MÉTODO RNP PARA CONFORMIDADE À LGPD

VERSÃO 2.0

REALIZAÇÃO

RNP

Lisandro Zambenedetti Granville
Diretor Geral

Eduardo Cezar Grizendi
Diretor de Engenharia e Operações

Emilio Tissato Nakamura
Diretor Adjunto de Cibersegurança

Liliana Esther Velásquez Alegre Solha
Gerente de Projetos Especiais de Segurança

ATUALIZAÇÕES DE VERSÃO

VERSÃO	TÍTULO	ANO
1.0	**Método RNP para Adequação à LGPD**	**2022**
2.0	**Método RNP para Conformidade à LGPD**	**2025**

AGRADECIMENTOS INSTITUCIONAIS

A construção do **Método RNP para Conformidade à LGPD – Versão 2.0** reúne o compromisso contínuo da Rede Nacional de Ensino e Pesquisa com a proteção de dados pessoais e o fortalecimento de uma cultura de privacidade nas instituições conectadas.

Este material é resultado de um processo que envolveu a escuta ativa, a expertise técnica e o engajamento de uma rede qualificada de Especialistas em segurança e privacidade, Gestores de TI e de Segurança, e Encarregados pelo tratamento de dados pessoais de diferentes instituições. Ao longo de sua elaboração, foram promovidos encontros, validações e discussões que contribuíram significativamente para o seu aprimoramento do material, a definição de diretrizes e a identificação de soluções aplicáveis.

Esse compromisso coletivo reforça o papel da RNP como articuladora de uma comunidade que valoriza o conhecimento compartilhado, a ética, a transparência e a responsabilidade com os dados pessoais.

A RNP expressa seu sincero agradecimento a todos(as) que, direta ou indiretamente, contribuíram para a consolidação desta segunda versão do Método RNP para Conformidade à LGPD.

ESSE COMPROMISSO COLETIVO REFORÇA O PAPEL DA RNP COMO ARTICULADORA DE UMA COMUNIDADE QUE VALORIZA O CONHECIMENTO COMPARTILHADO, A ÉTICA, A TRANSPARÊNCIA E A RESPONSABILIDADE COM OS DADOS PESSOAIS.

© Rede Nacional de Ensino e Pesquisa (RNP), 2025. Este material está licenciado sob uma
Licença Creative Commons Atribuição-NãoComercial 4.0 Internacional (CC BY-NC 4.0).

Licença de Uso – Atribuição Não Comercial 4.0 Internacional (CC BY-NC 4.0)

VOCÊ É LIVRE PARA:

1. Compartilhar – copiar e redistribuir o material em qualquer meio ou formato.

2. Adaptar – remixar, transformar e criar a partir do material.

O licenciante não pode revogar essas permissões, desde que os termos da licença sejam respeitados.

TERMOS DE USO:

- ATRIBUIÇÃO:
  É obrigatória a devida atribuição de autoria, fornecendo crédito apropriado, link para a licença e indicação de eventuais modificações, sem sugerir endosso por parte do autor.
- USO NÃO COMERCIAL:
  O material não pode ser utilizado para fins comerciais.
- SEM RESTRIÇÕES ADICIONAIS:
  Não é permitido aplicar restrições legais ou tecnológicas que impeçam os usos autorizados por esta licença.

LICENÇA COMPLETA DISPONÍVEL EM:
https://creativecommons.org/licenses/by-nc/4.0/

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS
ANPD	AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
APF	ADMINISTRAÇÃO PÚBLICA FEDERAL
ATPP	AGENTES DE TRATAMENTO DE PEQUENO PORTE
CNIL	COMISSÃO NACIONAL DE INFORMÁTICA E LIBERDADE DA FRANÇA
CNS	CONSELHO NACIONAL DE SAÚDE
COBIT	CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGIES (OBJETIVOS DE CONTROLE PARA INFORMAÇÃO E TECNOLOGIA RELACIONADA)
DPO	DATA PROTECTION OFFICER (ENCARREGADO DE PROTEÇÃO DE DADOS)
EDPB	EUROPEAN DATA PROTECTION BOARD (COMITÊ EUROPEU PARA A PROTEÇÃO DE DADOS)
ENAP	ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA
ENISA	EUROPEAN UNION AGENCY FOR CYBERSECURITY (AGÊNCIA EUROPEIA PARA CIBERSEGURANÇA)
ETP	ESTUDO TÉCNICO PRELIMINAR
FIOCRUZ	FUNDAÇÃO OSWALDO CRUZ
FINEP	FINANCIADORA DE ESTUDOS E PROJETOS
GDPR	GENERAL DATA PROTECTION REGULATION (REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA)
IAPP	INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (ASSOCIAÇÃO INTERNACIONAL DE PROFISSIONAIS DE PRIVACIDADE)
IFPR	INSTITUTO FEDERAL DO PARANÁ
INEP	INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS
ISACA	INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ASSOCIAÇÃO DE AUDITORIA E CONTROLE DE SISTEMAS DE INFORMAÇÃO)
ISO	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
LAI	LEI DE ACESSO A INFORMAÇÃO
LGPD	LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS
MCTI	MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
MGI	MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS
NIST	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
NPF	NIST PRIVACY FRAMEWORK (FRAMEWORK DE PRIVACIDADE DO NIST)
PDCA	PLAN, DO, CHECK, ACT (PLANEJAR, FAZER, VERIFICAR, AGIR)
PIPC	COMISSÃO DE PROTEÇÃO DE INFORMAÇÕES PESSOAIS DA COREIA DO SUL
PGP	PROGRAMA DE GOVERNANÇA EM PRIVACIDADE
PPSI	PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO
PSI	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
RCIS	REGULAMENTO DE COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA
RIPD	RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS
RNP	REDE NACIONAL DE ENSINO E PESQUISA
SGD	SECRETARIA DO GOVERNO DIGITAL
SISP	SISTEMA DE ADMINISTRAÇÃO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO
STF	SUPREMO TRIBUNAL FEDERAL
TCU	TRIBUNAL DE CONTAS DA UNIÃO
TIC	TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
UFOP	UNIVERSIDADE FEDERAL DE OURO PRETO

APRESENTAÇÃO DO MÉTODO RNP PARA CONFORMIDADE À LGPD

A **Lei Geral de Proteção de Dados Pessoais (LGPD)**, instituída pela Lei nº 13.709 em 14 de agosto de 2018, impôs às organizações públicas e privadas a necessidade de se adequarem a uma série de diretrizes para o tratamento adequado de dados pessoais, além de conferir aos titulares um papel central na gestão do uso de suas informações.

É importante destacar que, no contexto do fortalecimento jurídico no Brasil sobre o tema, a **Emenda Constitucional nº 115/2022** elevou a proteção de dados pessoais à categoria de **direito fundamental** dos cidadãos brasileiros.

Neste contexto, a Rede Nacional de Ensino e Pesquisa (RNP) desenvolveu o **Método RNP para Conformidade à LGPD (Método RNP)** para auxiliar organizações na estruturação ou aprimoramento do Programa de Governança em Privacidade. Com abordagem educativa e voltada para a aplicação prática da LGPD, o Método RNP apresenta módulos que abordam temas, como: governança, mapeamento de dados, gestão de riscos, resposta a incidentes, medidas de segurança e atendimento de titulares.

O Método RNP é fruto de esforço colaborativo que envolveu grupo de trabalho composto por pesquisadores e profissionais da área, além de projetos-piloto implementados em instituições parceiras e contribuições compartilhadas por meio do SIG-LGPD@RNP.

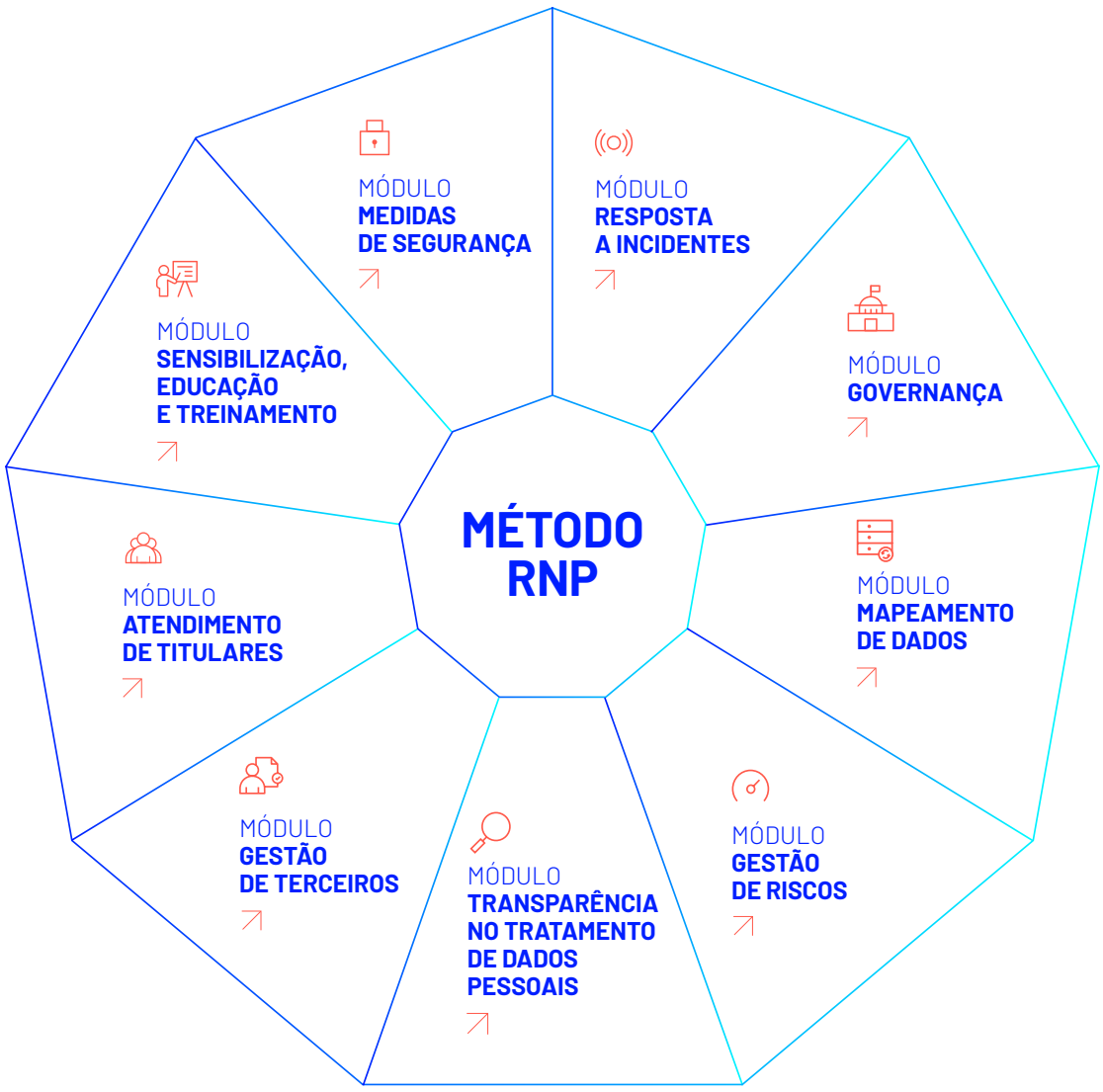
O Método RNP destina-se a organizações de diferentes perfis e níveis de maturidade em relação à LGPD. Seu principal objetivo é oferecer orientações e ferramentas para a estruturação e manutenção de processos e rotinas alinhados à LGPD, promovendo transparência, segurança e respeito aos direitos dos titulares de dados pessoais.

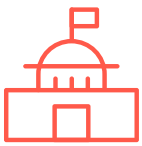
O que você encontrará neste material?

O Método RNP é estruturado em módulos, contendo artefatos e boas práticas, organizados de forma não linear, permitindo a construção e gestão de Programa de Governança em Privacidade que atenda às diretrizes da LGPD.

Os módulos do Método RNP abordam rotinas de conformidade com a LGPD, estruturados em consonância com fundamentos presentes em *frameworks* consolidados, como o NIST Privacy Framework e o Programa de Privacidade e Segurança da Informação (PPSI).

A seguir, veja o que cada módulo contempla:





MÓDULO **GOVERNANÇA**

Apresenta a estruturação do **Programa de Governança em Privacidade (PGP)**, abordando a definição de missão e visão, a adoção de *frameworks* (NIST Privacy Framework, ISO/IEC 27701) e a nomeação do **Encarregado pelo Tratamento de Dados.** Também trata da criação de um **Comitê Multidisciplinar** e integração do programa à estrutura organizacional e da aplicação do ciclo **PDCA (*Plan-Do-Check-Act*)**. Ainda, este módulo destaca a importância de **monitoramento contínuo** para a evolução do Programa de Governança em Privacidade.

MÓDULO **MAPEAMENTO DE DADOS**

Explica como identificar e documentar atividades de **tratamento de dados pessoais**, desde a fase de diagnóstico até a elaboração do **Inventário de Dados Pessoais**. Aborda o **conteúdo do mapeamento**, como o levantamento dos dados pessoais tratados, as finalidades, hipóteses legais, compartilhamentos, mecanismos de transferência internacional, medidas de segurança, prazos de retenção, etc. Também enfatiza a necessidade de atualização contínua e a definição de **planos de ação** para mitigar riscos.

MÓDULO **GESTÃO DE RISCOS**

Detalha o processo de gestão de riscos relacionados ao tratamento de dados pessoais, contemplando metodologias de identificação, análise e mitigação de riscos. Também aborda a necessidade de elaboração de **Relatórios de Impacto à Proteção de Dados (RIPD)** para atividades de alto risco.

MÓDULO **TRANSPARÊNCIA NO TRATAMENTO DE DADOS PESSOAIS**

Trata da obrigação de fornecer informações claras aos titulares, abordando a elaboração de **Avisos de Privacidade, Termos de Uso e Políticas de Cookies**. Explica como estruturar um **Portal da Privacidade**, disponibilizando informações sobre direitos dos titulares, identidade do Encarregado e meios de contato.

MÓDULO
GESTÃO DE TERCEIRROS

Explora as melhores práticas para a **contratação e monitoramento de fornecedores e terceiros** que realizam o tratamento de dados pessoais em nome da Organização, garantindo conformidade e segurança jurídica nas relações contratuais.

MÓDULO
ATENDIMENTO DE TITULARES

Apresenta diretrizes para estruturar um **canal de atendimento eficiente aos titulares**. Explica o fluxo para atendimento de direitos de titulares, além da necessidade de controle de prazos e documentação das interações para conformidade regulatória.

MÓDULO
SENSIBILIZAÇÃO, EDUCAÇÃO E TREINAMENTO

Foca na criação de uma **cultura organizacional de privacidade**, apresentando estratégias para **sensibilização, campanhas educativas e treinamentos periódicos**. Explica como estruturar treinamentos gerais e direcionados, garantindo que colaboradores compreendam suas responsabilidades e propõe abordagens para **capacitação contínua**.

MÓDULO
MEDIDAS DE SEGURANÇA

Fornece orientações sobre **boas práticas em segurança** para proteger os dados pessoais, considerando normas e refêrencias nacionais e internacionais. Também orienta sobre a criação de uma **Política de Segurança da Informação (PSI)** e a adoção de um **termo de responsabilidade para colaboradores**.

MÓDULO
RESPOSTA A INCIDENTES

Explica como preparar a Organização para lidar com incidentes de segurança envolvendo dados pessoais, incluindo a elaboração de um **Plano de Resposta a Incidentes, protocolos de comunicação à ANPD e aos titulares** e estratégias para **contenção e mitigação de danos.**

Como utilizar este material?

Cada módulo traz elementos, recomendações práticas e, quando aplicável, modelos de documentos e ferramentas que podem ser adaptadas à realidade de diferentes organizações.

O Método RNP não exige que os módulos sejam seguidos em uma sequência linear, o que o torna mais flexível, dinâmico e adaptável à realidade de cada organização. Essa característica permite que as instituições ajustem o processo de adequação e gestão do Programa de Governança em Privacidade conforme suas necessidades específicas e estágio de maturidade.

O Método RNP é, portanto, essencial para organizações que buscam não apenas cumprir as exigências legais, mas também fortalecer a confiança dos titulares de dados e consolidar boas práticas de governança e privacidade.

Para facilitar a compreensão dos termos e definições utilizados ao longo do Método RNP, recomenda-se a leitura conjunta com o material publicado pela Autoridade Nacional de Proteção de Dados (ANPD).

Glossário da Autoridade Nacional de Proteção de Dados.

CONCEITOS E FIGURAS IMPORTANTES

Sem prejuízo da consulta ao **Glossário da Autoridade Nacional de Proteção de Dados**, destacaremos neste tópico alguns conceitos e figuras mencionados no Método RNP.

O que significa tratar um dado pessoal?

De acordo com o artigo 5º, inciso X, da LGPD, tratamento é: "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (Brasil, 2018).

Qualquer atividade de tratamento implica a necessidade de medidas de proteção dos dados envolvidos e o atendimento das regras e princípios estabelecidos na LGPD.

Quem é o titular de dados pessoais?

O **titular de dados pessoais** é a **pessoa natural** a quem os dados pessoais se referem, conforme definido no **artigo 5º, inciso V, da LGPD**. Trata-se do indivíduo que fornece suas informações a uma organização ou tem seus dados coletados e tratados por ela.

Os titulares podem fornecer seus dados para contratar ou usufruir de serviços prestados, seja por empresas públicas ou privadas. Além disso, a LGPD garante ao titular uma série de direitos sobre seus dados pessoais. Para saber mais sobre o exercício desses direitos e como atendê-los, consulte o **Módulo Atendimento de Titulares**.

Os titulares de dados podem incluir diferentes perfis de indivíduos, como:

FUNCIONÁRIOS, EMPREGADOS PÚBLICOS E SERVIDORES

PRESTADORES DE SERVIÇOS E TERCEIRIZADOS

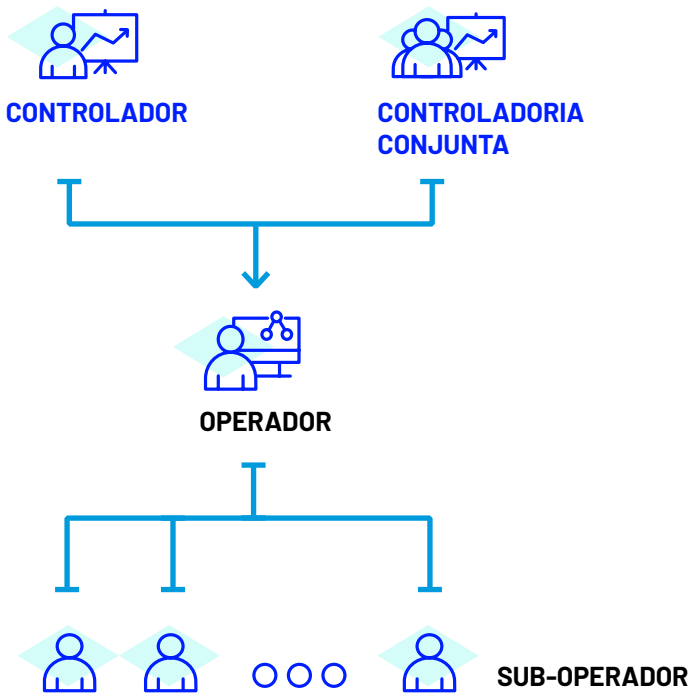
PESQUISADORES E ALUNOS DE INSTITUIÇÕES ACADÊMICAS

A proteção dos direitos dos titulares é um dos princípios fundamentais da LGPD e deve orientar as atividades de todos os agentes de tratamento de dados.

Quais são os agentes de tratamento de dados?

Os agentes de tratamento são as pessoas físicas ou jurídicas, de direito público ou privado, responsáveis pelo tratamento de dados pessoais, conforme figura a seguir:

FIGURA 1 _ AGENTES DE TRATAMENTO



CONTROLADOR

O controlador é **responsável por tomar decisões relativas ao tratamento de dados pessoais**. Ele determina as diretrizes e finalidades do tratamento, sendo o principal responsável pelo cumprimento da LGPD e pela adoção de medidas de segurança e governança em privacidade.

Exemplos:

01_ Uma universidade coleta, armazena e utiliza dados pessoais de alunos (como nome, CPF, histórico escolar e informações de contato) para fins de matrícula, emissão de diplomas, controle de frequência e desempenho acadêmico.

02_ Um instituto federal realiza concursos públicos ou vestibulares, definindo os critérios, o formulário de inscrição e a finalidade do uso dos dados.

03_ Uma universidade gerencia os dados de seus servidores e empregados (efetivos e terceirizados) para fins de folha de pagamento, controle de ponto, benefícios, avaliação de desempenho etc.

04_ Uma instituição de ensino superior implementa um sistema para gerenciamento de projetos de pesquisa e extensão, coletando dados de professores, alunos, bolsistas e participantes externos.

CONTROLADORIA CONJUNTA

Em alguns casos, uma mesma operação de tratamento de dados pessoais pode envolver mais de um controlador. Quando dois ou mais controladores determinam **conjuntamente** os propósitos e meios de tratamento de dados pessoais, podem ser considerados como **controladores conjuntos**. Essa figura, embora não prevista na LGPD, foi sugerida pela Autoridade Nacional de Proteção de Dados no Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Nesse cenário, compartilham as responsabilidades no cumprimento das obrigações legais, especialmente em relação ao exercício dos direitos dos titulares e ao fornecimento de informações, mediante acordo entre eles.

Exemplos:

01_ Duas universidades desenvolvem e mantêm em conjunto um sistema de autenticação federada para acesso a serviços acadêmicos. Ambas definem de forma conjunta as finalidades e regras do tratamento dos dados de identificação e acesso dos usuários. Nesse cenário, as instituições podem ser caracterizadas como controladoras conjuntas.

02_ Duas instituições de ensino superior coordenam, conjuntamente, um programa de intercâmbio de alunos, estabelecendo políticas comuns para coleta, armazenamento e uso dos dados dos participantes. Dependendo da forma como as decisões são tomadas, podem exercer controladoria conjunta.

03_ Três instituições coorganizam um congresso científico e gerenciam juntas os dados de inscrição, pagamento e emissão de certificados. Ao definirem conjuntamente os propósitos e meios do tratamento desses dados, podem ser consideradas controladoras conjuntas.

OPERADOR

O operador é **quem realiza o tratamento de dados pessoais em nome do controlador**, seguindo suas instruções. Embora, em geral, o operador seja uma pessoa jurídica, nada impede que uma pessoa física também seja considerada operadora de dados.

Exemplos:

01_ Uma universidade firma contrato com uma empresa especializada em AVA (Ambiente Virtual de Aprendizagem) para hospedar, manter e operar a plataforma utilizada por alunos e docentes. Nessa situação, a empresa prestadora de serviço pode ser caracterizada como operadora, ao tratar os dados conforme as instruções da universidade.

02_ Uma instituição contrata uma empresa de *call center* para prestar atendimento ao público externo (alunos, responsáveis e comunidade em geral). Caso a empresa atue conforme os procedimentos definidos pela instituição, ela tende a assumir o papel de operadora no tratamento dos dados.

03_ Uma universidade contrata uma consultoria para aplicar avaliações institucionais envolvendo alunos, servidores e docentes. Dependendo do grau de autonomia no tratamento dos dados, a consultoria pode ser considerada operadora, caso siga exclusivamente as orientações da contratante.

Importante: conforme entendimento da ANPD, funcionários que tratam dados pessoais sob subordinação direta ao controlador não são considerados operadores.

Importante: vale destacar que uma mesma organização pode assumir papeis distintos a depender das circunstâncias existentes. Logo, pode ser **tanto controladora quanto operadora**, considerando sua função em diferentes operações de tratamento de dados pessoais.

SUBOPERADOR

O suboperador é contratado pelo operador para auxiliá-lo na execução das atividades de tratamento de dados. Ele deve seguir estritamente as determinações acordadas entre o controlador e o operador.

Exemplos:

01_ Uma empresa especializada em AVA (Ambiente Virtual de Aprendizagem), contratada por uma universidade, subcontrata um provedor de serviços em nuvem para hospedar os dados dos usuários da plataforma. Caso o provedor atue apenas conforme as orientações da contratada (operadora), sem autonomia nas decisões sobre o tratamento, pode ser caracterizado como suboperador.

