-92, 2007.

HERRMANN, Augusto. Dados abertos: a retrospectiva de um comitê. Blog Herrmann Tech. 2020. Disponível em: https://herrmann.tech/pt/blog/2020/12/07/dados-abertos-a-retrospectiva-de-um-comite.html.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION [ISO]. **ISO 9001 and related standards**: Quality management. [s. l.], [s. d.]. Disponível em: https://www.iso.org/iso-9001-quality-management.html.

_____. **ISO/IEC 27001:2005**: Information technology — Security techniques — Information security management systems — Requirements. [s. l.], 2005. Disponível em: https://www.iso.org/standard/42103.html. Acesso em: 27 jan. 2023.

JEFFERSON Emily *et al*. Green paper: recommendations for disclosure control of trained machine learning (ML) models from trusted research environments. 2022. Disponível em: https://zenodo.org/record/7089491#.Yyt76HbMI2w.

KERASIDOU, Charalampia (Xaroula); MALONE, Maeve; DALY, Angela; TAVA, Francesco. Machine learning models, trusted research environments and UK health data: ensuring a safe and beneficial future for AI development in healthcare. **Journal of Medical Ethics**, 2023.

LIAROPOULOS, Andrew N. A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia. **Journal of Information Warfare**, v. 14, ed. 4, p. 15-24, 2015. Disponível em: https://www.jstor.org/stable/26487503. Acesso em: 26 jan. 2023.

MERCOSUL. **XII Reunión Ordinaria del Subgrupo de Trabajo nº 13 "Comercio Electrónico**". Buenos Aires, 14-15 jun. 2004. Disponível em: https://documentos.mercosur.int/simfiles/docreuniones/23116_SGT13_2004_ACTA02_ES.pdf. Acesso em: 26 jan. 2023.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS**. Do Eletrônico ao Digital**: linha do tempo — governo eletrônico. [s. l.], 2020. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital. Acesso em: 26 jan. 2023

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Governo Digital**: material de apoio. [s. l.], 2019. Disponível em: https://www.gov.br/governodigital/pt-br/dados-abertos/material-de-apoio. Acesso em: 26 jan. 2023.

MINISTÉRIO DA GESTÃO E INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Estratégia Nacional de Segurança Cibernética**. [s. l.], 2021. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/estrategia-nacional-de-seguranca-cibernetica. Acesso em: 27 jan. 2023.

MINISTÉRIO DA GESTÃO E INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Política Nacional de Segurança da Informação**. [s. l.], 2021. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/politica-nacional-de-seguranca-da-informacao. Acesso em: 27 jan. 2023.

MINISTÉRIO DA INFRAESTRUTURA. **INDE (Infraestrutura Nacional de Dados Espaciais)**. [s. l.], 2015. Disponível em: https://www.gov.br/infraestrutura/pt-br/assuntos/conteudo/inde-especificacoes-tecnicas. Acesso em: 26 jan. 2023

MINISTÉRIO DO ORÇAMENTO, PLANEJAMENTO E GESTÃO. Comitê Gestor da Infraestrutura Nacional de Dados Abertos. Resolução nº 3 de 13 de outubro de 2017. Aprova as normas sobre elaboração e publicação de Planos de Dados Abertos, conforme disposto no Decreto nº 8.777, de 11 de maio de 2016. **Diário Oficial da União**, 17 out. 2017. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes/resolucao-n-o-3-de-13-de-outubro-de-2017.

MINISTÉRIO DO ORÇAMENTO, PLANEJAMENTO E GESTÃO. **Estratégia Geral de Tecnologia da Informação**: ECTI 2011-2012. [s. l.], 2011. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/Estrategia_Geral_de_TI__2011_2012_SISP.pdf. Acesso em: 26 jan. 2023.

MOBILITY DATA. **GBFS e Política de Dados de Mobilidade Compartilhada**. [s. l.], 30 jun. 2021. Disponível em: https://mobilitydata.org/gbfs-e-politica-de-dados-de-mobilidade-compartilhada/. Acesso em: 20 dez. 2022.

O'HARA, K. **Transparent Government, Not Transparent Citizens**: A Report on Privacy and Transparency for the Cabinet Office. Londres, 2011. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61279/transparency-and-privacy-review-annex-a.pdf. Acesso em: 26 jan. 2023.

OPEN DATA INSTITUTE (ODI). **Anonymisation**: A Short Guide. Eticas Research and Consulting. 2018-2019. 2019. Disponível em: https://docs.google.com/document/d/15pzteCSuadyNkXnQ1k8pniOzRKITuiJQFhLQ8cQQT8E/edit#heading=h.8elmqg3mx84b.

OPEN DATA INSTITUTE (ODI). **Anonymising data in times of crisis**. 2020. Disponível em: https://theodi.org/article/anonymising-data-in-times-of-crisis/.