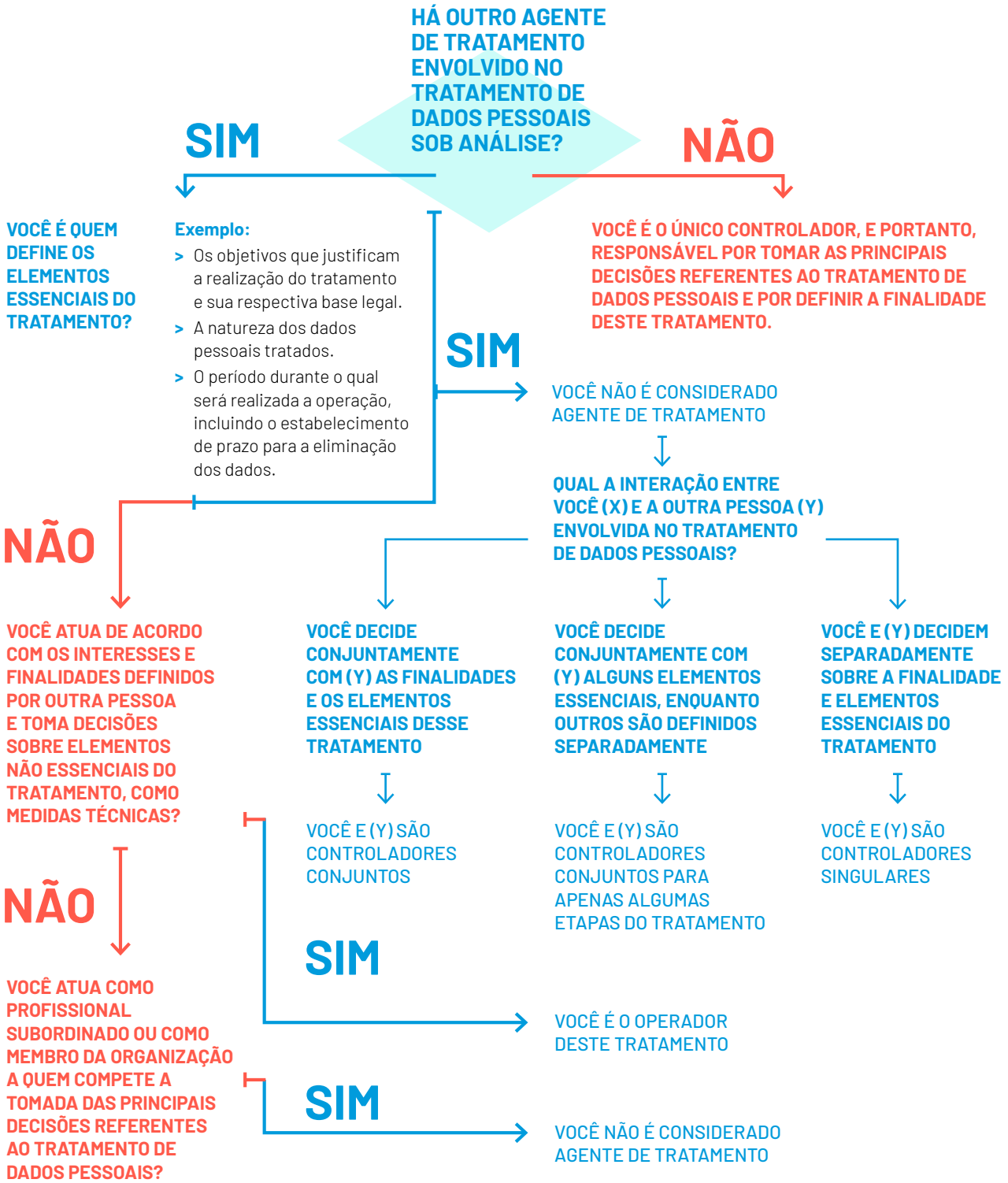
02_ Uma consultoria é contratada por uma empresa responsável pelo processamento da folha de pagamento de uma instituição para dar suporte técnico e manutenção nos sistemas utilizados. Quando atua sob as instruções da operadora, a consultoria pode ser considerada suboperadora.

03_ Uma empresa de *call center*, contratada por uma instituição para atendimento ao público, firma contrato com uma prestadora de serviços de *backup* para garantir a segurança dos dados tratados. A empresa de *backup*, sem definir finalidades próprias, pode atuar como suboperadora.

A figura apresenta, de forma resumida, a aplicabilidade dos conceitos de agentes de tratamento, conforme a publicação da ANPD:

Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado

FIGURA 2 _ CONCEITOS DE AGENTES DE TRATAMENTO DE DADOS PESSOAIS



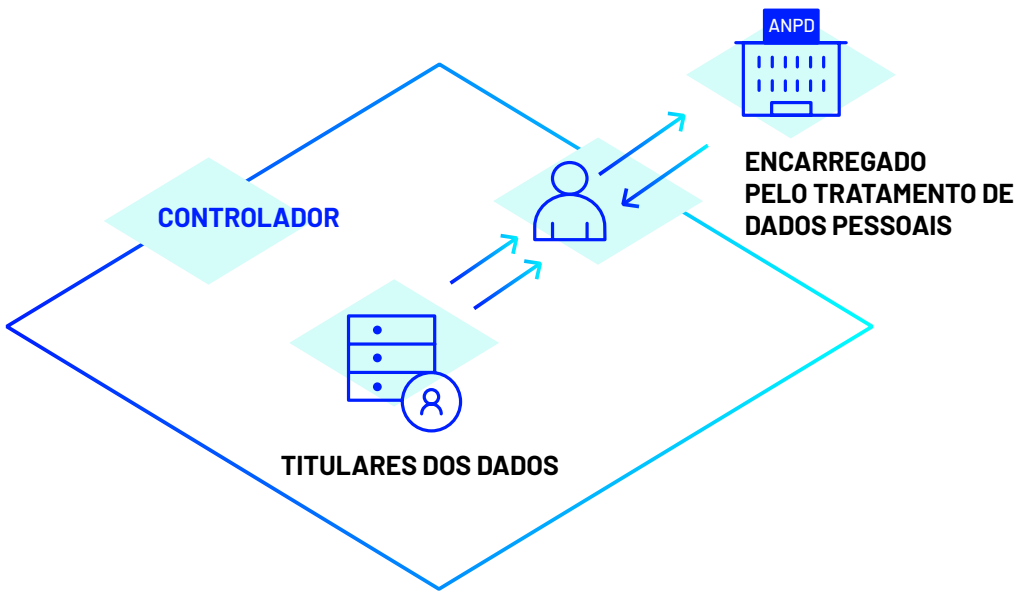
Fonte: Autoridade Nacional de Proteção de Dados (2022d, p. 25).

Importante: os exemplos apresentados neste tópico são ilustrativos e não possuem caráter vinculativo. A definição do papel de cada agente de tratamento (controlador, operador, controlador conjunto etc.) deve ser realizada com base nas especificidades de cada relação contratual e prática de tratamento, observando o contexto, as finalidades e o grau de autonomia na tomada de decisões relacionadas aos dados pessoais.

Quem é o Encarregado?

O **Encarregado pelo Tratamento de Dados Pessoais** é a pessoa indicada pelo controlador para atuar como canal de comunicação entre a organização, os titulares dos dados e a **Autoridade Nacional de Proteção de Dados (ANPD)**, conforme figura a seguir:

FIGURA 3 _ PAPEL DO ENCARREGADO COMO ELO ENTRE OS TITULARES, A ORGANIZAÇÃO E A ANPD



A nomeação do Encarregado é prevista no **artigo 41 da LGPD** e sua função é essencial para a governança em privacidade dentro das organizações.

A obrigatoriedade da nomeação do Encarregado pode variar conforme o porte da organização e o volume de dados tratados. A **Resolução CD/ANPD nº 2/2022** flexibilizou essa exigência para agentes de pequeno porte, como microempresas, *startups* e organizações de menor estrutura. No entanto, independentemente da obrigatoriedade legal, a presença do Encarregado é considerada uma **boa prática de governança em privacidade**, aumentando a transparência e a segurança jurídica da organização.

Para saber mais sobre as atribuições do Encarregado, como realizar a sua nomeação e a importância de divulgar informações a seu respeito, consulte o **Módulo Governança.**

Quem é a Autoridade Nacional de Proteção de Dados (ANPD)?

A **Autoridade Nacional de Proteção de Dados (ANPD)** é o órgão responsável por **zelar, implementar e fiscalizar** o cumprimento da LGPD no Brasil. Suas competências estão previstas no **art. 55-J da LGPD** e incluem:

01_ Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e Privacidade;

02_ Fiscalizar e aplicar sanções administrativas a agentes de tratamento que descumpram a legislação;

03_ Promover o conhecimento das normas de proteção de dados entre a população;

04_ Fomentar a cooperação com autoridades de proteção de dados de outros países;

05_ Orientar titulares de dados pessoais e agentes de tratamento sobre a correta aplicação da LGPD.

A ANPD tem papel fundamental na garantia da conformidade com a LGPD e na criação de normas complementares para esclarecer aspectos da legislação. A sociedade, os agentes de tratamento e os titulares devem acompanhar as orientações emitidas pela ANPD por meio de seus regulamentos e guias técnicos.

ACESSE!

Além da fiscalização, a ANPD também tem uma função educativa e publica materiais para auxiliar agentes de tratamento e titulares de dados pessoais. A Autoridade disponibiliza guias orientativos, normativos e documentos técnicos em suas Centrais de Conteúdo. Esses materiais são referência para o entendimento da legislação e podem ser utilizados para a capacitação de colaboradores e na estruturação de programas de governança em privacidade.

Centrais de Conteúdo

FISCALIZAÇÃO, SANÇÕES E RISCOS DA NÃO CONFORMIDADE COM A LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece um conjunto de regras para o tratamento de dados pessoais no Brasil, impondo obrigações a organizações públicas e privadas. O não cumprimento dessas normas pode resultar em **sanções administrativas, processos regulatórios e riscos reputacionais**. Aqui abordaremos os aspectos essenciais do processo de fiscalização conduzido pela **Autoridade Nacional de Proteção de Dados (ANPD)**, a aplicação de penalidades e os impactos reputacionais da não conformidade.

Como é o processo de fiscalização da ANPD?

A **ANPD** é a autoridade responsável por fiscalizar a aplicação da LGPD e garantir o cumprimento das normas de proteção de dados pessoais. A **Resolução CD/ANPD nº 1/2021** aprovou o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Já a Portaria nº 1 de 8 de março de 2021 estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados.

A fiscalização realizada pela ANPD tem como objetivo garantir o cumprimento da LGPD, avaliar o grau de adequação das organizações e mitigar riscos relacionados à proteção de dados pessoais. Esse processo pode ser conduzido por meio de diferentes mecanismos de controle, incluindo monitoramento, averiguação preliminar e processos administrativos sancionadores.

AÇÕES DE MONITORAMENTO:
Atuação preventiva, acompanhamento de boas práticas e avaliação de setores específicos.

PROCEDIMENTOS DE AVERIGUAÇÃO PRELIMINAR:
Investigação inicial sobre indícios de irregularidades.

PROCESSOS ADMINISTRATIVOS SANCIONADORES:
Aplicação de penalidades formais contra organizações que descumpram a LGPD.

O **monitoramento** tem um papel essencial na prevenção de infrações e na promoção de boas práticas. A ANPD realiza esse monitoramento por meio de **acompanhamento de setores específicos**, identificando setores críticos onde há maior risco de violação da LGPD e emitindo diretrizes específicas para esses segmentos, **análise de padrões de tratamento de dados,** examinando as práticas adotadas por instituições de grande porte e setores estratégicos para avaliar sua conformidade, **e orientação regulatória,** por meio da elaboração de guias e manuais explicativos que permitem que as organizações compreendam melhor suas obrigações legais.

Segundo a **Resolução CD/ANPD nº 4/2023**, que regulamenta a fiscalização, o monitoramento também pode incluir auditorias programadas e revisões periódicas de medidas de segurança e governança.

Passando para a **averiguação preliminar**, trata-se de uma etapa investigativa inicial, utilizada para verificar indícios de irregularidades antes da abertura de um processo sancionador..

Os principais instrumentos dessa fase incluem:

REQUISIÇÃO DE INFORMAÇÕES:
A ANPD pode solicitar dados e documentos para esclarecer aspectos do tratamento de dados.

CONVOCAÇÃO PARA ESCLARECIMENTOS:
Organizações podem ser chamadas a prestar informações sobre suas práticas de conformidade.

ADOÇÃO DE MEDIDAS CORRETIVAS VOLUNTÁRIAS:
A ANPD pode recomendar que a organização tome providências para ajustar-se à legislação.

Caso as irregularidades não sejam resolvidas nessa etapa e a ANPD identifique violações à LGPD, pode ser instaurado um **processo administrativo sancionador**. Esse processo segue ritos formais e pode resultar na aplicação de penalidades previstas no **artigo 52 da LGPD**.

A LGPD também concede aos titulares de dados o direito de questionar práticas de tratamento de dados pessoais e denunciar possíveis violações. As denúncias podem ser feitas diretamente por meio do Sistema de Requerimentos à ANPD. A ANPD considera essas manifestações no planejamento de ações de fiscalização, nas melhorias regulatórias e em suas ações educativas.

Sistema de Requerimentos à ANPD

Quais são as sanções administrativas?

A aplicação de sanções pela ANPD segue critérios estabelecidos no **Regulamento de Dosimetria e Aplicação de Sanções Administrativas da ANPD (Resolução CD/ANPD nº 7/2023)**. As penalidades variam de advertências a multas significativas e até proibição do tratamento de dados.

Conforme o **artigo 52 da LGPD**, as sanções aplicáveis incluem:

01_ Advertência: em caso de infração leve, sem danos significativos aos titulares.

02_ Multa simples: até **2% do faturamento da organização**, limitada a **R$ 50 milhões por infração.**

03_ Multa diária: para incentivar a regularização da infração.

04_ Publicização da infração: divulgação da irregularidade para alertar titulares e sociedade.

05_ Bloqueio dos dados pessoais: suspensão do uso dos dados até a regularização.

06_ Eliminação dos dados: determinação para que a organização apague os dados pessoais tratados em desconformidade.

07_ Suspensão parcial do funcionamento do banco de dados: impede a organização de realizar tratamento de dados por um período determinado.

08_ Proibição total ou parcial do exercício de atividades relacionadas ao tratamento de dados: em casos extremos, pode inviabilizar o funcionamento da organização.

O art. 52, §3º da LGPD determina que não se aplica a instituições públicas a penalidade de multa, seja ela simples ou diária. Todas as demais sanções previstas são aplicáveis.

Já a dosimetria (forma de cálculo) das sanções considera fatores como a **natureza e gravidade da infração**, o **dano causado aos titulares,** o **grau de boa-fé e colaboração da organização,** a **adoção de medidas preventivas e corretivas** e a **reincidência em práticas irregulares.**

Organizações que implementam Programas de Governança em Privacidade e demonstram comprometimento com boas práticas podem atenuar penalidades ou até evitar sanções mais severas.

É fundamental também destacar que o servidor público que violar a LGPD pode ser responsabilizado administrativamente de forma pessoal e autônoma, conforme estabelece o **art. 28 do Decreto-Lei nº 4.657/1942** (Lei de Introdução às Normas do Direito Brasileiro). Isso significa que condutas irregulares, como comercialização indevida de bancos de dados, alteração ou exclusão inadequada de cadastros, ou o uso de informações pessoais para finalidades ilícitas, podem resultar em sanções diretamente ao agente público responsável pelo ato.

MÓDULO GOVERNANÇA

Neste módulo você encontrará respostas para as seguintes perguntas:

1.1_ *Qual a importância da governança em um programa de privacidade?*

1.2_ *Qual a importância e como definir a visão e missão no contexto do programa de governança em privacidade?*

1.3_ *Como delimitar o escopo do programa de governança em privacidade?*

1.4_ *Adoção de* frameworks*: qual a relevância e quais critérios devem ser considerados na escolha?*

1.5_ *Como desenvolver um plano estratégico para criação e manutenção de um programa de governança em privacidade?*

1.6_ *Como estruturar e quem deve compor a estrutura do programa de governança em privacidade?*

1.7_ *Quais são as especificidades da posição de Encarregado pelo tratamento de dados?*

1.8_ *Quais documentos devem compor um programa de governança em privacidade?*

1.9_ *Quais os requisitos mínimos de uma Política de Proteção de Dados Pessoais?*

1.10_ *O que é e qual a importância do* Privacy by Design*?*

1.11_ *Como monitorar a maturidade do programa de governança em privacidade?*

Artefatos relacionados:

ARTEFATO Nº 1_ *Sugestão de Portaria para estruturação do Comitê Multidisciplinar*

ARTEFATO Nº 2_ *Modelo da ANPD de ato formal para indicação de encarregado pessoa natural*

ARTEFATO Nº 3_ *Modelo da ANPD de ato formal para indicação de encarregado pessoa jurídica*

ARTEFATO Nº 4_ *Modelo de Política de Proteção de Dados Pessoais do PPSI*

1.1_ Qual a importância da governança em um programa de privacidade?

De acordo com o **Instituto Brasileiro de Governança Corporativa**, governança corporativa é um "sistema formado por princípios, regras, estruturas e processos pelos quais as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização" (Instituto Brasileiro de Governança Corporativa, 2023).

Segundo o **artigo 50º da LGPD**, um Programa de Governança em Privacidade (PGP) deve considerar:

> [...] as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (Brasil, 2018).

O § 2º, incisos I e II, do mesmo artigo estabelece o conjunto mínimo de componentes a ser considerado na implementação de um Programa de Governança em Privacidade (PGP).

> [...] a) demonstrar o **comprometimento do controlador** em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) ser **aplicável a todo o conjunto de dados pessoais** que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) ser **adaptado** à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabelecer **políticas e salvaguardas adequadas** com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) ter o objetivo de

> estabelecer **relação de confiança com o titular**, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) estar **integrado a sua estrutura geral de governança** e estabeleça e aplique mecanismos de supervisão internos e externos; g) conter **planos de resposta a incidentes** e remediação; e h) ser **atualizado constantemente** com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas. II. **demonstrar a efetividade** de seu Programa de Governança em Privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei (Brasil, 2018, grifo nosso).

É possível perceber, portanto, que a governança em privacidade vai além da simples adequação à Lei Geral de Proteção de Dados Pessoais (LGPD). Trata-se, portanto, de um conjunto de práticas, pessoas e processos que visa edificar e manter uma cultura organizacional orientada pela transparência, ética, respeito a direitos e prestação de contas.

Na tentativa de abranger todos os aspectos que envolvem a construção e gestão de um Programa de Governança em Privacidade, recorremos à abordagem apresentada no livro ***Privacy Program Management***, publicado pela Associação Internacional de Profissionais de Privacidade (APP). Essa estrutura, organizada em cinco elementos, oferece um guia prático para orientar a implementação e gestão de um PGP que seja abrangente e adaptável às especificidades de cada instituição.

Elementos para estruturação e manutenção de um PGP:

DEFINIÇÃO DA VISÃO E MISSÃO NO CONTEXTO DA PRIVACIDADE

DELIMITAÇÃO DO ESCOPO DO PGP

SELEÇÃO DE UM *FRAMEWORK* DE PRIVACIDADE ADEQUADO

DESENVOLVIMENTO DA ESTRATÉGIA DE PRIVACIDADE

ESTRUTURAÇÃO DA EQUIPE RESPONSÁVEL PELA GOVERNANÇA DA PRIVACIDADE

Além dos tópicos acima, adiciona-se a essa fórmula, a elaboração e gestão de documentos que formalizem as diretrizes do Programa de Governança em Privacidade, assegurando padronização, aplicabilidade das regras estabelecidas e o monitoramento contínuo do programa.

Embora os componentes apresentados neste módulo sejam amplamente reconhecidos como boas práticas e sirvam de referência para a estruturação e gestão de Programas de Governança em Privacidade, sua aplicação pode variar conforme as especificidades e demandas de cada instituição.

A seguir, aprofundaremos análise desses elementos e seu papel na construção ou manutenção de um PGP que privilegie a flexibilidade e a adaptação ao contexto específico de cada instituição.

1.2_ Qual a importância e como definir a visão e missão no contexto do programa de governança em privacidade?

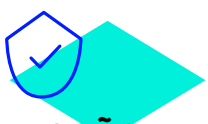
Embora este seja um passo de simples execução, a definição e comunicação claras da **visão** e **missão** do Programa de Governança em Privacidade desempenham papel estratégico, pois pacificam a compreensão de todos os integrantes da instituição, desde a liderança até parceiros externos, acerca da **razão de ser/existir** do PGP.

Essa abordagem orienta as iniciativas relacionadas ao programa, garantindo que estejam em conformidade com os objetivos da instituição. Além disso, a consolidação desses elementos fortalece a cultura de segurança e proteção de dados e assegura elevado nível de transparência junto a todas as partes interessadas da instituição.

Para estruturar a visão e missão de sua instituição, é importante considerar que a **missão** deve comunicar de forma clara o propósito do PGP, enquanto a **visão** deve refletir a ambição de longo prazo e os princípios que guiarão as rotinas relacionadas ao programa.

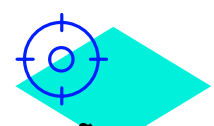
É possível a opção por uma abordagem unificada. Nesse caso, os conceitos de missão e visão podem ser integrados em uma única declaração. De acordo com o livro *Privacy Program Management*, da IAPP, essa declaração deve ser elaborada de forma concisa, composta por poucas sentenças, de forma que a leitura não ultrapasse o período de 30 segundos.

Dicas para elaboração de declarações de missão e visão:



MISSÃO:

Descreva o propósito central do PGP, enfatizando seu compromisso com a proteção de dados e a conformidade regulatória.



VISÃO:

Articule as aspirações futuras do programa, destacando objetivos de longo prazo e princípios orientadores.

A seguir, relaciona-se alguns exemplos:

Information Commissioner's Office (ICO) Autoridade de Proteção de Dados do Reino Unido

Clique aqui para acessar a publicação

MISSÃO:

"Manter os direitos de informação no interesse público, promovendo a abertura por parte dos órgãos públicos e a privacidade dos dados para os indivíduos" (Information Commissioner's Office, 2016, tradução nossa).

VISÃO:

Ser reconhecido por nossos *stakeholders* como o árbitro autoritário dos direitos de informação, entregando resultados de alta qualidade, relevantes e oportunos, com uma abordagem responsiva e voltada para o exterior, e com uma equipe comprometida e de alto desempenho — um modelo de boa regulação e um ótimo lugar para trabalhar e se desenvolver (Information Commissioner's Office, 2016, tradução nossa).

Universidade de Stanford

Clique aqui para acessar a publicação

Nossa **missão** é ajudar a Universidade de Stanford a cumprir essas expectativas e responsabilidades perante os indivíduos e, de maneira mais ampla, **defender o uso de dados de forma justa, transparente, ética e inovadora**. Diante das inúmeras mudanças no cenário da privacidade nos últimos anos, é mais importante do que nunca que a universidade não apenas atenda às suas obrigações regulatórias básicas, mas também reflita criticamente sobre como priorizar, de maneira específica, a proteção da privacidade como um direito humano fundamental (University Stanford, 2021, tradução nossa, grifo nosso).

Autoridade Belga de Proteção de Dados

Clique aqui para acessar a publicação

"Em um mundo e uma sociedade em rápida mudança, nossa **missão** é: Liderar em direção a um mundo digital onde a **privacidade seja uma realidade para todos**" (Autorité de Protection des Données, c2025, grifo nosso).

1.3_ Como delimitar o escopo do programa de governança em privacidade?

Naturalmente, cada instituição possui características próprias, incluindo um conjunto específico de obrigações regulatórias. Dessa forma, para que o PGP seja efetivo, é importante que esteja alinhado à realidade da instituição, integrando-se às rotinas e normativas já estabelecidas.

Dois fatores podem ser determinantes para essa efetividade, primeiramente, a identificação e o conhecimento das atividades internas que envolvem o tratamento de dados pessoais, permitindo compreender a razão de existência de cada fluxo dentro da instituição. O segundo fator está atrelado ao mapeamento das leis e regulamentos aplicáveis à realidade da instituição, incluindo aqueles relacionados à segurança e à proteção de dados, de forma a garantir que o escopo do PGP esteja adequado às exigências operacionais e legais.

A identificação das atividades que envolvem o tratamento de dados pessoais é apresentada pelo Método RNP no **Módulo Mapeamento de Dados,** fornecendo diretrizes para mapear processos, compreender suas finalidades e avaliar eventuais riscos à privacidade e à segurança da informação.

No que se refere à identificação do conjunto de leis e normativos aplicáveis, é fundamental reconhecer que esse mapeamento deve ser feito de maneira personalizada, considerando a realidade específica da instituição.

De forma a ilustrar o exercício de mapeamento de regulamentações aplicáveis, sugere-se que esse levantamento contemple tanto **normativas de aplicação geral**, como a Lei Geral de Proteção de Dados Pessoais (LGPD), o Marco Civil da Internet e a Lei de Acesso à Informação (LAI), quanto **legislações específicas voltadas para determinados setores**.

A tabela a seguir sintetiza esse exercício, que deve ser adaptado à realidade de cada instituição:

TABELA 1 _ LEGISLAÇÕES DE APLICAÇÃO GERAL E ESPECÍFICA

Legislações de aplicação geral	
Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018	
Marco Civil da Internet - Lei nº 12.965/2014	
Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011	
Legislações de aplicação específica	
Instituições de pesquisa e inovação	Marco Legal da Ciência, Tecnologia e Inovação Lei nº 10.973/2004
Centros de pesquisa em saúde	Lei Orgânica da Saúde Lei nº 8.080/1990 e Resoluções do Conselho Nacional de Saúde
Museus e instituições culturais	Estatuto dos Museus - Lei nº 11.904/2009

Fonte: elaboração própria.

1.4_ Adoção de *frameworks*: qual a relevância e quais critérios devem ser considerados na escolha?

Diante do desafio de gerenciar múltiplos princípios, direitos e obrigações, como transparência, gestão de riscos e comunicação de incidentes de segurança, optar por um *framework* já existente ou desenvolver um modelo próprio pode surgir como solução para pacificar direcionamentos e metas relacionadas ao PGP.

Segundo a *Information Systems Audit and Control Association* (ISACA), associação internacional focada em governança de tecnologia da informação e auditoria de sistemas, responsável por publicações de grande impacto como o *Controls Objectives for Information and Related Technology* (COBIT), um *framework* pode ser definido como: **"conjunto integrado de processos, estruturas organizacionais e diretrizes que suportam a governança"** (ISACA, 2018, grifo nosso).

No livro *Privacy Program Management*, da IAPP, o termo *framework* é empregado de forma abrangente para designar uma variedade de processos, modelos, padrões de mercado, guias e ferramentas que orientam o profissional de privacidade na gestão do programa de governança de sua instituição.

Atualmente, diversos *frameworks* podem servir como base para gestão de programas de governança em privacidade. A seguir, apresentamos modelos referência que têm sido amplamente adotados para essa finalidade:

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

O Programa de Privacidade e Segurança da Informação, também conhecido como PPSI é uma proposta da Secretaria de Governo Digital (SGD) que visa elevar a maturidade e a resiliência de órgãos e entidades da administração pública federal direta, autárquica e fundacional que possuem unidades que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), nas áreas de privacidade e segurança da informação.

Instituído por meio da Portaria SGD/MGI nº 852 de 2023, o PPSI dispõe de *framework* de privacidade e segurança da informação, composto por conjunto de controles, metodologias e ferramentas de apoio.

De acordo com o artigo 8º da referida Portaria, a adoção deste *framework* é obrigatória para órgãos e entidades integrantes do SISP sujeitas ao PPSI. É importante destacar que, embora não seja obrigatório para todas as instituições do Sistema RNP, este *framework* pode servir como referência na gestão do Programa de Governança em Privacidade.

O artigo 9º da Portaria que instituiu o PPSI divide em quatro as etapas para implementação deste *framework*:

01_ Autoavaliação: avaliação pela própria instituição, considerando a ferramenta disponibilizada pela SGD.

02_ Análise de lacunas: a partir da autoavaliação, esta etapa consiste na identificação de oportunidades melhorias.

03_ Planejamento: esta fase consiste no planejamento estratégico para adoção dos controles considerados como oportunidades de melhorias, definindo a forma, prazo de execução e aspectos orçamentários atrelados.

04_ Implementação: esta etapa inclui a efetiva adoção de medidas de melhoria, bem como a definição de rotinas que permitam a melhoria contínua dos controles já implementados.

As entidades sujeitas ao PPSI devem seguir ciclos de medição periódicos, priorizando a implementação de controles considerados como prioritários pela Secretaria de Governo Digital. Mesmo as instituições que não se enquadram no PPSI devem estabelecer processo regular de medição dos controles, o que, conforme o §5º do artigo 10º da Portaria do PPSI deve ocorrer a cada 12 meses.

ACESSE!

Com base no PPSI e visando oferecer subsídios para a estruturação e gestão de Programas de Governança em Privacidade por órgãos e entidades públicas, especialmente aquelas sujeitas à aplicação do PPSI, a Secretaria de Governo Digital (SGD) publicou

Guia de Elaboração de Programa de Governança em Privacidade

Ferramenta PPSI, Ciclo 4

Cartilha do Programa de Privacidade Segurança da Informação (PPSI)

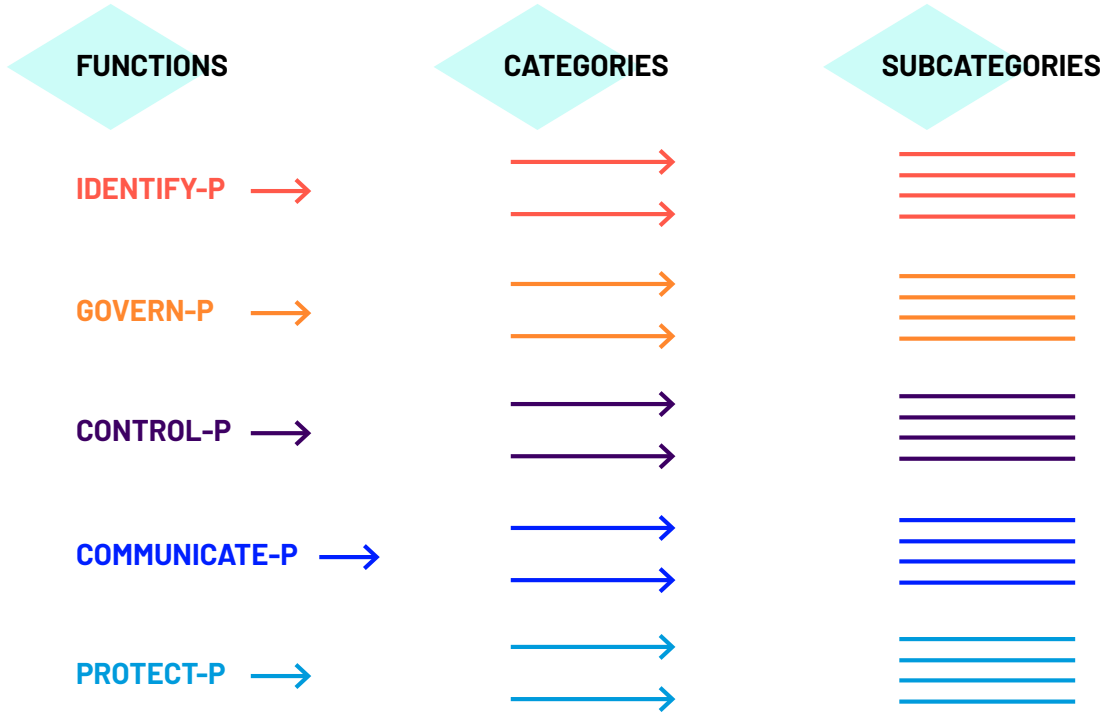
NIST PRIVACY FRAMEWORK

O NIST Privacy Framework (NPF) é um modelo voltado para a gestão de riscos de privacidade, baseado em práticas já consolidadas pelo NIST Cybersecurity Framework.

A estrutura do NIST Privacy Framework é flexível e pode ser adaptada a diferentes setores e tipos de organizações. Quanto à estrutura, o NPF é dividido em três principais componentes: *core* (núcleo), *profiles* (perfis) e *implementation tiers* (níveis de implementação).

O *core* é a espinha dorsal do NIST Privacy Framework, estruturando um conjunto de atividades e resultados para a proteção de dados e a gestão de privacidade. O *core* organiza a governança de privacidade em Funções, Categorias e Subcategorias.

FIGURA 4 _ *PRIVACY FRAMEWORK CORE STRUCTURE*



Fonte: National Institute of Standars and Technology (2020. p. 10).

Cada **Função** do *core* aborda aspectos relevantes de privacidade e direciona a instituição na implementação de práticas de proteção de dados. As funções do **NIST Privacy Framework** são:

Identify-P **(Identificar-P)**

Foca na compreensão dos riscos de privacidade da instituição, mapeando os dados processados e definindo responsabilidades para gestão do Programa de Governança em Privacidade.

Govern-P **(Governar-P)**

Abrange a criação de políticas, diretrizes e processos que integram privacidade à governança.

Control-P **(Controlar-P)**

Trata do gerenciamento do ciclo de vida dos dados, implementando controles técnicos e administrativos para minimizar riscos e proteger informações pessoais.

Communicate-P **(Comunicar-P)**

Garante a transparência no tratamento de dados pessoais, abrangendo a comunicação com os titulares e a notificação de incidentes de segurança.

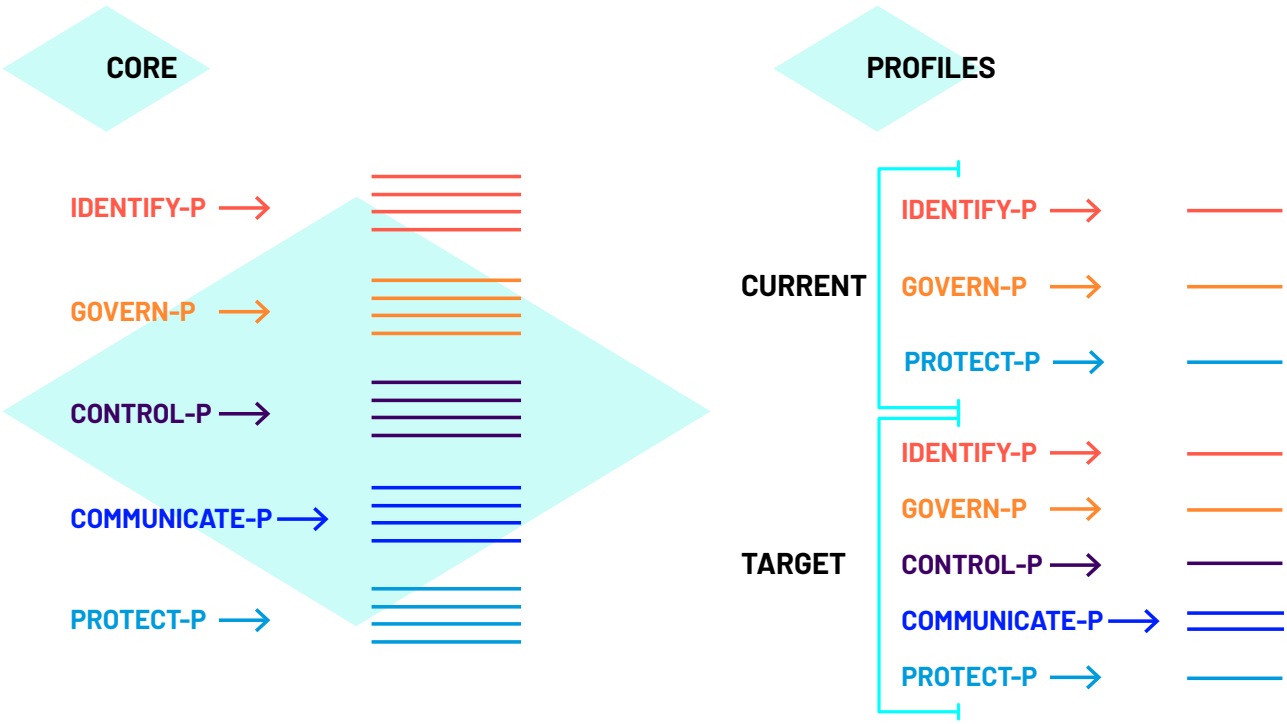
Protect-P **(Proteger-P)**

Envolve medidas de segurança cibernética para prevenir e mitigar impactos de incidentes como acessos indevidos.

As categorias subdividem as funções em grupos menores, representando resultados específicos para atender às necessidades do programa de privacidade. Cada Categoria agrupa atividades que visam auxiliar a instituição a alcançar seus objetivos de governança e proteção de dados. As subcategorias, por sua vez, refinam ainda mais as categorias, detalhando os resultados esperados de ações técnicas e de gestão.

Profile (perfil) deve ser construído com base nos elementos do *core*, permitindo que a organização identifique quais atividades são mais relevantes para sua realidade. Após identificação das atividades relevantes, é possível comparar o perfil atual com o perfil alvo (pretendido), permitindo planejamento de melhorias e avaliação do progresso ao longo do tempo.

FIGURA 5_ *RELATIONSHIP BETWEEN CORE AND PROFILES*



Fonte: National Institute Of Standars And Technology (2020, p. 12).

Implementation tiers (níveis de implementação) representam os diferentes níveis de maturidade na gestão de privacidade, indo de abordagens básicas e reativas (nível 1) até estratégias bem estruturadas e integradas ao gerenciamento de riscos da organização (nível 4).

ACESSE!

Para saber mais sobre esse tema, consulte:

NIST Cybersecurity Framework

Guia de Implementação do NIST Privacy Framework

NORMAS ISO

A International Organization for Standardization (ISO), é responsável pelo desenvolvimento e publicação de normas técnicas que estabelecem padrões para diversas áreas, incluindo a produção de produtos e a gestão de processos. Entre essas normas, há diretrizes específicas para segurança da informação e proteção de dados, que podem ser utilizadas como ferramentas na gestão de Programas de Governança em Privacidade.

Embora a ISO não emita nem realize certificações diretamente, suas normas são amplamente adotadas por organismos de certificação independentes como referência para certificar organizações que desejam demonstrar a implementação de controles mínimos exigidos para esses temas. Para segurança da informação e proteção de dados, algumas normas e diretrizes da **ISO/IEC** podem servir como referência:

01_ ISO/IEC 27001. Gestão da Segurança da Informação: define requisitos para a implementação e manutenção de sistemas de gestão em segurança da informação, estabelecendo controles para proteger dados contra ameaças e vulnerabilidades, incluindo medidas organizacionais, como políticas de segurança e técnicas, como controle de acessos e criptografia.

02_ ISO/IEC 27701. Gestão da Privacidade da Informação: extensão da ISO/IEC 27001, voltada especificamente para a proteção de dados pessoais, estabelecendo requisitos para um sistema de gestão em privacidade.

03_ ISO/IEC 27002. Código de Boas Práticas para Controles de Segurança da Informação: complementa a ISO/IEC 27001, oferecendo diretrizes sobre controles de segurança da informação aplicáveis para proteção de dados e mitigação de riscos. Essa norma não é certificável, pois serve como um guia de boas práticas para adoção de medidas de segurança.

1.5_ Como desenvolver um plano estratégico para criação e manutenção de um programa de governança em privacidade?

A estratégia de privacidade compreende a definição de objetivos e a implementação de ações voltadas à estruturação, manutenção e aprimoramento do Programa de Governança em Privacidade. A formulação dessa estratégia está intrinsicamente ligada à eventual adoção de *frameworks* de privacidade, inclusive aqueles já mencionados no item 1.3. do Método RNP, que podem servir como referência para a definição de diretrizes, requisitos e controles aplicáveis ao PGP.

Para viabilizar a aplicação prática desses controles, a combinação entre os controles previstos nos *frameworks* de privacidade e abordagens metodológicas voltadas à gestão de ações possibilita direcionamento preciso para a implementação de cada medida estabelecida no PGP.

Nesse contexto, metodologias como o ciclo PDCA (*Plan-Do-Check-Act*) podem ser utilizadas em conjunto com *frameworks*, como PPSI e NIST Privacy Framework, para direcionar a implementação e o aprimoramento contínuo do Programa de Governança em Privacidade.

FIGURA 6_ CICLO PDCA (*PLAN-DO-CHECK-ACT*)

Fonte: adaptado de ISO/IEC 27001:2022.

A aplicação do ciclo PDCA no contexto do PGP possibilita um fluxo estruturado de implementação e monitoramento. Na fase de planejamento (Planejar), são definidos os objetivos, políticas e procedimentos com base nos requisitos do *framework* adotado. A fase de execução (Fazer) envolve a implementação das diretrizes estabelecidas, incorporando os controles e processos definidos. O monitoramento (Checar) avalia se as ações executadas atendem aos critérios estabelecidos, permitindo a identificação de pontos de melhoria. Na fase de ajuste (Agir), as práticas adotadas são revisadas, e as correções ou otimizações necessárias são aplicadas, garantindo a evolução do programa.

Essa abordagem, que inclusive é mencionada no **Guia de Elaboração de Programa de Governança em Privacidade**, já mencionado no Método RNP, permite que eventuais *frameworks* de privacidade sejam implementados de forma dinâmica e adaptável, assegurando que o PGP permaneça alinhado aos requisitos regulatórios e às necessidades da instituição.

Guia de Elaboração de Programa de Governança em Privacidade

1.6_ Como estruturar e quem deve compor a estrutura do programa de governança em privacidade?

A governança em privacidade exige uma abordagem abrangente, envolvendo diferentes áreas da organização. Para garantir essa integração, é fundamental definir os atores responsáveis pela execução do PGP.

De partida, é importante ressaltar que a composição do PGP não segue um modelo único ou conjunto fixo de participantes. Essa estrutura pode variar conforme a realidade e complexidade de cada instituição, considerando fatores como serviços prestados, riscos associados, quantidade de servidores e colaboradores e recursos disponíveis.

Apesar de não haver conjunto fixo, a Lei Geral de Proteção de Dados Pessoais (artigo 41º) e a Portaria SGD/MGI nº 852/2023, aplicável a órgãos e entidade da administração pública federal direta, autárquica e fundacional que compõem o SISP, estabelecem alguns papéis mínimos.

Segundo a LGPD (artigo 41º) instituições controladoras de dados pessoais devem indicar Encarregado pelo Tratamento de Dados. Na prática, a nomeação de um Encarregado é obrigatória para qualquer pessoa jurídica de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, exceto em casos específicos de agentes de pequeno porte. No entanto, independentemente da obrigatoriedade, a presença desse profissional é considerada uma boa prática de governança.

O **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**, publicado pela ANPD em 2022, esclarece que a LGPD não impede que o Encarregado conte com o apoio de uma equipe de proteção de dados. Pelo contrário, de acordo com as boas práticas, **é recomendável que o Encarregado disponha de recursos adequados, incluindo recursos humanos, para garantir a conformidade** dos processos internos com a LGPD e outras normas de proteção de dados.

Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado

Veja os casos da Fundação Oswaldo Cruz (Fiocruz), que, **além de contar com um Encarregado titular e adjunto, dispõe de uma equipe dedicada à proteção de dados**, e o Sistema Sebrae, **onde cada uma das 27 unidades federativas designou um Encarregado de dados**.

Para órgãos e entidades sujeitos ao PPSI, para além da figura do Encarregado, outros representantes devem compor essa estrutura:

01_ Gestor de Tecnologia da Informação: responsável por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações.

02_ Gestor de Segurança da Informação: responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação, conforme Instrução Normativa 1 de 27 de maio de 2020 do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

03_ Responsável pela Unidade de Controle Interno: responsável por apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa (áreas responsáveis pela execução direta das atividades e pelo gerenciamento dos riscos inerentes aos seus processos) previsto na Instrução Normativa CGU nº 3, de 9 de junho de 2017.

A depender da composição da organização, o PGP pode envolver outras estruturas complementares, a exemplo de comitê multidisciplinar relacionado a privacidade e proteção de dados, que poderá atuar tanto no desenvolvimento e implementação, quanto na tomada de decisões estratégicas.

Esse comitê, inclusive, já foi adotado por alguns órgãos governamentais, como o Ministério da Gestão e da Inovação em Serviços Públicos, por meio da **Portaria MGI nº 7.601, de 27 de novembro de 2023**.

A criação de comitês pode ser obrigatória dependendo do contexto e da realidade de cada organização. Por exemplo, a Administração Pública Federal tem a obrigação de instituir um Comitê de Segurança da Informação ou estrutura equivalente, conforme disposto no art. 15º, inciso II, da norma aplicável.

Tanto a criação de novos comitês quanto a utilização ou ampliação de grupos já existentes promovem uma atuação coordenada entre diferentes áreas da organização, fortalecendo a governança e a gestão do Programa de Governança em Privacidade. Além disso, a participação de representantes da alta direção tende a aumentar o comprometimento institucional com o tema, facilitando a incorporação das diretrizes de privacidade nas práticas organizacionais.

ACESSE!

No Artefato nº 1, é possível visualizar uma sugestão de Portaria para estruturação do Comitê no caso de instituições públicas, que deve ser adaptada conforme as particularidades de cada organização.

Artefato nº 1

Veja o exemplo da **Portaria nº 105/2024** do Supremo Tribunal Federal (STF) que implementou grupo de trabalho para apoiar a adequação da instituição às normas da LGPD.

Portaria nº 105/2024

Veja também o **Pregão Eletrônico nº 09/2021** da Financiadora de Estudos e Projetos (FINEP), que adotou a estratégia de contratação de serviços de consultoria. Outros exemplos de Termos de Referência:

Pregão Eletrônico 09/2021

Câmara Municipal de Pará de Minas

Conselho Federal de Química

Governo do Estado do Mato Grosso do Sul

1.7_ Quais são as especificidades da posição de Encarregado pelo tratamento de dados?

Segundo o § 2º do artigo 41º da LGPD, o Encarregado deve desempenhar as seguintes funções:

01_ Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

02_ Receber comunicações da autoridade nacional e adotar providências;

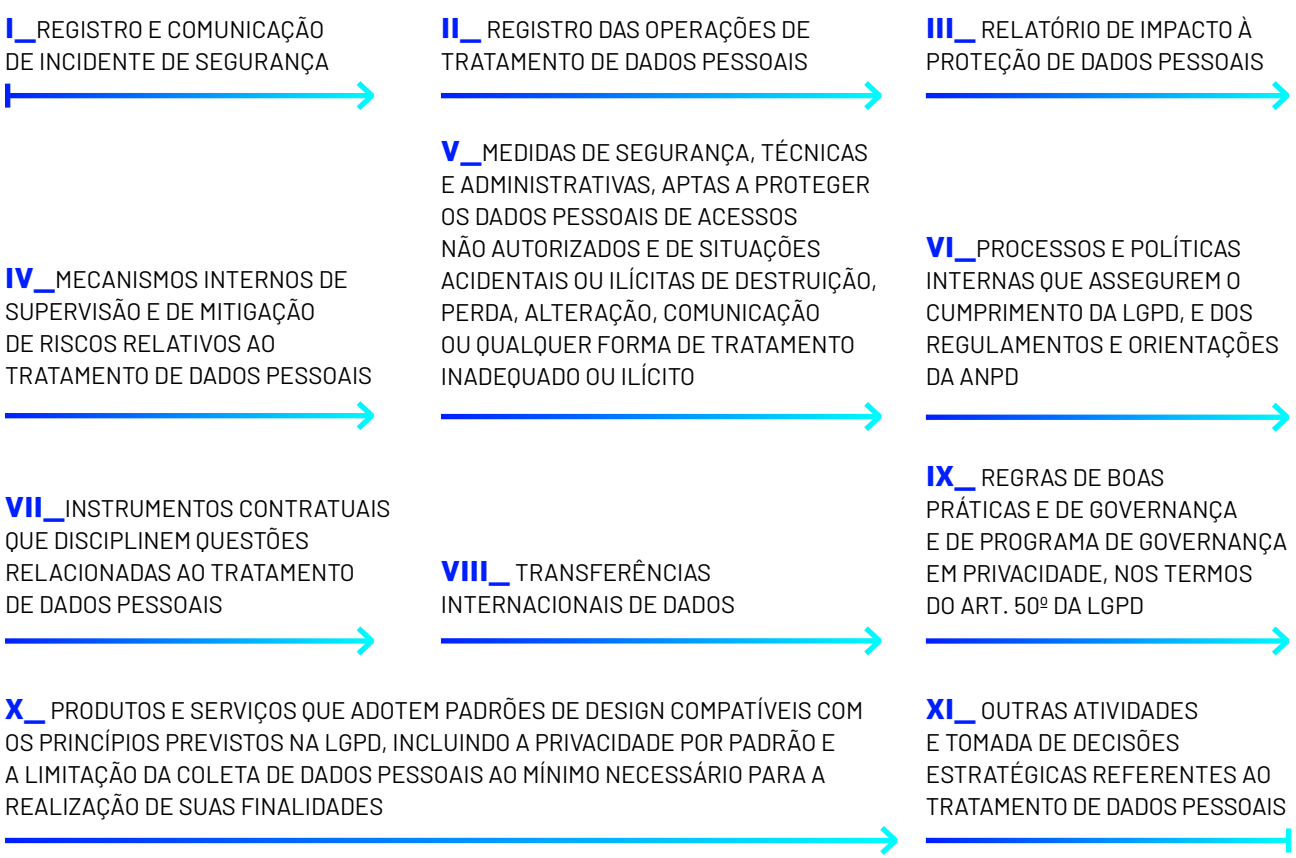
03_ Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

04_ Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Em complemento, a ANPD, por meio da **Resolução CD/ANPD nº 18**, definiu outras onze atividades que o Encarregado pode ser solicitado pela organização para elaborar, definir ou implementar:

Resolução CD/ANPD nº 18

FIGURA 7_ ATIVIDADES DO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS



Fonte: Autoridade Nacional de Proteção de Dados (2024d).

Para além das atribuições, a Resolução apresenta **requisitos de formação**, procedimentos para a **divulgação de identidade** e **informações de contato** do Encarregado e substituto, além de definir os deveres dos agentes de tratamento para evitar **situações de conflito de interesse**.

REQUISITOS DE FORMAÇÃO_ Embora ainda não exista uma formação obrigatória, capacitação ou certificação específica exigida para o desempenho da função de Encarregado dentro das organizações, é essencial que esse profissional tenha um sólido conhecimento da LGPD e de outras normas e legislações relacionadas à proteção de dados pessoais, bem como leis e regulamentações aplicáveis à realidade da organização.

Além disso, é desejável que o Encarregado possua conhecimentos em segurança da informação, especialmente na gestão de riscos e aplicação de controles, além de conhecimento sobre o negócio da instituição, uma vez que o Encarregado precisará interagir com todas as áreas ou setores para desempenhar sua função.

Vale dizer que a LGPD **não impõe restrições quanto ao Encarregado ser uma pessoa física ou jurídica**, permitindo que organizações também terceirizem a função a uma pessoa jurídica externa. Ao optar por essa modalidade, é importante verificar as mesmas exigências quanto ao conhecimento técnico adequado, ausência de conflito de interesses e possibilidade de integração e conhecimento da estrutura da organização.

CONFLITO DE INTERESSE_ *Outro ponto essencial na escolha do Encarregado é a prevenção de conflitos de interesse. O **DPO Handbook**, material de referência para a atuação de Data Protection Officers (DPOs) na União Europeia, destaca que o Encarregado deve atuar de forma independente e sem estar sujeito a influência indevida da organização. Isso significa que ele não pode ocupar uma posição que implique a definição de finalidades e meios de tratamento de dados, pois isso comprometeria sua capacidade de fiscalização e aconselhamento imparcial.*

ATENÇÃO!

Na administração pública federal direta, autárquica e fundacional, o Encarregado pelo tratamento de dados pessoais não deve estar lotado no setor de Tecnologia da Informação (TI) nem ser um gestor responsável por sistemas de informação, conforme a Instrução Normativa SGD/ME nº 117/2020.

Na prática, funções que possuem alto grau de poder decisório sobre o tratamento de dados – como Gestor de TI e Gestor de Segurança da Informação ou até mesmo posições de liderança em áreas como *Compliance* – podem gerar conflitos de interesse caso acumulem a função de Encarregado. A depender da estrutura organizacional, recomenda-se que o Encarregado esteja posicionado de forma a garantir **autonomia**, podendo atuar de maneira consultiva e supervisora, sem interferências de áreas que definem estratégias de tratamento de dados pessoais.