OPEN GOVERNMENT PARTNERSHIP. **São Paulo, Brazil**. [s. l.], 2023. Disponível em: https://www.opengovpartnership.org/members/sao-paulo-brazil/. Acesso em: 26 jan. 2023.

OPEN OWNERSHIP. **Principles for effective beneficial ownership disclosure** — updated January 2023. [s. l.], jan. 2023. Disponível em: https://www.openownership.org/en/principles/. Acesso em: 20 dez. 2022.

PORTAL BRASILEIRO DE DADOS ABERTOS. **Relatório da iniciativa**. [s. l.], [s. d.]. Disponível em: https://is.gd/2hymC5. Acesso em: 26 jan. 2023.

SCHULTES, Erik; WITTENBURG, Peter. FAIR Principles and Digital Objects: Accelerating Convergence on a Data Infrastructure. *In*: MANOLOPOULOS, Y.; STUPNIKOV, S. (Ed.). Data Analytics and Management in Data Intensive Domains. **Communications in Computer and Information Science**, Springer, v. 1003, 2019.

SECRETARIA DE FAZENDA DO ESTADO DA BAHIA. Guia de publicação de dados abertos. [s,.l], 2022. Disponível em: https://www.sefaz.ba.gov.br/administracao/controle_interno/Guia_Portal_Dados_Abertos.pdf. Acesso em: 26 jan. 2023.

STF valida compartilhamento de dados mediante requisitos. **Supremo Tribunal Federal**, Brasília, 15 set. 2019. Disponível em: https://portal.stf.

jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=494227&ori=1. Acesso em: 26 jan. 2023.

UK Health Data Research Alliance and NHSX. **Building trusted research environments** — principles and best practices; towards TRE ecosystems (1.0). Zenodo, 2021.

VAN DEN BERG, J. A Basic Set of Mental Models for Understanding and Dealing with the Cyber-Security Challenges of Today. **Journal of Information Warfare**, v. 19, n. 1, p. 26–47, 2020.

WHYTE, J. Cybersecurity, race, and the politics of truth. **Security Dialogue**, i. 53(a), p. 342-362, 2022.

WOLFF, J. What we talk about when we talk about cybersecurity: Security in Internet governance debates. **Internet Policy Review**, v. 5, n. 3, 2016.

WOOD, Alexandr; O'BRIEN, David; GASSER, Urs. Privacy and Open Data Research Briefing (26 de setembro de 2016). **Publicação de pesquisa do Berkman Klein Center nº 2016-16**. Disponível em: https://ssrn.com/abstract=2842816

WORLD WIDE WEB CONSORTIUM — ESCRITÓRIO BRASIL. **Dados abertos governamentais**. [s. l.], [s. d.]. Disponível em: https://www.w3c.br/pub/Materiais/PublicacoesW3C/dados-abertos-governamentais.pdf. Acesso em: 19 jan. 2023.

WORLD WIDE WEB CONSORTIUM [W3C]. **Boas práticas para dados na web**. [s. l.], 2017. Disponível em: https://w3c.br/traducoes/DWBP-pt-br/#intro. Acesso em: 26 jan. 2023.

ZELETI, F. A., OJO, A., & CURRY, E. Exploring the economic value of open government data. **Government Information Quarterly**, v. 33, n. 3, 535-551. 2016.

ZWITTER, Andrej; GSTREIN, Oskar J. Big data, privacy and COVID-19 — learning from humanitarian expertise in data protection. **Journal Of International Humanitarian Action,** v. 5, n. 1, p. 1-7, 18 maio 2020.

Conheça melhor a editora Lumen Juris

www.lumenjuris.com.br
@lumenjuriseditora
publique@lumenjuris.com.br

É com notável apreço que apresentamos o livro *Governança de Dados no Setor Público*, resultado de uma colaboração excepcional entre o CTS-FGV, Centro de Tecnologia e Sociedade da Fundação Getulio Vargas, Escola de Direito, Rio de Janeiro, e a UNU-EGOV, United Nations University Operating Unit on Policy-Driven Electronic Governance. Este trabalho emerge do Memorando de Entendimento estabelecido entre as duas instituições, refletindo seu comprometimento conjunto com a promoção e aprimoramento das práticas de governança e transformação digital no âmbito do setor público.

A obra aborda de maneira abrangente as complexidades da governança e regulação de dados no contexto público, promovendo uma visão integrada que conecta a abertura de dados, a proteção de dados pessoais e a segurança da informação.

Este estudo interconecta dimensões cruciais da transformação digital sustentável e oferece uma análise complexa do arcabouço regulatório no Brasil, identificando boas práticas, normas e recomendações sobre abertura, proteção e segurança de dados para administradores públicos.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

UNU

ISBN 978-85-519-2992-6

Lumen Juris Direito | 35 anos