NOMEAÇÃO_ *A LGPD exige a nomeação e formalização do Encarregado. Essa designação deve ser feita por meio de um ato formal do agente de tratamento, que descreva as formas de atuação e as atividades a serem desempenhadas.*

Veja o exemplo do:

Laboratório Nacional de Computação Científica

ENCARREGADO SUBSTITUTO_ *É importante destacar que, em casos de ausência, impedimento ou vacância do Encarregado, a função deve ser exercida por um* ***substituto****, também formalmente designado. Em nenhuma circunstância o agente de tratamento pode criar obstáculos ao exercício dos direitos dos titulares ou ao atendimento das comunicações da ANPD.*

ATENÇÃO!

A ANPD recomenda que a formalização da designação do encarregado titular e de seu substituto ocorra de forma simultânea, conforme orientações apresentadas no:

Guia da Atuação do Encarregado pelo Tratamento de Dados Pessoais

ATENÇÃO!

O Encarregado deve ter acesso direto à alta administração para garantir a efetiva aplicação e supervisão das normas de proteção de dados, facilitando a implementação e a gestão do programa de privacidade. Essa conexão permite que decisões estratégicas sejam tomadas com rapidez e alinhadas às exigências legais, além de viabilizar a adoção de medidas corretivas e preventivas de forma eficiente. O envolvimento da alta administração também fortalece a autoridade do Encarregado, garantindo os recursos necessários para o cumprimento das diretrizes de privacidade.

ACESSE!

Os Artefatos nº 2 e nº 3 apresentam os modelos de ato formal para indicação de encarregado pessoa natural e pessoa jurídica, respectivamente, disponibilizados pela ANPD.

Artefatos nº 2

Artefatos nº 3

ATENÇÃO!

As pessoas jurídicas de direito público devem publicar a nomeação do Encarregado no Diário Oficial da União, do Estado, do Distrito Federal ou do Município, conforme a esfera de atuação do agente de tratamento.

IDENTIDADE E INFORMAÇÕES DE CONTATO_ *Para garantir transparência, a identidade e os contatos do Encarregado (e do substituto) devem ser amplamente divulgados, preferencialmente no site oficial da organização ou por outros meios de comunicação acessíveis aos titulares de dados.*

Veja exemplos de divulgação nos:

Site da Universidade Federal de Ouro Preto (UFOP)

Site do Ministério da Ciência, Tecnologia e Inovação (MCTI)

RESPONSABILIDADE DO ENCARREGADO_ *Apesar de todas os deveres que recaem sobre o papel do Encarregado, é importante ressaltar que o exercício de suas atividades e atribuições não o torna responsável, perante a ANPD, pela conformidade das ações de tratamento de dados realizadas pelo agente de tratamento.*

ATENÇÃO!

O responsável pela conformidade do tratamento de dados pessoais, conforme estabelecido pela LGPD, é o próprio agente de tratamento. O papel do Encarregado é atuar como um suporte, prestando assistência e orientação para garantir que as melhores práticas sejam seguidas.

1.8_ Quais documentos devem compor um programa de governança em privacidade?

A estrutura documental de um Programa de Governança em Privacidade permite a definição de diretrizes, responsabilidades e processos para o tratamento de dados pessoais.

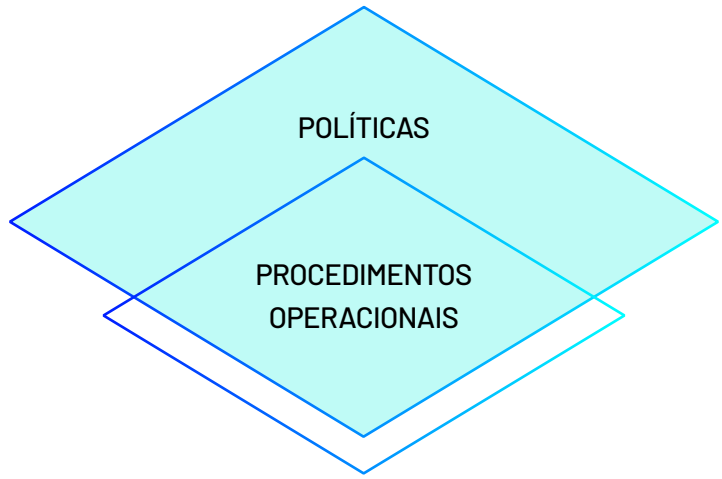
Nesse sentido, o artigo 50 § 2º, alíneas "a" "d" da LGPD expressamente menciona a importância de políticas e normas internas para implementação de programa de governança em privacidade:

> a) demonstre o comprometimento do controlador em **adotar processos e políticas internas** que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; [...] d) **estabeleça políticas e salvaguardas adequadas** com base em processo de avaliação sistemática de impactos e riscos à privacidade (Brasil, 2018, grifo nosso).

Nesse sentido, conforme abordado no livro *Privacy Program Management* (CIPM – IAPP), diferentes tipos de documentos podem compor essa estrutura, variando em nível de abrangência e detalhamento.

Sem prejuízo de adaptações considerando a realidade da organização, uma variação possível e comumente adotada é a divisão dos documentos relacionados ao PGP em camadas, conforme representação exemplificativa a seguir:

FIGURA 8_ DIVISÃO DOS DOCUMENTOS RELACIONADOS AO PGP



Fonte: elaboração própria.

Na representação acima, as **Políticas** ocupam papel estratégico de estabelecer diretrizes e objetivos gerais, definindo o escopo, fundamentos legais e responsabilidades, mas sem apresentar detalhes operacionais.

Os **Procedimentos**, por sua vez, ficam a cargo de especificar detalhes e ações operacionais necessários para implementar as diretrizes estabelecidas nas políticas.

Aplicando essa segmentação para o universo do Programa de Governança em Privacidade, é possível considerar que a Política Interna de Proteção de Dados Pessoais ocupa papel central no programa, estabelecendo as balizas principais para o tratamento de dados pessoais na instituição. Como exemplo, destaca-se a Política Interna de Proteção de Dados Pessoais da Autoridade Nacional de Proteção de Dados:

Disponível aqui

Além da Política Interna de Proteção de Dados Pessoais, outros documentos podem integrar a estrutura documental do Programa de Governança em Privacidade. Nesse contexto, destaca-se a Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que determina a implementação obrigatória de uma política de segurança da informação nos órgãos integrantes da Administração Pública Federal. Adicionalmente, é recomendável que o arcabouço documental contemple procedimentos operacionais destinados a orientar rotinas específicas relacionadas ao PGP, como, por exemplo, o atendimento a solicitações de titulares.

1.9_ Quais os requisitos mínimos de uma Política de Proteção de Dados Pessoais?

De partida, de forma a evitar confusões, é importante diferenciarmos a **política interna de privacidade** ou **política de proteção de dados** do instrumento de transparência comumente chamado de **aviso de privacidade**. Enquanto a **política interna de privacidade ou proteção de dados** estabelece as diretrizes e regras do programa de governança de privacidade da organização, definindo responsabilidades, controles e práticas para o tratamento de dados pessoais, o **aviso de privacidade**, regido pelo artigo 9º da LGPD, é um instrumento de transparência voltado ao público geral, geralmente disponibilizado em sites ou outros canais de comunicação (o **Módulo Transparência do Método RNP** aborda diretrizes sobre o aviso de privacidade).

Feita a diferenciação, passa-se a expor o conteúdo mínimo sugerido para uma política de proteção de dados e, nesse ponto, vale uma ressalva importante de que as informações relacionadas a seguir consideraram o repertório de conhecimento da RNP, bem como orientações contidas na publicação da IAPP, sabendo que estrutura documental de uma política pode variar consideravelmente de acordo com a realidade da organização, não havendo padrão único a ser seguido.

VISÃO E COMPROMISSO	*Declaração sobre a importância da privacidade e compromisso da organização com a proteção de dados pessoais.*
ESCOPO DE APLICAÇÃO	*Definição das áreas e gerências, processos e sistemas que estão cobertos pela política, incluindo terceiros envolvidos.*
DIRETRIZES GERAIS DE PRIVACIDADE	*Referência a princípios como necessidade, finalidade e transparência, bem como outras diretrizes gerais sobre o tema.*
PAPÉIS E RESPONSABILIDADES	*Descrição dos papéis e responsabilidades dos envolvidos na governança de privacidade e proteção de dados.*
REVISÃO E ATUALIZAÇÃO	*Critérios para atualização da política, incluindo frequência de revisão e adequações normativas.*

ATENÇÃO!

A Política Interna de Proteção de Dados deve ser amplamente divulgada e acessível a todos os servidores, colaboradores e terceiros vinculados à organização. Recomenda-se que o seu conteúdo e forma de acesso seja reforçado em programas de treinamento e conscientização.
Ela também deve ser revisada e atualizada regularmente, além de estar alinhada a outras diretrizes internas, como aquelas contidas em políticas de segurança da informação e *compliance*.

Considerando a importância deste documento e todos os aspectos necessários para seu desenvolvimento, apresentamos sugestões para auxiliar órgãos e entidades na elaboração de sua Política de Proteção de Dados Pessoais no âmbito institucional:

ACESSE!

No Artefato nº 4, disponibilizamos o Modelo de Política de Proteção de Dados Pessoais elaborado pela Secretaria de Governo Digital que contém os pré-requisitos mínimos para o documento.

Artefato nº 4

1.10_ O que é e qual a importância do Privacy by Design?

A privacidade desde a concepção, também conhecida como *Privacy by Design*, é um princípio que determina que a proteção da privacidade e dos dados pessoais deve ser considerada desde o início do desenvolvimento de qualquer serviço, produto ou processo de negócio.

As regras de governança, os controles de segurança e as medidas para garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais devem ser incorporados desde a fase de concepção, evitando que a privacidade seja tratada apenas como um ajuste posterior.

Além de atender às exigências regulatórias, essa abordagem fortalece a confiança dos titulares de dados, demonstra um compromisso real com a privacidade, reduz a probabilidade de incidentes de segurança e não conformidade, e representa uma medida essencial para uma efetiva gestão de riscos.

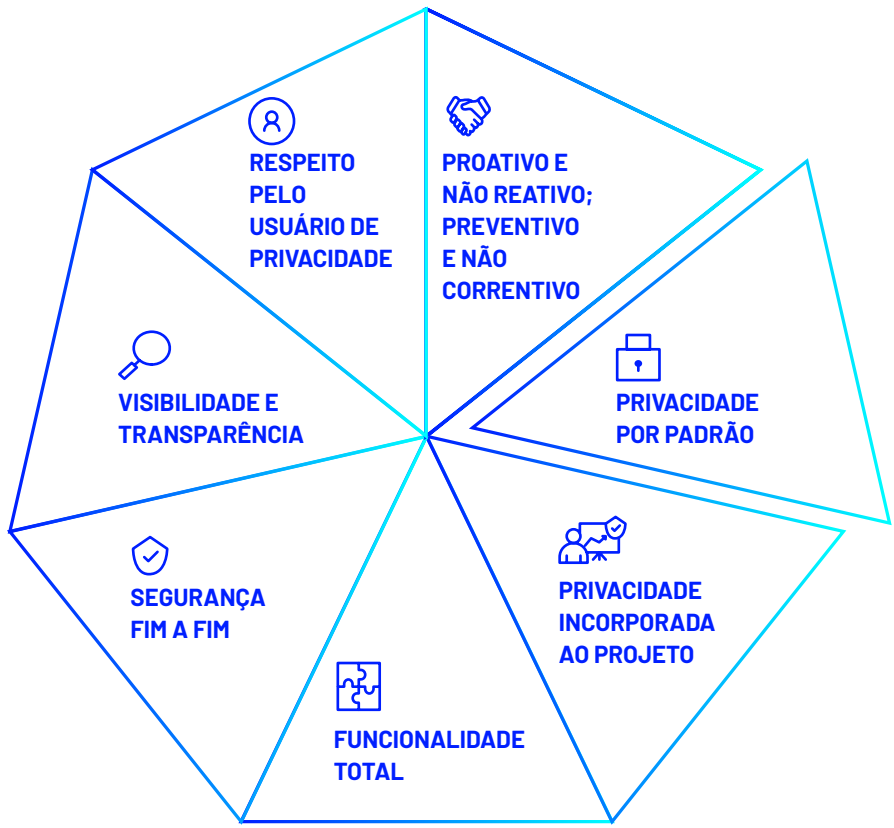
A LGPD, no **artigo 46, § 2º**, reforça a necessidade dessa abordagem ao estabelecer que os agentes de tratamento devem adotar medidas técnicas e administrativas de segurança "desde a fase de concepção do produto ou do serviço até a sua execução" (Brasil, 2018).

Esse requisito visa garantir que a proteção de dados seja uma prioridade estrutural, reduzindo riscos desde o planejamento até a implementação de qualquer iniciativa que envolva o tratamento de dados pessoais.

Implementar a privacidade desde a concepção implica considerar a proteção dos dados ao longo de todo o ciclo de vida das informações, desde a coleta até sua eliminação. Para isso, as organizações devem adotar práticas que limitem a coleta ao mínimo necessário, assegurem que os dados sejam utilizados apenas para finalidades legítimas e proporcionais e implementem mecanismos eficazes de segurança e governança.

Trata-se de uma metodologia baseada em sete princípios fundamentais de privacidade, desenvolvida na década de 1990 pela especialista canadense Ann Cavoukian (2010), que são:

FIGURA 9 _ SETE PRINCÍPIOS DA PRIVACIDADE DESDE A CONCEPÇÃO



Fonte: Cavoukian, [2010].

PROATIVO E NÃO REATIVO; PREVENTIVO E NÃO CORRETIVO_ *antecipar e evitar violações de privacidade antes que ocorram.*

PRIVACIDADE POR PADRÃO_ *garantir que a privacidade seja protegida por padrão, não dependendo de qualquer ação por parte do titular de dados.*

PRIVACIDADE INCORPORADA AO PROJETO_ *integrar a privacidade desde a concepção do projeto.*

FUNCIONALIDADE TOTAL_ *implementar medidas que protejam a privacidade sem diminuir ou prejudicar a funcionalidade pretendida do projeto, garantindo um equilíbrio entre os interesses e objetivos de todas as partes envolvidas.*

SEGURANÇA FIM A FIM_ *assegurar privacidade durante todo o ciclo de existência do projeto, desde a coleta até o descarte dos dados.*

VISIBILIDADE E TRANSPARÊNCIA_ *manter operações e práticas transparentes, garantindo que os dados pessoais sejam tratados conforme as informações fornecidas aos titulares.*

RESPEITO PELO USUÁRIO DE PRIVACIDADE_ *priorizar a experiência dos titulares de dados, colocando seus interesses em primeiro plano e fornecendo opções claras, acessíveis e fáceis de usar para a tomada de decisões.*

Esse conceito também está previsto na Resolução CD/ANPD nº 18, de 16 de julho de 2024, que determina que o encarregado de proteção de dados deve auxiliar na elaboração, definição e implementação de produtos e serviços que adotem padrões compatíveis com os princípios da LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados ao mínimo necessário.

ACESSE!

O Guia sobre Privacidade desde a Concepção e por Padrão, disponibilizado pela Secretaria de Governo Digital (SGD), oferece orientações detalhadas sobre a implementação destes procedimentos e pode ser utilizado como ferramenta auxiliar. De forma adicional, listamos alguns pontos relevantes a serem considerados:

01_ Envolver o Encarregado de Dados Pessoais e/ou equipe de privacidade desde a etapa inicial do desenvolvimento de produtos e serviços que estejam sendo desenvolvidos e que tratem dados pessoais;

02_ Garantir o atendimento, pelo sistema ou processo, aos requisitos de privacidade, como minimização da coleta de dados, definição de bases legais aplicáveis etc.;

03_ Identificar previamente riscos relacionados à privacidade do titular, com a adoção de medidas mitigatórias e documentação de justificativas para aceitação, com elaboração de RIPD quando aplicável;

04_ Restringir opções relacionadas à privacidade, como visualização de dados pessoais, configurações de compartilhamento, permissões e controles de acesso;

05_ Incorporar requisitos de privacidade ao desenho de produtos, serviços ou processos;

06_ Manter registros das medidas técnicas e administrativas, voltadas para a privacidade e proteção de dados, adotadas na concepção do produto ou serviço;

07_ Aplicar requisitos e controles de segurança da informação em todas as fases do produto, serviço ou processo, incluindo as fases de coleta, armazenamento, transmissão de dados etc.;

08_ Disponibilizar documentações e procedimentos de forma clara e transparente aos titulares em relação a todos os produtos, serviços ou processos que tratem seus dados;

09_ Realizar treinamentos periódicos de conscientização com relação ao privacy by design.

Ao integrar princípios de proteção de dados desde a concepção de processos, essa abordagem tende a fortalecer a confiança dos titulares e a resiliência da instituição a diante de desafios regulatórios e tecnológicos.

Dessa forma, ao priorizar a privacidade como um elemento central da governança corporativa, as organizações conseguem mitigar riscos, reduzir impactos de incidentes e promover uma cultura organizacional alinhada aos valores da proteção de dados de forma proativa e preventiva.

Guia sobre Privacidade desde a Concepção e por Padrão

1.11_ Como monitorar a maturidade do Programa de Governança em Privacidade?

Este tópico aborda a importância de possuir objetivos e métricas de avaliação para a evolução contínua do Programa de Governança em Privacidade.

A construção de métricas que permitam a medição de maturidade de um Programa de Governança em Privacidade é especialmente relevante não apenas para garantir a conformidade com a LGPD, mas também para assegurar que o programa evolua continuamente em resposta a novos posicionamentos e resoluções emitidos pela Autoridade Nacional de Proteção de Dados.
Essas métricas proporcionam uma visão objetiva do desempenho do programa e oportunidades de melhoria, verificação da eficácia das políticas implementadas e adaptação às novas exigências regulatórias. Assim, a governança de dados pessoais torna-se um processo dinâmico e sustentável.

Uma vez identificadas não conformidades, a organização deve adotar medidas corretivas para resolver os problemas. Isso pode envolver ajustes nos processos, treinamentos adicionais, a implementação de controles mais rigorosos, entre outras ações necessárias.

Para garantir a melhoria contínua, recomendam-se duas frentes: **desenvolvimento e acompanhamento de indicadores** e **condução de auditorias**.

O uso de indicadores adequados permite avaliar o desempenho e a eficácia das medidas implementadas para a conformidade com a LGPD. Monitorar esses indicadores regularmente ajuda a identificar áreas de melhoria e possibilita a implementação de ações corretivas ou preventivas conforme necessário.

Para apoiar a construção e a avaliação de indicadores, recomenda-se a adoção de *frameworks* de referência amplamente utilizados na governança de dados e privacidade.

Outros materiais de apoio podem ser consultados para essa finalidade. Um exemplo é o relatório ***Privacy Metrics for Accountability***, publicado pelo **Future of Privacy Forum (FPF)**, que apresenta métricas sugeridas de acordo com as principais rotinas de um programa de governança.

Privacy Metrics for Accountability

Com base nos módulos do Método RNP, a tabela a seguir representa indicadores que podem ser adotados para medir a efetividade do Programa de Governança em Privacidade:

TABELA 2_ INDICADORES PARA MEDIR A EFETIVIDADES DO PGP

MAPEAMENTO DE DADOS	*% de áreas/gerências mapeadas* *# quantidade de atividades de alto risco identificadas* *# tempo médio para conclusão do processo de atualização do inventário de dados*
GESTÃO DE RISCOS	*# quantidade de relatórios de impacto a proteção de dados elaborados* *# tempo médio para mitigação dos riscos identificados*
TRANSPARÊNCIA	*% de portais da instituição que contam com avisos de privacidade dedicados* *# quantidade de acessos ao aviso de privacidade ou portal de privacidade* *# quantidade de solicitações de direito de acesso recepcionadas*
GESTÃO DE TERCEIROS	*% de fornecedores submetidos ao processo de avaliação prévia* *% de fornecedores críticos auditados* *# tempo médio para avaliação de riscos de terceiros* *% de contratos com fornecedores que contam com cláusulas de privacidade*
ATENDIMENTO A TITULARES	*# quantidade de solicitações de titulares recepcionadas* *# tempo médio de resposta às requisições recepcionadas*
CONSCIENTIZAÇÃO E TREINAMENTO	*# quantidade de treinamentos aplicados* *% de áreas/gerências que participaram dos treinamentos* *# nota de desempenho de participantes em ações de engajamento pós treinamento*
MEDIDAS DE SEGURANÇA	*% de sistemas/aplicações submetidos a medidas técnicas de verificação* *# tempo médio para aplicação de medidas para correção de vulnerabilidades*
RESPOSTA A INCIDENTES	*% de incidentes de segurança reportados à ANPD* *# quantidade de ações de simulações preventivas realizadas*

Fonte: elaboração própria.

Recomenda-se que a organização revise periodicamente os tipos de métricas utilizadas, avaliando a possibilidade de ajustar os indicadores e até mesmo acrescentar novos, conforme o aumento da maturidade organizacional em privacidade e proteção de dados. É fundamental priorizar aqueles que possam impulsionar estrategicamente a eficácia da governança de dados pessoais.

FIGURA 10_ SUGESTÃO DE FLUXO DE GESTÃO DE INDICADORES

Fonte: elaboração própria.

A realização de auditorias, por sua vez, é crucial para avaliar a efetividade dos controles de segurança, a conformidade com as políticas e normas internas e a aderência às diretrizes da LGPD. As auditorias podem ser conduzidas internamente ou por auditores externos especializados. Essa avaliação sistemática auxilia na identificação de lacunas, falhas ou não conformidades, permitindo que a organização tome medidas corretivas e melhore continuamente seus processos e práticas.

Para fortalecer a abordagem das auditorias, sugere-se considerar:

AUDITORIAS INTERNAS_ *conduzidas pela equipe de governança e* compliance *da organização, permitindo ajustes mais ágeis em processos internos.*

AUDITORIAS EXTERNAS_ *realizadas por consultorias especializadas, trazendo uma visão isenta sobre riscos e oportunidades de melhoria.*

A combinação de indicadores e auditorias proporciona uma visão abrangente do status de conformidade com a LGPD, permitindo que a organização monitore seu desempenho, implemente melhorias contínuas e demonstre seu compromisso com a proteção dos dados pessoais. Além disso, a elaboração periódica de relatórios detalhados reforça a transparência institucional, identificando as ações realizadas, as pendências existentes e orientando as prioridades futuras para garantir uma gestão eficaz do Programa de Governança em Privacidade.

PPSI

O Método RNP foi desenvolvido com o objetivo de apoiar instituições no fortalecimento da governança e da gestão de conformidade para proteção de dados pessoais. Para reforçar sua aderência a práticas reconhecidas nacionalmente, cada módulo do Método RNP foi mapeado em relação aos controles previstos no Programa de Proteção à Segurança da Informação (PPSI), uma iniciativa estruturante da Secretaria de Governo Digital que orienta órgãos e entidades da Administração Pública Federal na implementação de medidas de segurança e proteção de dados. Confira a seguir os controles do PPSI abordados neste módulo:

TABELA 3_ COMPARATIVO ENTRE O MÓDULO GOVERNANÇA E O *FRAMEWORK* DO PPSI

CONTROLES DO PPSI	ID DE IDENTIFICAÇÃO
Controle 21_ *Governança*	*21.1; 21.2; 21.3; 21.4; 21.6; 21.7; 21.9; 21.10;*
Controle 22_ *Políticas, processos e procedimentos*	*22.2; 22.5; 22.8; 22.12;*
Controle 30_ *Avaliação de impacto, monitoramento e auditoria*	*30.9; 30.10; 30.11; 30.12;*

Fonte: elaboração própria.

MÓDULO MAPEAMENTO DE DADOS

Neste módulo você encontrará respostas para as seguintes perguntas:

2.1_ *Qual é o objetivo do mapeamento de dados?*

2.2_ *Como iniciar um mapeamento de dados?*

2.3_ *Qual é o passo a passo para o preenchimento do inventário de dados?*

2.4_ *Quais são os pontos de atenção no preenchimento do inventário de dados?*

2.5_ *O que fazer após finalização do inventário?*

Artefatos relacionados:

ARTEFATO Nº 5_ *Modelo de Inventário de Dados Pessoais do PPSI*

ARTEFATO Nº 6_ *Modelo de Registro das Operações de Tratamento de Dados Pessoais para Agentes de Tratamento de Pequeno Porte (ATPP) da ANPD*

ARTEFATO Nº 7_ *Sugestão de planilha para elaboração de planos de ação*

O mapeamento de dados é uma rotina essencial para compreensão e acompanhamento de como dados pessoais são tratados na organização. A execução dessa rotina permite identificar quais informações são coletadas, quem as acessa e por quais sistemas ou canais esses dados circulam, são processados e armazenados. Mapear os dados pessoais tratados pela organização é, portanto, passo de grande importância para que um PGP seja implementado e gerido.

Este módulo apresenta a forma de estruturação do mapeamento, desde a fase de diagnóstico até a atualização contínua do inventário de dados. Além disso, aborda a estruturação de planos de ação para mitigação de riscos de inconformidade.

2.1_ Qual é o objetivo do mapeamento de dados?

O mapeamento de dados é um compromisso contínuo que visa compreender e documentar, periodicamente, como a organização trata dados pessoais em suas atividades.

Além disso, executar rotina de mapeamento de dados contribui para o atendimento à exigência do **artigo 37º da LGPD**, que determina que controladores e operadores mantenham registro das operações de tratamento de dados pessoais que realizarem, assegurando maior controle e possibilitando a fiscalização por parte da ANPD.

ATENÇÃO!

É dever do controlador e operador manter registro das operações de tratamento de dados pessoais que realizarem. Assim, dado que as operações de tratamento de dados nas organizações estão em constante transformação, a rotina de mapeamento deve ser periodicamente executada, com o objetivo de refletir eventuais mudanças nas rotinas, garantindo que a documentação permaneça alinhada à realidade operacional.

2.2_ Como iniciar um mapeamento de dados?

Previamente ao início de uma rotina de constituição/atualização de inventário de dados, deve-se ter em mente que tal rotina pode ser conduzida de diversas formas, dependendo da estrutura e dos recursos disponíveis na organização.

Nesse sentido, é possível que essa rotina seja conduzida manualmente, por meio de entrevistas com gerências e áreas de negócio da instituição, do preenchimento de formulários e planilhas diretamente por essas unidades ou, de forma automatizada, por meio de sistemas especializados, também conhecidos como *Data Discovery*.

FIGURA 11_ POSSÍVEIS FORMAS DE CONDUZIR UM MAPEAMENTO DE DADOS

Fonte: elaboração própria.

Definido o método a ser adotado, em qualquer caso recomenda-se uma avaliação segmentada entre as áreas da organização, ainda que de forma concomitante, o que permite uma análise mais detalhada e precisa das práticas de tratamento de dados em cada equipe, garantindo que os riscos específicos e as necessidades de conformidade sejam identificados e tratados com maior precisão, além de facilitar a implementação de medidas corretivas e monitoramento contínuo.

2.3_ Qual o passo a passo para o preenchimento do inventário de dados?

ACESSE!

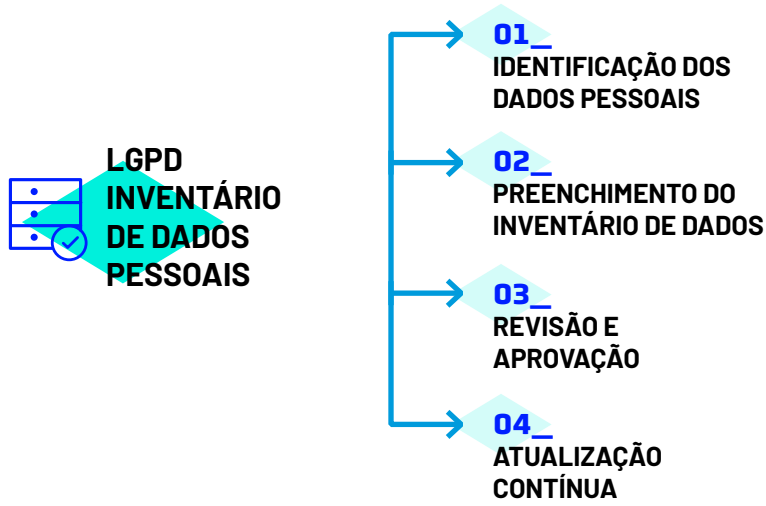
Com o objetivo de auxiliar no processo de elaboração do inventário de dados pessoais, a Secretaria de Governo Digital (SGD) publicou modelo de Inventário de Dados Pessoais, disponível em nosso Artefato nº 5, especialmente recomendado e direcionado aos órgãos e entidades da Administração Pública Federal (APF). Por sua vez, a ANPD disponibilizou o Modelo de Registro das Operações de Tratamento de Dados Pessoais para Agentes de Tratamento de Pequeno Porte (ATPP), acessível no Artefato nº 6. O documento possui abordagem simplificada e deve ser adaptado às particularidades de cada organização.

Artefato nº 5

Artefato nº 6

Com base no modelo da SGD e visando simplificar e padronizar essa atividade, o Supremo Tribunal Federal (STF) também publicou o **Guia de Elaboração de Inventário de Dados**, dispondo as seguintes etapas:

FIGURA 12_ ETAPAS DA ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS



Fonte: Brasil (2024b, p.7).

As quatro etapas apresentadas pelo STF para a elaboração do inventário de dados consistem em:

01_ Identificação dos dados pessoais: elaboração de uma lista detalhada dos serviços ou processos de negócio que envolvem o tratamento de dados pessoais.

02_ Preenchimento do Inventário de dados: catalogação de informações essenciais sobre cada atividade de tratamento de dados realizada pela organização, incluindo categorias de dados, finalidades e bases legais.

03_ Revisão e aprovação: revisões correções e complementações são feitos, se necessário, para garantir a precisão e integralidade do documento.

04_ Atualização contínua: reconhecendo a natureza dinâmica das operações de tratamento de dados, há o monitoramento e atualização regular do inventário, mantendo-o em conformidade com mudanças *nos processos e na legislação.*

Seguindo estas etapas, feita a identificação dos serviços, processos e atividades com o envolvimento de dados pessoais, é o momento de preencher o inventário, que deverá conter, no mínimo, as seguintes informações:

01_ Descrição detalhada da atividade, ou seja, apresentação de detalhes sobre como a atividade de tratamento de dados é realizada, fornecendo descrição sobre a forma de coleta dos dados e eventuais interações com o titular de dados.

02_ Dados pessoais tratados, ou seja, qualquer informação que identifique ou possa identificar uma pessoa, como nome, número de documentos oficiais, data de nascimento e endereço.

03_ Dados pessoais sensíveis tratados, se aplicável, como dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico;

04_ Categorias de titulares, ou seja, sobre quem são os dados envolvidos na atividade;

05_ Finalidade do tratamento, isto é, a razão pela qual a atividade existe.

06_ Base legal aplicável ao tratamento, em outras palavras, a hipótese legal que autoriza o tratamento de dados na atividade (o Método RNP apresenta as bases legais previstas na LGPD no item 2.4. a seguir).

07_ Forma de coleta dos dados pessoais, quer dizer, se obtidos diretamente do próprio titular, se recebidos de um terceiro, de alguma base pública etc.;

08_ Existência de compartilhamento dos dados pessoais tratados na atividade;

09_ Terceiros envolvidos, seja o recebedor dos dados eventualmente compartilhados, seja algum fornecedor que oferte determinado serviço essencial para as tratativas da atividade envolvendo dados pessoais;

10_ Existência de transferência internacional de dados pessoais; conforme abordado no item 2.4 "3" do Método;

11_ País de destino dos dados pessoais, se aplicável;

12_ Mecanismo de transferência internacional de dados, se aplicável;

13_ Período de retenção dos dados e formas de descarte, se houver;

14_ Local de armazenamento dos dados pessoais; e

15_ Medidas de segurança aplicadas para proteção dos dados pessoais.

Alguns dos itens descritos são autoexplicativos e de intuitivo preenchimento, pois refletem diretamente as características da atividade, sem exigir uma interpretação jurídica complexa. No entanto, outros exigem maior atenção, pois envolvem aspectos legais que requerem uma análise tanto contextual quanto técnica, os quais serão detalhados no próximo tópico.

2.4_ Quais são os pontos de atenção no preenchimento do inventário de dados?

HIPÓTESES LEGAIS

Dentre os aspectos essenciais, é importante compreender, inicialmente, que cada atividade de tratamento de dados deve estar respaldada por uma **hipótese legal** apropriada, garantindo que o tratamento ocorra em conformidade com os requisitos da LGPD.

As **bases legais** são as hipóteses previstas no **artigo 7º da LGPD** e, no caso de dados pessoais sensíveis, no **artigo 11º**, que funcionam como justificativas legais para o tratamento de dados pessoais por uma organização.

TABELA 4_ HIPÓTESES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS (ART. 7º, LGPD):	BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS (ART. 11º, LGPD):
Consentimento;	*Consentimento específico e destacado;*
Cumprimento de obrigação legal ou regulatória;	*Cumprimento de obrigação legal ou regulatória;*
Execução de políticas públicas previstas em leis e regulamentos ou respaldadas por contratos, convênios ou similares;	*Execução de políticas públicas previstas em leis ou regulamentos;*
Realização de estudos por órgãos de pesquisa;	*Realização de estudos por órgãos de pesquisa;*
Execução de contrato ou procedimentos preliminares;	*N/A*
Exercício regular de direitos em processo judicial, administrativo ou arbitral;	*Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;*
Proteção da vida ou da incolumidade física;	*Proteção da vida ou da incolumidade física;*
Tutela da saúde;	*Tutela da saúde;*
Interesse legítimo;	*N/A*
Proteção do crédito;	*N/A*
N/A	*Prevenção à fraude e à segurança do titular.*

Fonte: Brasil (2018).

Cada atividade de tratamento, portanto, deve estar vinculada a uma dessas bases, sempre em alinhamento com sua finalidade específica. Além disso, algumas bases podem ter particularidades que exigem atenção, especialmente no caso do tratamento de dados realizado pelo Poder Público.

ACESSE!

Para uma definição das bases legais aplicáveis, recomenda-se a consulta ao Guia Orientativo: Tratamento de Dados Pessoais pelo Poder Público, publicado pela ANPD, que fornece orientações sobre as bases legais e os princípios que devem guiar o tratamento de dados pessoais por entidades e órgãos públicos. Ainda, sugere-se a leitura da Cartilha sobre Finalidade e Hipóteses Legais, elaborada pelo Programa de Privacidade e Segurança da Informação (PPSI).

Guia Orientativo: Tratamento de Dados Pessoais pelo Poder Público

Cartilha sobre Finalidade e Hipóteses Legais

Algumas bases legais merecem destaque no tratamento de dados pessoais pelo Poder Público, e serão abordadas de forma mais aprofundada a seguir.

Quando o tratamento se baseia no consentimento, é imprescindível obter a autorização livre, informada e inequívoca do titular antes do início do processamento dos dados, conforme definido pela LGPD. No caso de dados sensíveis, o consentimento ainda deve ser fornecido de forma específica e destacada pelo titular.

Nesse sentido, o consentimento deve ser voluntário e deliberado, representando uma escolha legítima do titular para o tratamento de dados para determinado fim, que pode a qualquer momento ser revogada (**artigo 8º, §5º da LGPD**). Por essa razão, essa base legal exige que as organizações estejam preparadas para gerenciar consentimentos e atender prontamente às eventuais solicitações de revogações.

Uma observação trazida no Guia Orientativo: Tratamento de Dados Pessoais pelo Poder Público é de que a escolha pela base legal do consentimento pelo Poder Público somente pode ocorrer quando o uso dos dados não for obrigatório, e quando o Estado não estiver diante de seus poderes típicos, derivados de obrigações e atribuições legais, em que há um desbalanceamento de forças entre o Estado e o titular. Isto porque, nestes casos, haveria um vício de consentimento, considerando o caráter compulsório do tratamento de dados a ser realizado.

A mesma recomendação é dada com relação à base legal do **legítimo interesse**, que, por sua vez, exige a realização de um teste de balanceamento prévio, uma avaliação que verifica se o interesse do controlador ou de terceiros é legítimo e se não se sobrepõe aos direitos e liberdades fundamentais dos titulares (**artigo 10º da LGPD**). O Guia explica que quando houver um tratamento compulsório pelo Estado, quando este estiver em cumprimento de suas obrigações legais, não seria possível ponderar os supostos interesses estatais com os do titular, sendo mais recomendável o uso de outras bases legais.

Contudo, não havendo tratamento compulsório associado a prerrogativas Estatais típicas, o uso do **legítimo interesse** poderá ser possível, desde que com o devido balanceamento prévio e desde que sem o envolvimento de dados pessoais sensíveis.

ACESSE!

Para orientar a aplicação da hipótese de legítimo interesse, recomenda-se consultar o tópico Teste de Balanceamento do Guia Orientativo: Hipóteses Legais de Tratamento de Dados Pessoais - Legítimo Interesse, publicado pela ANPD.

Guia Orientativo: Hipóteses Legais de Tratamento de Dados Pessoais - Legítimo Interesse

A base legal de **cumprimento de obrigação legal ou regulatória**, por sua vez, também é relevante no contexto do Poder Público e está diretamente relacionada ao **artigo 23º da LGPD**. Esse artigo estabelece que o tratamento de dados pessoais por órgãos e entidades públicas deve ocorrer para executar suas competências legais ou cumprir atribuições do serviço público, sempre observando o interesse público e a finalidade específica da atividade.

Dessa forma, a base legal de **obrigação legal ou regulatória** justifica o tratamento de dados sempre quando alinhada às funções institucionais do órgão, necessária e proporcional à prestação do serviço público, podendo ser forte aliada do Poder Público no tratamento de dados pessoais.

Ainda, especial atenção deve ser dada à base legal de **realização de estudos por órgãos de pesquisa**, especialmente se considerado que, de acordo com a própria LGPD, os órgãos de pesquisa são "**órgão ou entidade da administração pública direta ou indireta** ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, **que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico**" (Brasil, 2018, art. 5º, grifo nosso).

Ou seja, no contexto de instituições de ensino públicas que possuam como missão institucional a promoção da pesquisa, esta base legal poderá ser aplicada, desde que adotadas as medidas de segurança necessárias, como a anonimização.

ACESSE!

Para mais informações, a ANPD disponibilizou:

Guia Orientativo sobre o Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas

Quanto à base legal de **tutela da saúde**, conforme as diretrizes da Autoridade Nacional de Proteção de Dados (ANPD) sobre as hipóteses legais de tratamento de dados pessoais, quando um órgão público realiza o tratamento desses dados com base na hipótese de tutela da saúde, ele deve restringir esse tratamento exclusivamente a profissionais de saúde, serviços de saúde ou autoridades sanitárias.

Essa medida visa assegurar que informações sensíveis sejam manejadas apenas por agentes devidamente autorizados e capacitados, garantindo a confidencialidade e a segurança necessárias no contexto da saúde pública.

Por fim, ainda que existam outras bases legais que justifiquem o tratamento de dados pelo Poder Público, também é relevante dar destaque para o tratamento e compartilhamento de dados pela administração pública para a **execução de políticas públicas**.

A administração pública, nesse contexto, de acordo com o Guia da ANPD citado neste tópico, abrange órgãos dos três Poderes, incluindo Cortes de Contas e Ministério Público, quando atuam em funções administrativas. Já políticas públicas, de acordo com esse Guia, são programas ou ações governamentais formalmente instituídos por lei, regulamento ou ajuste contratual, embora, no caso de dados sensíveis, a base legal seja mais restrita, permitindo o tratamento apenas para políticas previstas em leis e regulamentos.

Em qualquer situação, o tratamento de dados também deve seguir o artigo 23º da LGPD, garantindo que ocorra para fins legítimos e no interesse público.

COMPARTILHAMENTO DE DADOS PESSOAIS

Outro ponto relevante, especialmente para órgãos públicos, é o **compartilhamento de dados pessoais**.

Isso porque a LGPD exige maior cautela destes entes, com o objetivo de garantir que esse processo ocorra **apenas para o atendimento de finalidades públicas** e com a devida **transparência**, conforme exigido pelos **artigos 26º e 27º da LGPD**.

O compartilhamento entre entidades públicas deve respeitar princípios como **necessidade, adequação e segurança**, além de ser realizado **exclusivamente para o cumprimento de políticas públicas ou atribuições legais**. Já o compartilhamento com **entidades privadas** é permitido apenas em hipóteses específicas. Essas regras visam evitar o uso indevido dos dados e proteger os direitos dos titulares.

Nesse sentido, o **Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público** publicado pela ANPD aborda as especificidades do compartilhamento de dados pessoais entre órgãos públicos e apresentou um resumo de recomendações essenciais, as quais estão ilustradas abaixo.

Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público

FIGURA 13 _ USO COMPARTILHADO DE DADOS PESSOAIS PELO PODER PÚBLICO

REQUISITO	RECOMENDAÇÃO
FORMALIZAÇÃO E REGISTRO	> Instauração de processo administrativo; > Análise técnica e jurídica; > Decisão administrativa ou celebração de contrato, convênio ou instrumento congênere; > Edição de ato normativo interno.
OBJETO E FINALIDADE	> Descrição dos dados pessoais de forma objetiva e detalhada; > Indicação de finalidade específica; > Avaliação da compatibilidade entre a finalidade original e a finalidade do compartilhamento.
BASE LEGAL	> Indicação da base legal utilizada.
DURAÇÃO DO TRATAMENTO	> Definição do período (duração) do uso compartilhado dos dados, de forma fundamentada, e esclarecimento sobre a possibilidade de conservação ou a necessidade de eliminação após o término do tratamento.
TRANSPARÊNCIA E DIREITOS DOS TITULARES	> Divulgação das informações pertinentes na página eletrônica dos órgãos e das entidades responsáveis; > Divulgação de maneira que as informações sobre dados pessoais tratados pela entidade sejam de fácil compreensão; > Definição de responsabilidades e de procedimentos relativos ao atendimento de solicitações de titulares.
PREVENÇÃO E SEGURANÇA	> Descrição das medidas técnicas e administrativas adotadas para proteger os dados pessoais de incidentes de segurança.
OUTROS REQUISITOS (AVALIAÇÃO CONFORME O CASO CONCRETO)	> Autorização ou vedação para novo compartilhamento ou transferência posterior dos dados pessoais; > Ônus financeiro; > Requisitos específicos para compartilhamento de dados pessoais com entidades privadas (art. 26º, §1º e art. 27º, LGPD); > Elaboração de relatório de impacto à proteção de dados pessoais, caso necessário; > Identificar as funções e responsabilidades dos agentes de tratamento.

Fonte: Autoridade Nacional de Proteção de Dados (2023b, p. 49).

TRANSFERÊNCIA INTERNACIONAL DE DADOS

Ainda com o intuito de esclarecer os tópicos do inventário que exigem uma análise mais técnica, é essencial abordar a **Transferência Internacional de Dados**, prevista nos **artigos 33º a 36º da LGPD** e regulamentada pela **Resolução CD/ANPD nº 19/2024**, que nada mais é do que a transferência de dados pessoais tratados no Brasil para país estrangeiro ou organismo internacional do qual o Brasil seja membro, independentemente do meio utilizado para essa transferência.

A Transferência Internacional de Dados é prevista de forma expressa na LGPD, e Resolução CD/ANPD nº 19/2024, ao regulamentar os **artigos 33º a 36º da Lei**, estabeleceu procedimentos e regras aplicáveis às operações de Transferência Internacional de Dados, bem como mecanismos válidos autorizadores dessas transferências, como:

01_ Transferências para países e organismos internacionais com grau de proteção de dados pessoais reconhecido como adequado pela ANPD, permitindo que a transferência ocorra de forma célere e simplificada.

02_ Quando o controlador oferece e comprova garantias de conformidade com a LGPD por meio de: cláusulas contratuais específicas para a transferência, cláusulas-padrão contratuais aprovadas pela ANPD ou normas corporativas globais, que garantem o cumprimento das exigências de proteção.

Identificar processos e atividades que envolva transferência internacional de dados é essencial para estabelecer o mecanismo autorizador específico para cada caso e uma base legal específica para justificar a transferência, o que deverá ser registrado no inventário de dados com o objetivo de documentar e fortalecer a governança dos dados.

Veja a página disponibilizada pela ANPD sobre **Transferência Internacional de Dados**. Esse recurso busca garantir maior transparência e auxiliar empresas e cidadãos no entendimento dos mecanismos que regulam a movimentação de dados pessoais para fora do Brasil.

Transferência Internacional de Dados

RETENÇÃO E DESCARTE DE DADOS PESSOAIS

A LGPD, nos **artigos 15º e 16º**, estabeleceu também as condições para o término do tratamento de dados pessoais, especificando quando e como esse processo deve ocorrer para garantir a proteção dos direitos dos titulares, e evidenciando a importância da definição de um **prazo de retenção e descarte** dos dados pessoais tratados pela organização.

A eliminação representa a **etapa final do ciclo de vida dos dados**, em que os dados pessoais são removidos dos sistemas da organização quando não são mais necessários para as finalidades originais ou mediante solicitação do titular. É fundamental definir e documentar os prazos de retenção dos dados pessoais, assegurando que a exclusão seja realizada de forma adequada e segura.

Conforme orienta o **Programa de Privacidade e Segurança da Informação (PPSI)**, as organizações devem:

01_ Implementar procedimentos para o término do tratamento: garantir que o encerramento do tratamento dos dados pessoais do titular siga as hipóteses previstas no artigo 15º da LGPD.

02_ Estabelecer técnicas de exclusão segura: utilizar métodos adequados para a exclusão ou destruição segura dos dados pessoais, incluindo originais, cópias e registros arquivados, de forma a impedir sua recuperação.

03_ Avaliar a necessidade de retenção: *manter os dados pessoais apenas pelo tempo estritamente necessário para cumprir as finalidades de tratamento inicialmente identificadas.*

04_ Implementar detecção de expiração do período de retenção: configurar sistemas para identificar a expiração dos prazos de retenção, com avisos automáticos para avaliar a possibilidade de exclusão dos dados após o cumprimento das finalidades.

05_ Bloquear dados para retenção legal: quando os propósitos informados ao titular forem atingidos, mas a retenção for exigida por leis aplicáveis, adotar medidas de proteção para isentar esses dados de processamento adicional.

06_ Descarte seguro de materiais impressos: garantir que todos os materiais impressos contendo dados pessoais sejam descartados de forma segura, evitando qualquer exposição ou recuperação não autorizada.

Essas práticas asseguram que a organização gerencie o ciclo de vida dos dados de maneira eficaz, protegendo a privacidade dos titulares e atendendo aos requisitos legais de segurança da informação.

Programa de Privacidade e Segurança da Informação (PPSI)

2.5_ O que fazer após finalização do inventário?

Com o registro detalhado das atividades e processos no inventário, abrangendo todos os tópicos já abordados em itens anteriores, a fase **pós inventário** materializa o principal objetivo do mapeamento: assegurar e manter a conformidade da organização com a Lei Geral de Proteção de Dados Pessoais regularmente.

Nesse contexto, após a conclusão do inventário, é essencial analisá-lo para identificar possíveis riscos, definir medidas de mitigação e estabelecer um planejamento para uma atualização contínua, consultar o **Módulo Gestão de Riscos**.

A elaboração de planos de ação pode ser um recurso complementar ao inventário, responsável por estruturar de forma clara as atividades necessárias para corrigir inconformidades e aprimorar a governança de dados, garantindo que a organização esteja sempre alinhada às exigências regulatórias, inclusive às iniciativas delineadas no Programa de Privacidade e Segurança da Informação (PPSI).

ACESSE!

Para a elaboração de planos de ação, o Artefato nº 7 disponibiliza uma sugestão de planilha, a ser preenchida de acordo com as particularidades de cada organização, desenvolvida com base nos questionamentos feitos pelo Tribunal de Contas da União, conforme o Acórdão nº 1384/2022 – TCU, que aborda o levantamento da implementação da LGPD na Administração Pública Federal.

Artefato nº 7

PPSI

O Método RNP foi desenvolvido com o objetivo de apoiar instituições no fortalecimento da governança e da gestão de conformidade para proteção de dados pessoais. Para reforçar sua aderência a práticas reconhecidas nacionalmente, cada módulo do Método RNP foi mapeado em relação aos controles previstos no Programa de Proteção à Segurança da Informação (PPSI), uma iniciativa estruturante da Secretaria de Governo Digital que orienta órgãos e entidades da Administração Pública Federal na implementação de medidas de segurança e proteção de dados. Confira a seguir os controles do PPSI abordados neste módulo:

TABELA 5_ COMPARATIVO ENTRE O MÓDULO MAPEAMENTO DE DADOS E O *FRAMEWORK* DO PPSI

CONTROLES DO PPSI	ID DE IDENTIFICAÇÃO
Controle 19_ *Inventário e Mapeamento*	*19.1; 19.2; 19.3; 19.4; 19.5; 19.6; 19.7; 19.8; 19.9; 19.10; 19.11; 19.12; 19.13; 19.14*
Controle 20_*Finalidade e Legitimidade*	*20.6; 20.9*
Controle 22_*Políticas, processos e procedimentos*	*22.9*
Controle 25_ *Gestão do tratamento*	*25.5; 25.6; 25.7; 25.8*
Controle 27_ *Compartilhamento, transferência e divulgação*	*27.1; 27.2; 27.5*
Controle 30_ *Avaliação de impacto, monitoramento e auditoria*	*30.8*

Fonte: elaboração própria.

MÓDULO GESTÃO DE RISCOS

Neste módulo você encontrará respostas para as seguintes perguntas:

3.1_ *Como estruturar uma gestão de riscos?*

3.2_ *Como e quando elaborar um Relatório de Impacto à Proteção de Dados Pessoais?*

Artefatos relacionados:

ARTEFATO Nº 8_ *Sugestão de planilha para mapeamento de riscos*

ARTEFATO Nº 9_ *Guia/Modelo de Elaboração de RIPD do PPSI*

A gestão de riscos é um componente essencial para assegurar a conformidade com a Lei Geral de Proteção de Dados Pessoais e a proteção efetiva dos direitos dos titulares. Não à toa, o **artigo 50º da LGPD** incentiva a implementação de programas de governança em privacidade que estabeleçam regras de boas práticas e mecanismos para identificar, avaliar e mitigar riscos relacionados ao tratamento de dados pessoais.

Esse processo exige uma análise cuidadosa de diversos fatores, como a natureza dos dados tratados, seu escopo, a finalidade do tratamento e a probabilidade de ocorrência de riscos, sempre considerando a gravidade dos impactos potenciais para os titulares e para a própria organização.

Nesse sentido, o controlador deve conduzir uma análise detalhada, considerando possíveis riscos de segurança e proteção dos dados, riscos à privacidade do titular, e riscos organizacionais relacionados à não conformidade com a legislação.

O **artigo 6º, inciso VII, da LGPD** reforça a necessidade de adoção de medidas de segurança, exigindo a proteção dos dados contra acessos não autorizados, além de situações acidentais ou ilícitas que possam resultar em destruição, perda, alteração, comunicação ou difusão indevida.

O **artigo 44º da LGPD** estabelece que qualquer tratamento de dados será considerado irregular se não observar a legislação ou não oferecer um nível adequado de segurança, levando em conta o modo como o tratamento é realizado, os riscos envolvidos e as técnicas utilizadas.

3.1_ Como estruturar uma gestão de riscos?

Para estruturar a gestão de riscos dentro do programa de privacidade, o primeiro passo é a **identificação dos riscos** específicos relacionados aos processo/atividades contidos no inventário de tratamento de dados (Módulo Mapeamento de Dados do Método RNP).

Assim, ao analisar as atividades mapeadas, é fundamental avaliar se estas estão de acordo com os princípios da LGPD, avaliando, por exemplo, se a coleta de dados possui uma **finalidade legítima** e claramente definida, se há **proporcionalidade** no tratamento ou se a organização está processando **dados desnecessários** ou de maneira excessiva. Além disso, deve-se verificar se há **compartilhamento desnecessário** de informações, bem como analisar vulnerabilidades nos sistemas que possam comprometer a confidencialidade, a integridade ou a disponibilidade das informações.

Após essa identificação inicial, a organização pode **definir medidas de mitigação adequadas**, como o fortalecimento dos controles de acesso, a adoção de políticas de minimização e retenção de dados e a implementação de mecanismos de segurança mais robustos.

ATENÇÃO!

A minimização de dados deve ser um critério fundamental em todas as etapas do tratamento de informações, abrangendo desde a coleta até o gerenciamento de acessos. O tratamento deve se limitar ao estritamente necessário para atingir a finalidade pretendida, evitando a captação excessiva ou desproporcional de dados pessoais. Além disso, o controle de acesso deve seguir o princípio do *need to know*, garantindo que apenas usuários com justificativa específica tenham permissão para acessar determinadas informações, reduzindo a exposição indevida e mitigando riscos de uso inadequado.

ATENÇÃO!

A exatidão, relevância e integridade dos dados pessoais devem ser asseguradas em todas as etapas do tratamento, especialmente no momento da coleta. A organização deve adotar mecanismos que reduzam a incidência de informações imprecisas, desatualizadas ou irrelevantes, garantindo que os dados armazenados sejam adequados à finalidade específica para a qual foram coletados.

A gestão de riscos não deve ser vista como uma atividade isolada, mas sim como um processo contínuo que exige **monitoramento e revisão periódica**. À medida que o cenário regulatório e tecnológico evolui, bem como que as próprias atividades mapeadas passem por alterações, é essencial revisar a análise de riscos e reavaliar as medidas adotadas para garantir sua eficácia.

ACESSE!

Para facilitar a análise de cada tratamento de dados, elaboramos planilha para mapeamento de riscos, disponível em nosso Artefato nº 8. Para cada risco identificado, é essencial documentar a resposta planejada ou, nos casos de aceitação do risco, incluir uma justificativa detalhada.

Artefato nº 8

3.2_ Como e quando elaborar um Relatório de Impacto à Proteção de Dados Pessoais?

Conforme mencionado, um aspecto fundamental da gestão de riscos é a identificação, dentro de cada atividade de tratamento de dados mapeada pela organização, daquelas que apresentam potenciais riscos que precisam ser mitigados.

Em alguns casos, além da implementação de estratégias específicas para mitigação de riscos, pode ser necessária a elaboração de um **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. Esse documento tem a função de detalhar as medidas, salvaguardas e mecanismos adotados para reduzir os riscos associados a determinadas atividades de tratamento de dados pessoais que possam comprometer os direitos fundamentais e as liberdades civis dos titulares.

A exigência do RIPD é particularmente relevante para atividades classificadas como de "alto risco", conforme critérios estabelecidos pela Autoridade Nacional de Proteção de Dados (ANPD), e para agentes do Poder Público, que possuem, de acordo com a LGPD, a recomendação inclusive de publicação de eventuais RIPDs (**artigo 32º**).

É relevante destacar que a **recomendação da ANPD** é de que o RIPD seja sempre elaborado **antes** de o controlador iniciar o tratamento de dados pessoais, justamente para servir como uma orientação com relação aos possíveis riscos, as salvaguardas e mecanismos de mitigação apropriados.

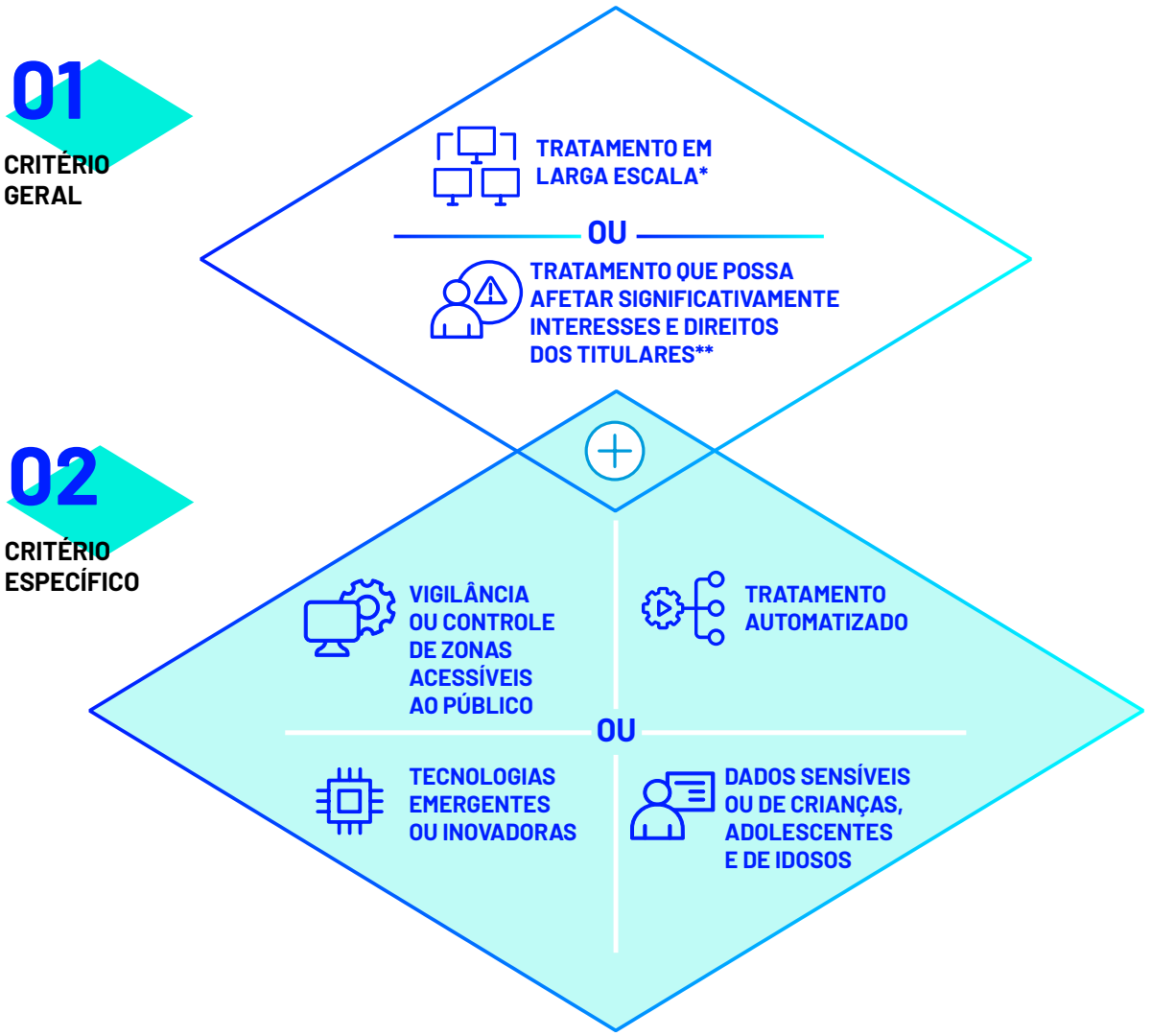
Recomendação da ANPD

Para definição mais clara do que seria considerado uma atividade de "alto risco", os controladores podem adotar como referência o conceito estabelecido no **artigo 4º** do Regulamento de Aplicação da LGPD para Agentes de Tratamento de Pequeno Porte, aprovado pela Resolução nº 2/2022.

Regulamento de Aplicação da LGPD para Agentes de Tratamento de Pequeno Porte

Conforme a previsão, o tratamento é considerado de alto risco ao atender, pelo menos, a um critério geral ("larga escala" ou "afetar significativamente interesses e direitos fundamentais dos titulares") e um critério específico ("uso de tecnologias emergentes ou inovadoras", "vigilância ou controle de zonas acessíveis ao público", "decisões tomadas exclusivamente com base em tratamento automatizado de dados pessoais", ou "uso de dados pessoais sensíveis ou de dados pessoais de crianças, adolescentes e idosos"), conforme ilustrado a seguir:

FIGURA 14_ TRATAMENTO DE ALTO RISCO



*** LARGA ESCALA**

Quando o tratamento abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.

**** AFETAR SIGNIFICATIVAMENTE INTERESSES E DIREITOS**

Quando o tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

Fonte: Autoridade Nacional de Proteção de Dados (2023c).

ACESSE!

Para obter mais informações sobre o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), a ANPD disponibiliza em seu site uma seção de perguntas e respostas para auxílio, que, inclusive, traz o fluxograma a seguir para refletir os pontos recomendáveis para a elaboração do RIPD.

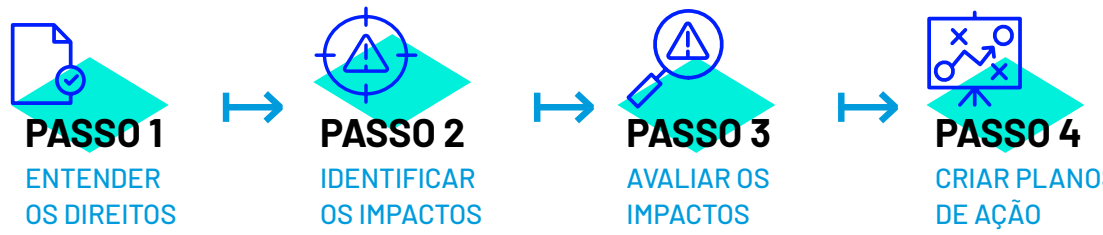
Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

ATENÇÃO!

Segundo Enunciado CD/ANPD nº 1, de 22 de maior de 2023, o melhor interesse da criança e do adolescente deve ser considerado como critério fundamental para a avaliação de atividades de tratamento de dados pessoais que envolvam esse público. Por isso, é importante que as instituições realizem uma avaliação cautelosa em relação ao melhor interesse da criança e do adolescente no caso concreto.

A Information Commissioner's Office (ICO), autoridade britânica de proteção de dados, propõe que a Avaliação do Melhor Interesse seja realizada em quatro etapas:

FIGURA 15_ AVALIAÇÃO DO MELHOR INTERESSE



Fonte: adaptado de Information Commissioner's Office (2021).

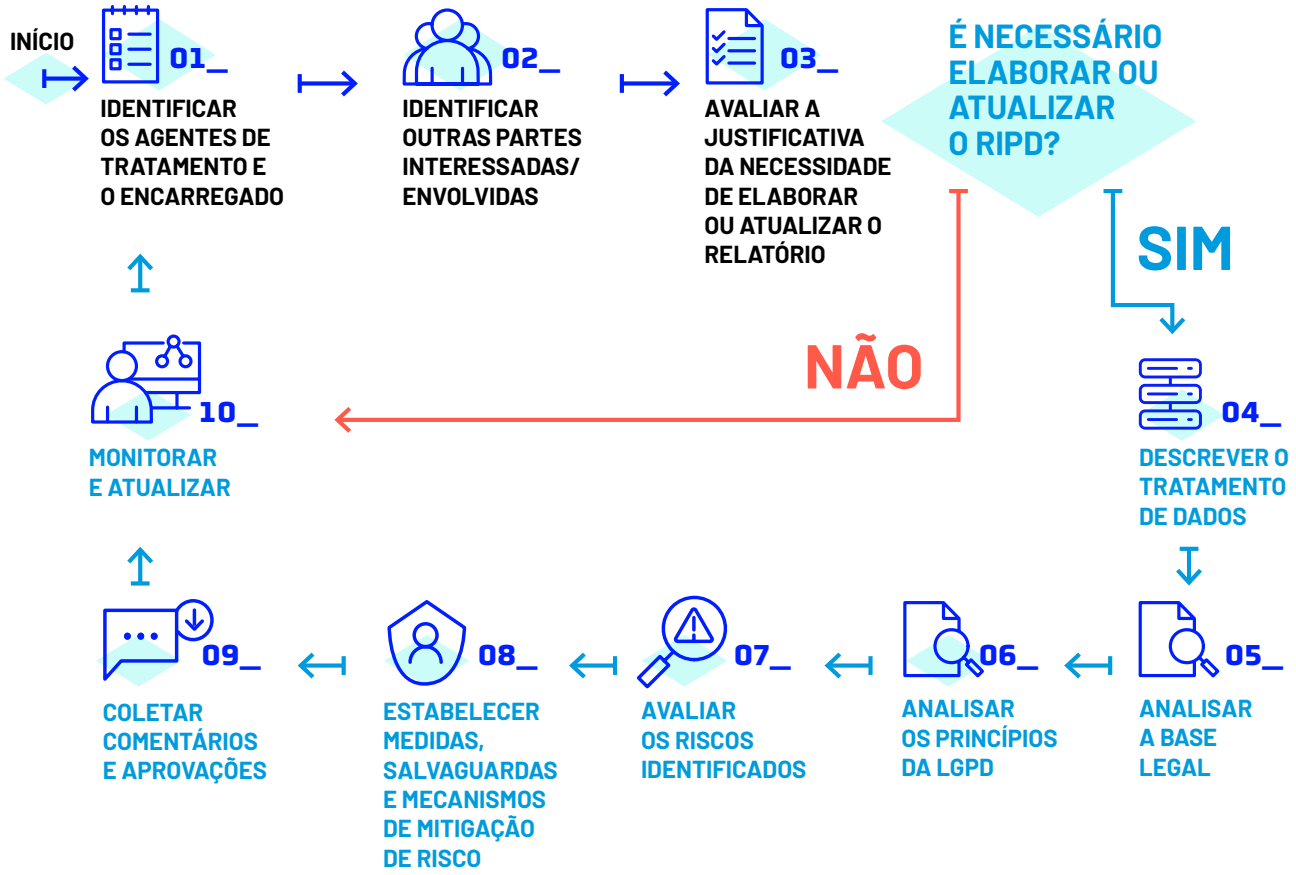
Passo 1_ Entender os impactos. Para esse passo é importante analisar o sistema de proteção infantil já existente, incluindo leis, regulações, acordos internacionais e políticas relevantes para as circunstâncias da atividade de tratamento de dados pessoais. No Brasil, é especialmente importante considerar os direitos previstos no Estatuto da Criança e do Adolescente (ECA)(Lei nº 8.069/1990), como direito à vida e à saúde, direito à cultura e ao lazer, direito à educação.

Passo 2_ Identificar os impactos. De acordo com a ICO, a avaliação dos melhores interesses requer a compreensão de como, por que e quando ocorrem os tratamentos de dados pessoais de crianças e adolescentes.

Passo 3_ Avaliar os impactos. A partir do mapeamento de impactos, recomenda-se a avaliação da probabilidade de ocorrência destes, bem como o impacto em caso de ocorrência. Importante destacar que essa avaliação deve considerar tanto os impactos negativos como os positivos para a promoção de direitos das crianças e adolescentes.

Passo 4_ Criar planos de ação. Após a identificação de impactos, recomenda-se a definição de planos de ação para implementação de medidas mitigatórias aos riscos (impactos negativos) identificados para este público.

FIGURA 16_ INFORMAÇÕES NECESSÁRIAS PARA A ELABORAÇÃO DO RIPD



Fonte: Autoridade Nacional de Proteção de Dados (2023d).

ACESSE!

Sugerimos o acesso ao Guia/Modelo de elaboração do Relatório de Impacto à Proteção de Dados disponibilizado pela Secretaria de Governo Digital (SGD), que está em nosso Artefato nº 9.

Artefato nº 9

A recomendação da elaboração do RIPD pode decorrer, portanto, de uma determinação da ANPD, conforme previsto nos **artigos 32º e 38º da LGPD**, ou como parte das obrigações do controlador para atender ao princípio da responsabilização e prestação de contas (**artigo 6º, X, da LGPD**).

O Programa de Privacidade e Segurança da Informação (PPSI) orienta como uma boa prática que o órgão público, quando aplicável, divulgue relatórios (como relatórios sobre violações, investigações e auditorias) para demonstrar responsabilidade e conformidade com as leis e regulamentos de proteção de dados pessoais. Essa transparência contribui para fortalecer a confiança dos titulares de dados e reflete o compromisso da organização com a segurança e a proteção da privacidade.

O Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) mapeou o risco de identificação dos titulares a partir da base de microdados do Censo Escolar e do Exame Nacional do Ensino Médio (Enem). Com a **elaboração do RIPD**, solicitado pela ANPD, o INEP pôde descrever as atividades de tratamento de dados pessoais que representam potenciais riscos às liberdades civis e aos direitos fundamentais, além de indicar as medidas, salvaguardas e mecanismos adotados para mitigar possíveis violações de privacidade.

Elaboração do RIPD

ATENÇÃO!

A ANPD tem dado especial atenção para situações de desconformidade com a legislação, demonstrando o rigor da Autoridade em assegurar a transparência e o pleno exercício dos direitos dos titulares de dados. Em 2023, instaurou dois processos sancionadores devido à ausência do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme ilustrado abaixo:

TABELA 6_ PROCESSOS SANCIONADORES DA ANPD POR AUSÊNCIA DE RIPD

AGENTE DE TRATAMENTO	MOTIVO DA INSTAURAÇÃO
MINISTÉRIO DA SAÚDE	*Não indicação do encarregado,* ***ausência de envio do RIPD****, não comunicação de incidente de segurança à ANPD e aos titulares e por deixar de atender requisições da ANPD.*
SECRETARIA DE EDUCAÇÃO DO DISTRITO FEDERAL	*Falta de comunicação de incidente aos titulares, ausência de comprovação que os sistemas utilizados atendem aos requisitos de segurança, padrões de boas práticas e governança, ausência de comprovação da manutenção de registros das operações de tratamento de dados pessoais,* ***não apresentação de RIPD*** *e por deixar de atender requisições da ANPD*

Fonte: Autoridade Nacional de Proteção de Dados (2023d).

Em conclusão, o Relatório de Impacto à Proteção de Dados Pessoais se consolida como uma ferramenta essencial para a gestão de riscos no tratamento de dados pessoais, permitindo não só a identificação antecipada de ameaças à privacidade e a adoção de medidas mitigatórias adequadas, mas também a conformidade com a legislação e redução dos riscos de sanções e processos fiscalizadores.

Seu caráter preventivo, dessa forma, alinha-se diretamente ao princípio do *Privacy by Design*, e fortalece a capacidade da organização de antecipação e resposta a riscos, promovendo uma cultura de proteção de dados robusta e eficaz.

ATENÇÃO!

As medidas de mitigação de riscos identificadas na Relatório de Impacto à Proteção de Dados (RIPD) devem ser incorporadas desde as fases iniciais do desenvolvimento de sistemas, garantindo que a privacidade e a segurança da informação sejam princípios estruturantes. Recomenda-se que a Instituição adote abordagens como *Privacy by Design* e *Privacy by Default*, assegurando que os controles de proteção de dados estejam embutidos nas soluções tecnológicas desde sua concepção.

A implementação dessas medidas envolve a aplicação de técnicas como minimização de dados, criptografia, anonimização e segregação de acessos, além da realização de testes contínuos para validar a efetividade dos mecanismos de segurança. Além disso, recomenda-se a revisão periódica das salvaguardas implementadas para garantir sua adequação diante da evolução tecnológica e de novas ameaças.

PPSI

O Método RNP foi desenvolvido com o objetivo de apoiar instituições no fortalecimento da governança e da gestão de conformidade para proteção de dados pessoais. Para reforçar sua aderência a práticas reconhecidas nacionalmente, cada módulo do Método RNP foi mapeado em relação aos controles previstos no Programa de Proteção à Segurança da Informação (PPSI), uma iniciativa estruturante da Secretaria de Governo Digital que orienta órgãos e entidades da Administração Pública Federal na implementação de medidas de segurança e proteção de dados. Confira a seguir os controles do PPSI abordados neste módulo:

TABELA 7_ COMPARATIVO ENTRE O MÓDULO GESTÃO DE RISCOS E O PPSI

CONTROLES DO PPSI	ID DE IDENTIFICAÇÃO
Controle 20_ *Finalidade e Legitimidade*	*20.1; 20.2; 20.3; 20.4; 20.5; 20.14*
Controle 21_ *Governança*	*21.8*
Controle 22_ *Políticas, processos e procedimentos*	*22.7*
Controle 24_ *Minimização de dados*	*24.1; 24.2; 24.3; 24.4; 24.5; 24.6; 24.10*
Controle 25_ Gestão do tratamento	*25.2; 25.3*
Controle 26_ *Acesso e qualidade*	*26.8; 26.9; 26.10*
Controle 30_ *Avaliação de impacto, monitoramento e auditoria*	*30.1; 30.2; 30.3; 30.4; 30.5; 30.6; 30.7*
Controle 31_ *Segurança aplicada a privacidade*	*31.11; 31.12*

MÓDULO TRANSPARÊNCIA NO TRATAMENTO DE DADOS PESSOAIS

Neste módulo você encontrará respostas para as seguintes perguntas:

4.1_ *Como elaborar o Aviso de Privacidade e os Termos de Uso?*

4.2_ *O que são cookies e como cumprir com a transparência?*

4.3_ *Por que e como elaborar um Portal da Privacidade?*

Artefatos relacionados:

ARTEFATO Nº 10_ *Orientações para Elaboração do Termo de Uso e Política de Privacidade do PPSI*

A transparência no tratamento de dados pessoais é um dos princípios da LGPD, disposto no seu **artigo 6º, VI**, essencial para garantir que os titulares tenham acesso fácil a informações claras e precisas sobre como suas informações estão sendo utilizadas.

O **artigo 9º da LGPD** estabelece que o titular dos dados pessoais tem direito a um acesso facilitado minimamente às seguintes informações sobre o tratamento de seus dados:

01_ Finalidade específica do tratamento;

02_ Forma e duração do tratamento, observados os segredos comercial e industrial;

03_ Identificação do controlador;

04_ Informações de contato do controlador;

05_ Informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

06_ Responsabilidades dos agentes que realizarão o tratamento; e

07_ Menção explícita aos direitos do titular.

Em âmbito internacional, o European Data Protection Board (EDPB), no documento *Guidelines on transparency under Regulation 2016/679 (GDPR)*, reforça a importância de as informações serem apresentadas em uma linguagem simples, evitando jargões técnicos ou jurídicos que dificultem o entendimento pelo titular.

Guidelines on transparency under Regulation 2016/679 (GDPR)

A elaboração de documentos que descrevam as práticas de tratamento de dados da organização de forma clara e objetiva representa uma etapa fundamental para materializar a transparência.

O **Aviso de Privacidade** e os **Termos de Uso** são exemplos de instrumentos que possibilitam prestar essas informações aos titulares. Quanto aos ***cookies***, também é importante ter banners adequados e cumprir com a transparência sobre a sua coleta e uso. Outra boa prática sugerida para reforçar o compromisso com a transparência envolve a criação de um **Portal da Privacidade**, reunindo em um só lugar políticas, guias, formulários de requisição de direitos e outros recursos que facilitem o exercício dos direitos pelo titular.

A seguir, veremos como estruturar de forma prática essas iniciativas, garantindo que reflitam a essência do princípio da transparência e assegurem um relacionamento de confiança com os titulares de dados.

4.1_ Como elaborar o Aviso de Privacidade e os Termos de Uso?

Garantir a transparência no tratamento de dados passa, entre outras medidas, pela elaboração de um **Aviso de Privacidade**, que informa de maneira clara e acessível como os dados pessoais são coletados, utilizados e armazenados. Quando aplicável, a criação de **Termos de Uso** também é fundamental, pois detalha as condições de funcionamento do serviço e os direitos e deveres dos usuários.

AVISO DE PRIVACIDADE

01_ Essencial para garantir que os titulares compreendam como seus dados são coletados, processados, armazenados e compartilhados.

02_ Informa o titular, por exemplo, sobre os dados coletados, sua finalidade, base legal para o tratamento, compartilhamento de dados e medidas de segurança adotadas.

TERMOS DE USO

01_ Necessário quando a organização oferece serviços digitais ou plataformas que exigem a adesão a regras específicas por parte dos usuários.

02_ Define, por exemplo, o funcionamento do serviço, as regras aplicáveis, as responsabilidades do usuário e da organização, os contatos para esclarecimentos e o foro para solução de conflitos.

ACESSE!

Para facilitar o desenvolvimento desses documentos, a Secretaria de Governo Digital elaborou o Guia de Elaboração de Termo de Uso e Política de Privacidade. Veja também no Artefato nº 10 o modelo com orientações para elaboração desses documentos elaborado pela SGD, que pode ser usado e/ou adaptado pelas organizações para atender às necessidades específicas de cada contexto.

Guia de Elaboração de Termo de Uso e Política de Privacidade

Artefato nº 10

Para garantir que o Aviso de Privacidade e os Termos de Uso estejam sempre disponíveis e facilmente acessíveis, sem necessidade de solicitação, recomendam-se as seguintes medidas:

01_ Localização estratégica: posicionar os documentos em locais de fácil acesso no site da organização, como no rodapé da página inicial, em formulários de contato e em qualquer página onde dados pessoais sejam coletados.

02_ Exibição antecipada: assegurar que, sempre que possível, os documentos sejam apresentados antes da coleta de dados, com destaque adequado.

03_ Acessibilidade: garantir que os documentos sejam compreensíveis a todos, incluindo pessoas com deficiências visuais, auditivas, motoras ou cognitivas.

ATENÇÃO!

É essencial que o Aviso de Privacidade seja atualizado regularmente para refletir qualquer alteração na forma de tratamento dos dados pessoais. Sempre que houver mudanças, por exemplo, na finalidade do uso de dados, compartilhamento com terceiros ou novos procedimentos de segurança, os titulares devem ser informados de maneira clara.

Veja o exemplo do Aviso de Privacidade disponibilizado que pode servir também como referência para a sua elaboração:

Site da Autoridade Nacional de Proteção de Dados (ANPD)

4.2_ O que são cookies e como cumprir com a transparência?

Cookies são pequenos arquivos de texto armazenados no dispositivo do usuário quando ele acessa um site. Esses arquivos permitem a coleta de informações sobre a navegação e podem ser utilizados para diferentes finalidades, como personalização de conteúdo, segurança, estatísticas de uso e veiculação de anúncios direcionados.

Segundo apresentado pela ANPD em seu **Guia Orientativo sobre Cookies e Proteção de Dados Pessoais**, as categorias de cookies são variadas e podem partir de diferentes perspectivas, como: (i) a entidade responsável pela sua gestão, como *cookies* próprios ou de terceiros; (ii) a finalidade, como cookies de desempenho ou de publicidade; (iii) período de retenção das informações, como cookies temporários; e (iv) de acordo com a necessidade dos *cookies*, se necessários ou não, conforme explicado a seguir:

01_ *Cookies* necessários: essenciais para o funcionamento do portal e não podem ser desativados pelo usuário.

02_ *Cookies* não necessários: cuja desabilitação não impede o funcionamento do site ou aplicação ou a utilização do serviço pelo usuário. Exemplo de *cookies* não necessários incluem, aqueles utilizados para medir o desempenho de um determinado portal ou utilizados para exibição de conteúdos específicos, como anúncios.

Guia Orientativo sobre *Cookies* e Proteção de Dados Pessoais

ACESSE!

Para orientar os agentes de tratamento sobre as boas práticas relacionadas ao tratamento de dados pessoais decorrentes da coleta de *cookies*, a ANPD elaborou o Guia Orientativo: *Cookies* e Proteção de Dados Pessoais. Consulte este material para aprofundamento no tema!

Guia Orientativo: *Cookies* e Proteção de Dados Pessoais

Ao coletar dados pessoais por meio de *cookies*, é fundamental atender aos princípios de proteção de dados, destacando o livre acesso e a transparência, para auxiliar os titulares na compreensão do tratamento de seus dados. Portanto, recomenda-se a elaboração de uma **Política de Cookies**.

A Política de Cookies deve incluir informações sobre as **finalidades específicas** que justificam a coleta de dados pessoais por meio de cookies, **o período de retenção** e a possibilidade de **compartilhamento** com terceiros.

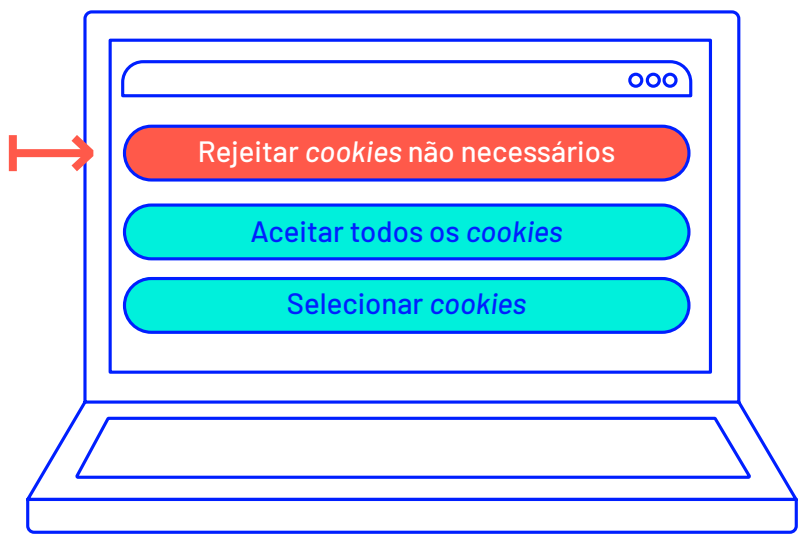
Essa política pode ser apresentada de diferentes formas:

01_ Como uma seção do Aviso de Privacidade;

02_ Em uma página dedicada no site;

03_ Diretamente no banner de *cookies**, permitindo ao usuário gerenciar suas preferências.

FIGURA 17_ BANNERS DE PRIMEIRO NÍVEL



Fonte: Autoridade Nacional de Proteção de Dados (2022b).

*O ***banner* de *cookies*** é um recurso visual que utiliza barras de leitura destacadas para informar ao usuário, de forma resumida, simples e direta, sobre a utilização de *cookies* naquele ambiente.

Além disso, ele fornece ferramentas que permitem maior controle sobre o tratamento, como um botão para rejeitar *cookies* não essenciais, conforme ilustrado na página da ANPD:

FIGURA 18_ BANNER DE *COOKIES* DA PÁGINA DA ANPD

Fonte: Autoridade Nacional de Proteção de Dados ([202-]).

É importante ressaltar que o fornecimento do serviço deve ser mantido mesmo quando os titulares de dados pessoais se recusam a fornecer consentimento para *cookies* não essenciais. Os *cookies* estritamente necessários podem ser fundamentados no legítimo interesse da instituição ou, quando aplicável, no cumprimento de obrigações ou atribuições legais.

4.3_ Por que e como elaborar um Portal da Privacidade?

O **Portal da Privacidade** também é uma boa prática para promover a transparência, fortalecer a confiança dos titulares e consolidar as diretrizes de proteção de dados institucionais. Esse ambiente pode oferecer informações acessíveis sobre o tratamento de dados pessoais, destacando os compromissos e diretrizes estabelecidos nas políticas institucionais de proteção de dados.

Embora não obrigatória, essa plataforma facilita o acesso dos titulares a informações sobre seus direitos e processos de tratamento, reforçando a confiança e o compromisso da organização com a privacidade.

Por meio do Portal da Privacidade, a organização pode, em um ambiente unificado, disponibilizar o Aviso de Privacidade, divulgar a identidade e forma de contato do Encarregado, viabilizar procedimento facilitado para exercício de direitos de titulares e prestar informações sobre *cookies*.

Para que os titulares encontrem as informações de forma intuitiva, é fundamental que o portal seja claro, objetivo e de fácil acesso, mesmo para aqueles que não têm familiaridade com termos técnicos ou jurídicos. Na tabela abaixo, é possível visualizar sugestões de itens a serem expostos no portal.

TABELA 8_ SUGESTÃO DE ESCOPO PARA CONSTRUÇÃO DO PORTAL DE PRIVACIDADE

ITEM	CONTEÚDO GERAL
APRESENTAÇÃO	*A apresentação pode conter o conteúdo geral sobre a LGPD e que medidas a instituição toma para se adequar à norma.*
DIREITOS DO TITULAR	*Podem ser apresentados os direitos do titular e o procedimento para realizar uma solicitação.*
GUIAS, MANUAIS E CAMPANHAS	*Sugere-se que todo e qualquer documento produzido pela instituição ou documentos informativos de outros órgãos (inclusive a ANPD) sejam disponibilizados no portal para facilitar o acesso de todos os interessados. Essa também é uma forma de aumentar o conhecimento das pessoas e propagar uma cultura de privacidade.*
EVENTOS, CURSOS E TREINAMENTOS	*Divulgação de eventos, cursos e treinamentos promovidos que foram ou serão realizados sobre o tema.*
FALE COM O ENCARREGADO	*Informações da identidade e contato do Encarregado pelo tratamento de dados e do seu substituto.*
AVISO DE PRIVACIDADE	*Link de acesso ou íntegra do conteúdo do Aviso de Privacidade.*
POLÍTICA DE *COOKIES*	*Link de acesso ou íntegra do conteúdo de eventual Política de Cookies.*

Fonte: elaboração própria.

ATENÇÃO!

O compartilhamento de dados pessoais deve estar alinhado ao propósito original informado ao titular no momento da coleta, garantindo que a nova utilização seja compatível com a finalidade previamente estabelecida. Essa compatibilidade deve ser analisada considerando o contexto do tratamento e a expectativa legítima do titular. A revisão periódica das práticas de compartilhamento e dos termos previstos em instrumentos de transparência é essencial para garantir que o tratamento dos dados continue alinhado às informações transmitidas e expectativas dos titulares envolvidos.

ATENÇÃO!

Recomenda-se a disponibilização de informações claras e acessíveis ao titular sobre os meios e procedimentos utilizados para o gerenciamento de seus dados pessoais. Isso inclui orientações sobre como os dados são coletados, armazenados, processados e, quando aplicável, compartilhados, garantindo transparência e controle sobre o tratamento. É essencial que o titular tenha acesso a canais específicos para exercer seus direitos, como confirmação da existência de tratamento, correção de dados imprecisos, anonimização, eliminação e portabilidade. Essas informações devem estar disponíveis de forma objetiva, preferencialmente por meio de portais institucionais, documentos informativos e políticas de privacidade.

PPSI

O Método RNP foi desenvolvido com o objetivo de apoiar instituições no fortalecimento da governança e da gestão de conformidade para proteção de dados pessoais. Para reforçar sua aderência a práticas reconhecidas nacionalmente, cada módulo do Método RNP foi mapeado em relação aos controles previstos no Programa de Proteção à Segurança da Informação (PPSI), uma iniciativa estruturante da Secretaria de Governo Digital que orienta órgãos e entidades da Administração Pública Federal na implementação de medidas de segurança e proteção de dados. Confira a seguir os controles do PPSI abordados neste módulo:

TABELA 9_ COMPARATIVO ENTRE O MÓDULO TRANSPARÊNCIA NO TRATAMENTO DE DADOS PESSOAIS E O *FRAMEWORK* DO PPSI

CONTROLES DO PPSI	ID DE IDENTIFICAÇÃO
Controle 20_ Finalidade e Legitimidade	*20.10; 20.11; 20.12; 20.13;*
Controle 24_ Minimização dos dados	*24.13; 24.14; 24.15;*
Controle 29_ Abertura, transparência e notificação	*29.1; 29.2; 29.3; 29.4; 29.5; 29.6; 29.7; 29.8; 29.9; 29.10; 29.11*

Fonte: elaboração própria.

MÓDULO GESTÃO DE TERCEIROS

Neste módulo você encontrará respostas para as seguintes perguntas:

5.1_ *Como realizar a gestão de terceiros?*

5.2_ *Como realizar a identificação e seleção de fornecedores?*

5.3_ *Como operacionalizar a contratação de fornecedores?*

5.4_ *Por que e como monitorar fornecedores?*

Artefatos relacionados:

ARTEFATO Nº 11_ *Sugestões de questionamentos para operadores*

ARTEFATO Nº 12_ *Sugestões de questionamentos para operadores fornecedores de softwares*

Terceiros, como fornecedores, prestadores de serviços e parceiros comerciais, desempenham um papel essencial no tratamento de dados pessoais em nome da Organização. Contudo, também representam um potencial risco de segurança, especialmente se não adotarem medidas de proteção e conformidade equivalentes às da organização.

A gestão de terceiros, portanto, é medida que visa assegurar que os terceiros que tratam dados pessoais em nome da organização também estejam em conformidade com a LGPD. De acordo com o **artigo 39º da LGPD**, o controlador deve assegurar que o tratamento de dados realizado por operador esteja de acordo com as suas instruções e as diretrizes estabelecidas pela lei.

Assim, avaliar previamente possíveis terceiros com quem pretende-se relacionar, estabelecer instrumentos contratuais com obrigações e responsabilidades bem definidas e monitorar o cumprimento dos contratos por esses parceiros são algumas das medidas consideradas essenciais para realizar a gestão de terceiros no contexto de um Programa de Privacidade.

A **gestão de terceiros** é uma rotina voltada a **mitigar riscos, garantir conformidade e proteger a reputação institucional**. Esse processo visa assegurar que todas as práticas de tratamento de dados do terceiro estejam alinhadas à LGPD e às políticas de segurança da informação da organização.

5.1_ Como realizar a gestão de terceiros?

Uma gestão eficaz deve abranger todas as etapas do relacionamento com terceiros, desde a **seleção inicial** dos fornecedores até a **avaliação contínua** de suas práticas de segurança e privacidade, incluindo, quando necessário, a renovação ou rescisão contratual. Nesse contexto, o Método RNP sugere três tópicos essenciais que as organizações devem observar para realizar esse controle de forma eficiente:

GESTÃO DE TERCEIROS

IDENTIFICAÇÃO E SELEÇÃO DE FORNECEDORES

CONTRATAÇÃO DE FORNECEDORES

MONITORAMENTO DE FORNECEDORES

5.2_ Como realizar a identificação e seleção de fornecedores?

Para garantir uma gestão eficaz de terceiros no tratamento de dados pessoais, é recomendável seguir processo estruturado que comece pelo **mapeamento de necessidades da organização**. Nesse estágio, a organização deve identificar quais serviços serão terceirizados e quais dados pessoais os terceiros envolvidos tratarão.

Em seguida, é fundamental estabelecer **critérios claros para a seleção de fornecedores**, considerando requisitos específicos de segurança da informação, privacidade e proteção de dados pessoais. Esses critérios devem ser aplicados na **avaliação prévia de fornecedores**, assegurando a conformidade com as legislações e políticas internas de privacidade e proteção de dados pessoais da organização.

ACESSE!

Organizamos um documento com sugestões de questionamentos a serem direcionados para operadores, que está disponível em nosso Artefato nº 11, e um específico para operadores fornecedores de software, acessível no Artefato nº 12, que podem ser complementados a depender das circunstâncias específicas do tratamento de dados e das tecnologias envolvidas.

Artefato nº 11

Artefato nº 12

ATENÇÃO!

Dadas as restrições na escolha de fornecedores em contratações públicas, a avaliação prévia deve considerar a realidade dos processos licitatórios. Assim, as medidas de privacidade e proteção de dados devem ser adotadas desde o planejamento da contratação até a execução do contrato.

No planejamento, o Estudo Técnico Preliminar (ETP) pode incluir exigências de conformidade com a LGPD, que serão incorporadas ao Termo de Referência. Isso é essencial quando a contratação envolve tratamento significativo de dados pessoais. Além disso, o fornecedor pode ser solicitado a apresentar uma declaração de cumprimento das normas de proteção de dados.

As regras definidas nessa fase devem ser refletidas nos documentos do processo licitatório e na execução do contrato. A minuta contratual, além de regulamentar a prestação do serviço, deve estabelecer normas e responsabilidades do fornecedor quanto à proteção de dados.

Após essa definição, deve-se executar a avaliação inicial dos fornecedores, considerando, para além dos pontos expostos nos Artefatos acima, a existência de certificações, como a ISO 27001, bem como de rotinas de governança em privacidade estabelecidas.

Rotinas relevantes que devem ser consideradas para avaliação de maturidade do Programa de Privacidade do terceiro:

01_ Mapeamento de dados e registro de inventário;

02_ Avaliações de risco;

03_ Estrutura de governança e Encarregado nomeado;

04_ Procedimento e canal para atendimento de titulares;

05_ Gestão de terceiros;

06_ Adoção de medidas de transparência;

07_ Procedimentos para tratativa de Incidentes de Segurança;

08_ Existência de reclamações, fiscalizações, processos e Incidentes relativos à proteção de dados pessoais.

ATENÇÃO!

Quanto mais pontos de risco forem identificados no serviço a ser contratado, maior a necessidade de um Programa de Privacidade sólido, com a maior parte das rotinas atendidas, e, consequentemente, com cláusulas contratuais mais robustas.

5.3_ Como operacionalizar a contratação de fornecedores?

Realizada a avaliação inicial e a seleção do(s) fornecedor(es) que se pretende contratar, é essencial formalizar a relação por meio de um **instrumento contratual** que estabeleça claramente as obrigações e responsabilidades do terceiro. Esse instrumento deve incluir **cláusulas específicas** para garantir a conformidade com a legislação de proteção de dados e resoluções aplicáveis, assegurando que o fornecedor adote efetivamente medidas adequadas de segurança e privacidade no tratamento de dados pessoais. A tabela abaixo traz exemplos de cláusulas essenciais para a formalização da relação:

FIGURA 19_ CLÁUSULAS EM CONTRATOS RELACIONADAS À LGPD

Fonte: elaboração própria.

Além disso, A ANPD disponibilizou um ***checklist*** para Agentes de Tratamento de Pequeno Porte com medidas de segurança a serem adotadas, inclusive cláusulas essenciais em contratos com terceiros, destacando:

01_ Regras para fornecedores e parceiros;

02_ Regras sobre compartilhamentos;

03_ Relações entre controlador-operador;

04_ Orientações sobre o tratamento a ser realizado com vedação de tratamentos incompatíveis com as orientações do controlador.

***Checklist* para Agentes de Tratamento de Pequeno Porte**

ATENÇÃO!

Os processos de contratação de soluções de Tecnologia da Informação e Comunicação (TIC) pelos órgãos e entidades que integram o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal devem seguir as diretrizes estabelecidas pela **Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022**. Essa normativa orienta a aquisição de soluções tecnológicas de forma a garantir conformidade com padrões de governança, segurança e eficiência no uso dos recursos de TIC.

Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022

Para auxiliar na adequação dos processos de contratação em conformidade com a Instrução Normativa nº 94, a Secretaria de Governo Digital (SGD) publicou:

Guia de Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação

Este guia fornece orientações detalhadas para garantir que as contratações atendam aos requisitos de privacidade e segurança exigidos, inclusive condições que devem ser consideradas na gestão dos contratos.

Entre as principais recomendações estão:

DEFINIÇÃO DE ESCOPO E FINALIDADE_	*Determinar, no contrato, o objetivo e o prazo do serviço, a forma e a finalidade do tratamento de dados, além dos tipos de dados processados.*
DEFINIÇÃO DAS FUNÇÕES DO OPERADOR_	*Estabelecer as responsabilidades do operador, com destaque para a obrigação de notificar violações de dados.*
RESPEITO À FINALIDADE_	*Prever que o processamento dos dados coletados seja limitado ao mínimo necessário para atendimento da finalidade pretendida.*
EXERCÍCIO DE DIREITOS PELO TITULAR_	*Instruir o operador, através das cláusulas contratuais, a fornecer meios que permitam o gerenciamento dos dados pessoais pelos titulares, bem como a obrigação de comunicar o controlador em caso de solicitações.*
PLANOS DE CONTINUIDADE_	*Dispor a necessidade de que o fornecedor tenha planos de continuidade de negócios e recuperação de desastres, especialmente se for responsável por tratar ou armazenar grandes volumes de dados da organização.*
CUMPRIMENTO DAS CLÁUSULAS CONTRATUAIS_	*Monitorar e exigir que o operador cumpra todas as cláusulas de confidencialidade e proteção de dados, salvo em casos de restrição legal.*

DETERMINAÇÃO DE RESPONSABILIDADES_	*Especificar as responsabilidades de cada operador e controlador conjunto no tratamento de dados pessoais.*
DIRECIONAR SUBCONTRATAÇÃO_	*Incluir cláusulas contratuais que disciplinem o uso de subcontratados no processamento de dados pessoais, com necessidade de aprovação prévia pelo controlador.*
SEGURANÇA NOS SISTEMAS DO OPERADOR_	*Especificar as exigências de segurança e requisitos de conformidade, e dispor que os sistemas utilizados pelo operador implementem mecanismos de proteção para controle da integridade dos dados e para identificação de operações realizadas com os dados pessoais.*
COMUNICAÇÃO COM O CONTROLADOR_	*Prever que o operador mantenha o controlador informado sobre questões relevantes relacionadas ao tratamento de dados, especialmente em casos de: (i) solicitações legais e/ou de titulares com relação aos dados objeto do contrato; (ii) incidentes de segurança envolvendo dados pessoais objeto do contrato; e (iii) alterações significativas nos serviços prestados.*
DESCARTE SEGURO DE DADOS_	*Estipular condições para que, ao término do contrato ou serviço, o operador devolva ou descarte os dados pessoais de forma segura, conforme orientações do controlador.*

ATENÇÃO!

O desenvolvimento de terceiros em relação às políticas da organização também é crucial! Compartilhar suas políticas internas e ofertar treinamentos a elas relacionados pode auxiliar com que terceiros compreendam suas responsabilidades e as melhores práticas de segurança.

De acordo com o **artigo 48º da LGPD**, é responsabilidade do controlador comunicar à ANPD e ao titular qualquer incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Os Incidentes deverão seguir o fluxo de comunicação estabelecido para que a organização controladora tome as medidas cabíveis relacionadas à comunicação.

ATENÇÃO!

Os instrumentos convocatórios, incluindo editais de licitação, devem estar alinhados às disposições da LGPD, garantindo que o tratamento de dados pessoais no processo licitatório ocorra de forma transparente, segura e proporcional à finalidade prevista. É recomendável que cláusulas específicas sobre confidencialidade, compartilhamento e descarte de dados sejam incluídas nos editais e contratos administrativos, bem como a exigência de conformidade com boas práticas de governança e segurança da informação. A revisão periódica dos instrumentos convocatórios é essencial para garantir que permaneçam atualizados frente às diretrizes regulatórias.

ATENÇÃO!

Qualquer alteração, correção ou remoção de dados pessoais deve ser devidamente comunicada a operadores e terceiros com quem essas informações tenham sido compartilhadas, assegurando a atualização e conformidade do tratamento. Essa comunicação deve seguir um processo estruturado, estabelecendo responsabilidades claras nos contratos e acordos firmados com operadores e demais entidades envolvidas.

Essas recomendações fortalecem a governança de dados e buscam garantir que operadores cumpram padrões rigorosos de proteção e conformidade, minimizando riscos para a organização e para os titulares dos dados.

5.4_ Por que e como monitorar fornecedores?

O monitoramento e a avaliação contínua de fornecedores são fundamentais para garantir que suas práticas de proteção de dados permaneçam alinhadas às exigências da LGPD, às políticas internas da organização e às obrigações contratuais estabelecidas.

Mesmo após a contratação, é essencial acompanhar regularmente se o fornecedor mantém medidas adequadas de segurança, privacidade e conformidade, minimizando riscos e prevenindo incidentes. Esse acompanhamento permite não apenas identificar e corrigir falhas rapidamente, mas também ajustar cláusulas contratuais conforme mudanças regulatórias e novas necessidades da organização.

O monitoramento contínuo fortalece a governança de dados, assegura a responsabilidade compartilhada e protege tanto a organização quanto os titulares dos dados envolvidos.

Uma medida crucial para garantir essa supervisão de forma efetiva é investir em capacitação contínua dos servidores da organização. Uma equipe interna capacitada em relação ao Programa de Privacidade é apta para gerenciar relações com terceiros, monitorar o cumprimento contratual, e, se necessário, realizar auditorias e relatórios de conformidade, garantindo o alinhamento às exigências da LGPD.

Além disso, é fundamental estabelecer um processo estruturado de comunicação com terceiros para que informações relevantes sobre o tratamento de dados, como em relação a Incidentes de Segurança, sejam compartilhadas de maneira rápida e satisfatória, auxiliando também no processo de monitoramento.

As **auditorias periódicas** também são uma ferramenta adicional essencial para revisar como os terceiros tratam os dados e se suas práticas estão alinhadas com a LGPD e as políticas internas da organização.

Essas auditorias podem ser realizadas internamente ou por auditores externos, avaliando a eficácia das medidas de segurança, a conformidade com os regulamentos vigentes e a atualização dos processos conforme as melhores práticas de proteção de dados. A revisão pode incluir análises de relatórios de incidentes, verificações de conformidade e avaliações contínuas de riscos.

Além das auditorias, a organização deve revisar regularmente as práticas de privacidade dos terceiros, o que pode ser feito a partir da **renovação periódica da avaliação dos terceiros**, com o objetivo de identificar se o Programa de Privacidade se encontra em melhoria contínua e se há, pelo terceiro, acompanhamento das atualizações regulatórias.

O fornecimento de **relatórios regulares de conformidade** pelo terceiro, detalhando suas práticas de tratamento de dados, incidentes de segurança e medidas corretivas adotadas, também auxiliarão a garantir que eventuais problemas sejam identificados e corrigidos rapidamente.

Assim, antes de renovar um contrato com um fornecedor, é essencial realizar uma revisão periódica de todos os processos de monitoramento para avaliar seu desempenho em relação às obrigações contratuais de proteção de dados.

Essa análise deve verificar se o fornecedor se manteve conforme em relação às obrigações previamente estabelecidas e se adotou medidas adequadas de segurança.

Com essas medidas, a organização mantém um controle eficaz sobre os terceiros, minimizando riscos e reforçando a proteção dos dados pessoais sob sua responsabilidade.

PPSI

O Método RNP foi desenvolvido com o objetivo de apoiar instituições no fortalecimento da governança e da gestão de conformidade para proteção de dados pessoais. Para reforçar sua aderência a práticas reconhecidas nacionalmente, cada módulo do Método RNP foi mapeado em relação aos controles previstos no Programa de Proteção à Segurança da Informação (PPSI), uma iniciativa estruturante da Secretaria de Governo Digital que orienta órgãos e entidades da Administração Pública Federal na implementação de medidas de segurança e proteção de dados. Confira a seguir os controles do PPSI abordados neste módulo:

TABELA 10_ COMPARATIVO ENTRE O MÓDULO GESTÃO DE TERCEIROS E O *FRAMEWORK* DO PPSI

CONTROLES DO PPSI	ID DE IDENTIFICAÇÃO
Controle 21_ *Governança*	*21.5*
Controle 22_ *Políticas, processos e procedimentos*	*22.4*
Controle 27_ *Compartilhamento, transferência e divulgação*	*27.3; 27.4*
Controle 28_ *Supervisão de terceiros*	*28.1; 28.2; 28.3; 28.4; 28.5; 28.6; 28.7; 28.8; 28.9; 28.10; 28.11; 28.12; 28.13*

Fonte: elaboração própria.

MÓDULO ATENDIMENTO AOS TITULARES

Neste módulo você encontrará respostas para as seguintes perguntas:

Os direitos dos titulares de dados pessoais estão dispostos ao longo da LGPD, com ênfase nos **artigos 17º a 22º** da Lei. Este módulo fornece diretrizes gerais para o atendimento aos titulares, apresentando ações que favorecem uma comunicação eficaz entre as partes envolvidas e asseguram a conformidade legal.

Para garantir a eficácia do atendimento, cada organização deve estabelecer um **canal oficial de comunicação** que seja ativo, seguro e autenticado para receber eventuais requisições, questionamentos e reclamações dos titulares de dados.

ATENÇÃO!
É essencial estruturar um fluxo claro e eficiente para responder às solicitações dos titulares dentro dos prazos estabelecidos pela legislação aplicável, garantindo padronização no atendimento.

6.1_ Quais são os direitos dos titulares de dados?

Abaixo, estão descritos os principais direitos dos titulares, conforme estabelecido na LGPD:

CONFIRMAÇÃO DE TRATAMENTO_	*o titular poderá solicitar confirmação sobre a existência de tratamento de seus dados pessoais pela organização;*
ACESSO AOS DADOS PESSOAIS_	*o titular poderá solicitar acesso a seus dados pessoais tratados pela organização;*
CORREÇÃO OU ATUALIZAÇÃO DOS DADOS PESSOAIS_	*o titular pode solicitar a correção de dados pessoais que estejam desatualizados, incorretos ou incompletos;*
ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO_	*o titular pode solicitar a exclusão, anonimização ou bloqueio de dados pessoais quando tratados de forma excessiva, desnecessária ou em desconformidade com a LGPD;*
PORTABILIDADE_	*uma vez regulamentado pela Autoridade Nacional de Proteção de Dados, o titular poderá solicitar a portabilidade de seus dados pessoais;*
ELIMINAÇÃO DE DADOS TRATADOS COM BASE NO CONSENTIMENTO_	*nos casos em que a base legal para o tratamento de dados pessoais for o consentimento, o titular poderá requerer a exclusão de seus dados pessoais tratados com base nessa autorização;*
REVOGAÇÃO DO CONSENTIMENTO_	*nos casos em que a base legal para tratamento de dados pessoais for o consentimento, o titular poderá revogar a autorização concedida, a qualquer tempo e de forma facilitada;*
OPOSIÇÃO AO TRATAMENTO_	*o titular pode se opor ao tratamento de seus dados pessoais, desde que verificada inconformidade com a LGPD;*

REVISÃO DE DECISÕES AUTOMATIZADAS E SOLICITAÇÃO DE INFORMAÇÕES SOBRE CRITÉRIOS ADOTADOS_	*o titular poderá solicitar a revisão de decisões tomadas unicamente com base no tratamento automatizado de seus dados pessoais (sem participação humana), desde que referidas decisões afetem os seus interesses, e/ou solicitar informações sobre os critérios adotados para a tomada dessa decisão; e*
INFORMAÇÕES SOBRE O COMPARTILHAMENTO_	*o titular poderá solicitar o fornecimento de informações sobre as entidades públicas e privadas com as quais foi realizado o compartilhamento de seus dados pessoais.*

ATENÇÃO!

A Autoridade Nacional de Proteção de Dados (ANPD) incluiu, em sua Agenda Regulatória para o Biênio 2025-2026, a elaboração de uma norma específica sobre os direitos dos titulares. Em fevereiro de 2024, a ANPD abriu uma consulta pública para receber contribuições sobre prazos, formas e procedimentos para o exercício desses direitos pelos titulares, bem como para sua operacionalização pelos controladores.

Agenda Regulatória para o Biênio 2025-2026

6.2_ Como implementar um fluxo de atendimento aos titulares?

Para garantir que os titulares de dados pessoais possam exercer seus direitos de forma eficaz, é essencial que as organizações estabeleçam um canal de atendimento estruturado, seguro e acessível e um fluxo organizado do procedimento.

ESTABELEÇA UM CANAL FACILITADO

A organização deve estabelecer um meio acessível para que os titulares realizem solicitações, como um *e-mail* exclusivo, um formulário no site institucional ou uma plataforma dedicada. Esse canal deve ser amplamente divulgado e projetado para ser intuitivo, permitindo que os titulares realizem suas solicitações de forma simples e sem burocracia excessiva.

No caso da administração pública, o **Guia de Boas Práticas do PPSI** sugere a utilização da plataforma **Fala.BR** como canal para endereçamento de solicitações dos titulares de dados.

Guia de Boas Práticas do PPSI

Essa foi a opção adotada, por exemplo, pelo Supremo Tribunal Federal por meio da **Resolução nº 838/2024.** O fluxo foi pensado para garantir mais segurança no cumprimento dos direitos dos titulares de dados no Tribunal, devido à possibilidade de autenticação do usuário, além da experiência da Ouvidoria no relacionamento com o público externo. Na prática, a Ouvidoria recebe as solicitações dos titulares de dados e as encaminha ao Encarregado do STF.

Resolução nº 838/2024

BOAS PRÁTICAS!

01_ Disponibilizar instruções claras sobre como os titulares podem exercer seus direitos.

02_ Prestar esclarecimentos e adotar providências cabíveis.

03_ Garantir que o canal seja acessível a pessoas com deficiência.

04_ Evitar solicitações excessivas de informações que dificultem o acesso aos direitos.

05_ Adotar medidas de segurança que garantam a proteção dos dados tanto na recepção quanto no processamento das solicitações.

CONFIRME A IDENTIDADE DO TITULAR

Antes de processar solicitações, é recomendável que a organização adote meios para garantir **que a pessoa que fez o pedido é realmente o titular dos dados**. Dessa forma, é sugere-se a implementação de mecanismos de identificação para evitar que terceiros não autorizados acessem dados pessoais indevidamente.

Algumas formas de verificação incluem a obtenção e validação de documentos de identidade oficiais. No caso da administração pública, como mencionado anteriormente, o uso da plataforma **Fala.BR** é sugerido por contar com a autenticação via **gov.br**, mecanismo de acesso digital único aos serviços públicos federais, estaduais e municipais regulamentado pelo Decreto nº 8.936/2016.

ACIONE AS ÁREAS INTERNAS DA ORGANIZAÇÃO

Em muitos casos, será necessário envolver diferentes departamentos para atender à solicitação do titular. O canal de atendimento deve ter um fluxo definido para encaminhar as demandas de forma eficiente.

BOAS PRÁTICAS!

01_ Criar um fluxo interno padronizado para direcionamento das solicitações.

02_ Definir pontos focais das áreas internas que devem ser envolvidos para garantir, quando necessário, informações acerca do tratamento de dados do titular requisitante.

03_ Garantir comunicação interna eficaz para evitar atrasos na resposta.

GERENCIE O TEMPO DE ATENDIMENTO

A LGPD estabelece no art. 19º, IIº, que a confirmação de existência ou o acesso a dados pessoais devem ser providenciados por meio de declaração completa no prazo de até **15 (quinze) dias** contados da data do requerimento do titular.

No art. 23º, §3°, a norma também estabelece que os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei do *Habeas Data*, Lei Geral do Processo Administrativo e Lei de Acesso à Informação.

É essencial monitorar e controlar o tempo entre o recebimento do pedido e a resposta final, organizando as solicitações recebidas e o tempo de retorno.

Para otimizar o tempo de resposta e garantir a conformidade com a legislação, é possível estabelecer prazos internos menores do que os definidos na norma aplicável. Isso permite um fluxo mais ágil e eficiente no tratamento das solicitações dos titulares.

Por exemplo, a **Resolução nº 838/2024** do Supremo Tribunal Federal estabeleceu, no âmbito das solicitações direcionadas ao órgão, a Ouvidoria deve encaminhar o pedido do titular ao Encarregado em até 4 dias, e o Encarregado tem até 11 dias para devolver a resposta elaborada à Ouvidoria. Além disso, no caso de acionamentos internos, as áreas devem responder às solicitações do Encarregado em até 7 dias.

Resolução nº 838/2024

Vale ressaltar que este exemplo não constitui uma regra geral, mas apenas ilustra como podem ser definidos prazos internos estratégicos para assegurar um retorno célere e eficaz ao titular.

GERE EVIDÊNCIAS DO PROCESSAMENTO DAS SOLICITAÇÕES

Para garantir transparência e conformidade, a organização deve documentar todas as solicitações realizadas pelos titulares, bem como as ações tomadas para atendê-las. Esses registros são essenciais para auditorias e inspeções regulatórias.

ATENÇÃO!

Recomenda-se que os dados sejam mantidos em formato interoperável e estruturado, possibilitando o uso compartilhado entre entidades públicas para fins de execução de políticas públicas, prestação de serviços, descentralização da atividade pública e acesso à informação.

A adoção de padrões abertos e estruturados viabiliza a integração entre sistemas, permitindo maior eficiência na gestão pública e evitando redundâncias na coleta e armazenamento de dados. Sem prejuízo, recomenda-se a implementação de protocolos de segurança, controles de acesso e auditorias regulares, garantindo que o uso compartilhado dos dados ocorra de forma controlada, transparente e alinhada aos princípios da proteção de dados pessoais. A revisão periódica dessas diretrizes é essencial para manter a integridade e a segurança das informações ao longo do tempo.

6.3_ LAI e LGPD: como compatibilizar as solicitações?

O **direito à informação** e o **direito à proteção de dados pessoais** são direitos fundamentais expressamente previstos na Constituição Federal, regulamentados, respectivamente, pela Lei nº 12.527/2011 - Lei de Acesso à Informação (LAI) e pela Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

A LGPD determina que a divulgação de dados pessoais seja precedida de cautela e de uma avaliação criteriosa dos riscos. Já a LAI adota a publicidade como regra, permitindo o sigilo apenas em situações excepcionais. Para compatibilizar essas normas, é necessário ponderar entre a proteção da privacidade e dos dados pessoais e o direito de acesso às informações sobre as atividades do Poder Público.

O **Enunciado CGU nº 4/2022** reforça a compatibilidade sistemática entre a LAI e a LGPD, indicando que não há conflito normativo entre seus dispositivos, mas sim uma relação de complementaridade na proteção dos direitos fundamentais. Essa compatibilização exige uma abordagem criteriosa na divulgação de informações que contenham dados pessoais, para garantir que a transparência não viole a privacidade dos titulares de dados.

Enunciado CGU nº 4/2022

A própria LAI já traz caminhos para essa ponderação, uma vez que o art. 31º atribui acesso restrito a informações pessoais, independentemente de classificação de sigilo, pelo prazo de até 100 anos. A sua divulgação poderá acontecer apenas com o consentimento expresso da pessoa a que elas se referirem ou se for necessária para:

01_ Prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

02_ Realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

03_ Cumprimento de ordem judicial;

04_ Defesa de direitos humanos; ou

05_ Proteção do interesse público e geral preponderante.

O **princípio da necessidade** estabelecido na LGPD é um elemento-chave nessa análise. De um lado, a administração deve exigir o mínimo de dados pessoais do requerente para atender à solicitação (art. 10º, § 1º da LAI). De outro, deve avaliar quais dados pessoais podem ser disponibilizados no atendimento do pedido de acesso à informação, observando os limites impostos pela LGPD.

Exemplo prático dessa ponderação é a divulgação da remuneração individualizada de servidores públicos federais, a qual é realizada sem a apresentação completa de números como o CPF e a matrícula do servidor. Com isso, a transparência foi assegurada mitigando riscos aos titulares sem comprometer o controle social sobre as despesas públicas.

Diante disso, na eventual hipótese de recebimento de requisições formuladas com base na LAI que envolvam o fornecimento de dados pessoais, é importante direcionar a solicitação ao Encarregado e que o caso seja avaliado também à luz da LGPD.

Nessa avaliação, deve ser ponderada a possibilidade de disponibilização das informações e, se for o caso, proceder com o fornecimento de justificativa para a ocultação dos dados pessoais em um documento (aplicando-se o disposto no art. 7°, § 2° da LAI) ou mesmo para a integral negativa de acesso, quando impossibilitada a ocultação.

PPSI

O Método RNP foi desenvolvido com o objetivo de apoiar instituições no fortalecimento da governança e da gestão de conformidade para proteção de dados pessoais. Para reforçar sua aderência a práticas reconhecidas nacionalmente, cada módulo do Método RNP foi mapeado em relação aos controles previstos no Programa de Proteção à Segurança da Informação (PPSI), uma iniciativa estruturante da Secretaria de Governo Digital que orienta órgãos e entidades da Administração Pública Federal na implementação de medidas de segurança e proteção de dados. Confira a seguir os controles do PPSI abordados neste módulo:

TABELA 11_ COMPARATIVO ENTRE O MÓDULO ATENDIMENTO AOS TITULARES E O *FRAMEWORK* DO PPSI

CONTROLES DO PPSI	ID DE IDENTIFICAÇÃO
Controle 25_ *Gestão do tratamento*	*25.4*
Controle 26_ *Acesso e qualidade*	*26.1; 26.2; 26.3; 26.4; 26.5; 26.6; 26.7; 26.11*

Fonte: elaboração própria.

MÓDULO SENSIBILIZAÇÃO, EDUCAÇÃO E TREINAMENTO

Neste módulo você encontrará respostas para as seguintes perguntas:

7.1_ *O que significa criar uma cultura de privacidade?*

7.2_ *Como conduzir iniciativas de sensibilização?*

7.3_ *Como conduzir campanhas educativas?*

7.4_ *Como conduzir treinamentos?*

Artefatos relacionados:

ARTEFATO Nº 13_ *Exemplos práticos de campanhas de conscientização da RNP*

ARTEFATO Nº 14_ *Sugestão de plano de curso para treinamento geral*

ARTEFATO Nº 15_ *Modelo de Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação do PPSI*

A conscientização e o treinamento são elementos fundamentais para o sucesso de qualquer programa de governança em privacidade. A fim de que se estabeleça uma **cultura de privacidade**. É essencial garantir que todos os envolvidos compreendam a relevância da proteção de dados pessoais e apliquem boas práticas no dia a dia.

7.1_ O que significa criar uma cultura de privacidade?

Uma cultura de privacidade vai além da implementação de normas e procedimentos. Ela exige uma transformação cultural que envolva todos os colaboradores, promovendo:

CONSCIENTIZAÇÃO

Entendimento claro dos princípios e responsabilidades da LGPD

ENGAJAMENTO

Comprometimento em adotar boas práticas para o tratamento de dados pessoais

RESPONSABILIDADE

Respeito pelos direitos dos titulares e pela conformidade legal

De acordo com o **artigo 50º da LGPD**, é essencial integrar ações educativas às regras de boas práticas e governança, destacando que medidas técnicas isoladas não são suficientes para garantir a proteção dos dados pessoais. Dessa forma, a criação de uma cultura de privacidade é um processo contínuo e colaborativo.

Essa abordagem pode ser dividida em três pilares interligados: **sensibilização**, que estabelece as bases para o entendimento da relevância da LGPD; **campanhas educativas**, que disseminam informações de maneira acessível e ampla; e **treinamentos**, que garantem o desenvolvimento de competências específicas e contínuas. Esses pilares trabalham em conjunto para promover um ambiente que valorize a privacidade e a governança de dados em todos os níveis da organização. A seguir, detalharemos cada um deles.

7.2_ Como conduzir iniciativas de sensibilização?

Sensibilizar os servidores, funcionários e colaboradores da instituição, especialmente os membros da alta e média administração, é um passo crucial para promover o engajamento de toda a organização em relação à conformidade com a LGPD. Ela garante um ambiente mais preparado e receptivo para as medidas de conscientização e treinamento.

Para isso, é fundamental:

01_ Explicar os objetivos da Lei Geral de Proteção de Dados Pessoais e a sua importância para proteger direitos fundamentais, como a privacidade e a liberdade.

02_ Demonstrar os impactos organizacionais, indicando como as mudanças afetam processos e operações.

03_ *E*videnciar os benefícios da conformidade, como a mitigação de riscos, fortalecimento da confiança dos titulares e melhoria da reputação.

04_ Engajar as lideranças como facilitadores do processo, ressaltando que o sucesso depende de um esforço conjunto.

05_ Assegurar o comprometimento da alta gestão, garantindo que as atividades relacionadas à adequação sejam priorizadas.

O QUE PODE SER FEITO?

01_ Promover palestras dinâmicas e interativas que apresentem de forma clara os principais conceitos da LGPD, permitindo que os participantes compreendam a importância da proteção de dados pessoais.

02_ Incentivar a participação em cursos de capacitação, como os oferecidos pela **Escola Nacional de Administração Pública (ENAP)** e pela **Escola Superior de Redes**, que fornecem conteúdos acessíveis e de alta qualidade sobre proteção de dados.

Escola Nacional de Administração Pública (ENAP)

Escola Superior de Redes

7.3_ Como conduzir campanhas educativas?

As campanhas educativas têm como objetivo disseminar informações precisas e atualizadas, promovendo a conscientização e, quando necessário, a mudança de comportamentos.

O QUE PODE SER FEITO?

01_ Desenvolver infográficos atrativos para serem distribuídos em plataformas digitais ou impressos. Veja o exemplo de **mangá educativo sobre direitos dos titulares** disponibilizado pela ANPD, em parceria com a CNIL e PIPC, para promover a conscientização entre jovens.

Mangá educativo sobre direitos dos titulares

02_ Implementar *quizzes* e jogos educativos para engajar os colaboradores de forma interativa.

03_ Produzir vídeos explicativos curtos para divulgar em intranets ou redes sociais corporativas. Veja o exemplo do Instituto Federal do Paraná (IFPR), que **produziu curtas-metragens e os disponibilizou gratuitamente em sua página web.**

Curtas-metragens

ACESSE!

No **Artefato nº 13,** estamos disponibilizando exemplos práticos de campanhas de conscientização que podem ser implementadas. Esses materiais abordam temas como os princípios e direitos previstos na LGPD, a distinção entre dados pessoais e sensíveis, o ciclo de vida dos dados, boas práticas para prevenir vazamentos, dentre outros.

Estruture um calendário de ações e construa um trabalho multidisciplinar junto de áreas de Comunicação e Recursos Humanos, que serão capazes de colaborar na definição das estratégias de divulgação e integrar as campanhas aos programas culturais já existentes.

Artefato nº 13

7.4_ Como conduzir treinamentos?

O treinamento é uma medida que visa desenvolver competências e gerar conhecimento em indivíduos ou grupos. Os treinamentos podem ser realizados de diversas formas, como *workshops*, seminários ou programas de desenvolvimento profissional, tanto de forma *online* como presencial. Essas atividades buscam fornecer informações relevantes, ensinar habilidades específicas e proporcionar oportunidades para a prática e aplicação dos conhecimentos adquiridos.

TREINAMENTOS GERAIS_ focados em maximizar o desempenho profissional no tratamento de dados pessoais, esses treinamentos visam aumentar o conhecimento e a conscientização sobre a execução adequada das atividades relacionadas à proteção de dados.

ACESSE!

No **Artefato nº 14**, estamos disponibilizando uma sugestão de **plano de curso** com os objetivos, conteúdo programático e referências aplicáveis para esse tipo de treinamento geral. Recomendamos que o curso seja obrigatório e periódico e que eventuais logs de acesso de colaboradores fiquem condicionados à sua conclusão.

Artefato nº 14

TREINAMENTOS DIRECIONADOS_ treinamentos personalizados para atender às particularidades e necessidades de cada unidade de trabalho. Esses treinamentos devem ser desenvolvidos com base em demandas específicas de cada setor.

TABELA 12_ PLANO DE AÇÃO PARA CONSTRUÇÃO DE TREINAMENTO DIRECIONADO

O quê?	*Treinamento direcionado na unidade "X" a fim de adequar os processos que envolvem tratamento de dados.*
Quem?	*Encarregado pela proteção de dados ou algum membro do comitê multidisciplinar que esteja apto.*
Onde?	*De forma presencial ou* online.
Por quê?	*Porque há processos por área que necessitam de atenção específica*
Como?	*Na forma de* workshops, *palestras educativas ou dinâmicas de treinamento interativas, a exemplo do uso de ferramentas próprias.*
Quando?	*Assim que os processos ou dados forem mapeados.*
Quanto?	*A definir.*

Fonte: elaboração própria.

DICA!

Registre a presença dos participantes nos treinamentos e conduza *quizzes* durante ou após as sessões para que sejam geradas estatísticas sobre a absorção do conteúdo abordado.

CAPACITAÇÃO CONTINUADA_ focada na expansão constante de habilidades por meio do aprendizado contínuo e do aumento do conhecimento. Recomenda-se o uso de estratégias planejadas, periódicas e regulares ao longo do ano.

VOCÊ PODE...

01_ Usar lembretes em forma de pop-up ao acessar sistemas ou ao fazer login nas estações de trabalho;

02_ Enviar e-mails informativos com "pílulas de conhecimento" sobre proteção de dados;

03_ Promover *webinars* ou *workshops* de curta duração;

04_ Conceder incentivos para os colaboradores por meio de gamificação.

ACESSE!

No **Artefato nº 15**, disponibilizamos um **Modelo de Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação** desenvolvido pela Secretaria de Governo Digital que apresenta diretrizes para o desenvolvimento pessoal dentro de uma organização.

Artefato nº 15

PPSI

O Método RNP foi desenvolvido com o objetivo de apoiar instituições no fortalecimento da governança e da gestão de conformidade para proteção de dados pessoais. Para reforçar sua aderência a práticas reconhecidas nacionalmente, cada módulo do Método RNP foi mapeado em relação aos controles previstos no Programa de Proteção à Segurança da Informação (PPSI), uma iniciativa estruturante da Secretaria de Governo Digital que orienta órgãos e entidades da Administração Pública Federal na implementação de medidas de segurança e proteção de dados. Confira a seguir os controles do PPSI abordados neste módulo:

TABELA 13 _ COMPARATIVO ENTRE O MÓDULO SENSIBILIZAÇÃO, EDUCAÇÃO E TREINAMENTO E O *FRAMEWORK* DO PPSI

CONTROLES DO PPSI	ID de identificação
Controle 23_ *conscientização e treinamento*	*23.1; 23.2; 23.3; 23.4*

Fonte: elaboração própria.

MÓDULO MEDIDAS DE SEGURANÇA

Neste módulo você encontrará respostas para as seguintes perguntas:

8.1_ *Quais medidas adotar para garantir a segurança dos dados pessoais?*

8.2_ *Como estruturar uma política de segurança da informação?*

8.3_ *Anonimização e pseudonimização: quais as implicações?*

8.4_ *Como garantir o comprometimento dos colaboradores com as diretrizes?*

Artefatos relacionados:

ARTEFATO Nº 16_ *Checklist de medidas de segurança para ATPP da ANPD*

ARTEFATO Nº 17_ *Modelo de Política de Segurança da Informação do PPSI*

ARTEFATO Nº 18_ *Sugestão de Termo de Responsabilidade para colaboradores*

A Lei Geral de Proteção de Dados Pessoais (LGPD), em seu **artigo 46º**, determina que os agentes de tratamento devem adotar medidas de segurança técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração ou qualquer outro tipo de tratamento inadequado ou ilícito.

Garantir a segurança das informações deve ser um compromisso presente desde a concepção de produtos e serviços até seu ciclo de vida completo. Este módulo apresenta medidas de segurança que podem ser adotadas pelas organizações para garantir conformidade com a LGPD e proteção adequada dos dados pessoais.

8.1_ Quais medidas adotar para garantir a segurança dos dados pessoais?

A proteção dos dados pessoais envolve tanto medidas administrativas quanto tecnológicas. A norma **ABNT NBR ISO/IEC 27701**, extensão da **ISO/IEC 27001 e 27002**, define requisitos e diretrizes de segurança para a gestão da privacidade da informação.

Embora a ABNT NBR ISO/IEC 27701 não seja exigida por lei, ela é considerada uma norma de referência e pode ser adotada voluntariamente por organizações que desejam demonstrar conformidade e compromisso com a segurança da informação. A adoção dessa norma permite que as organizações aprimorem seus processos de gerenciamento de privacidade, aumentando a confiança dos indivíduos na proteção de seus dados pessoais.

O **Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte**, publicado pela ANPD, apresenta sugestões de medidas de segurança administrativas e técnicas, além de medidas relacionadas ao uso de dispositivos móveis e ao serviço em nuvem. O material é endereçado aos agentes de tratamento de pequeno porte que, em razão de seu tamanho e eventuais limitações, muitas vezes não possuem pessoas especializadas em segurança da informação e necessitam aprimorá-la em relação ao tratamento de dados pessoais, mas pode ser útil como referência mínima para todas as organizações.

Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte

ACESSE!

Com o objetivo de facilitar a implementação e verificação das ações necessárias para garantir a segurança dos dados pessoais e assegurar a conformidade com a legislação, o Artefato n° 16 contém um *checklist* elaborado pela ANPD. Embora direcionado para pequenas e médias empresas, este documento pode ser útil também para outras organizações, auxiliando na checagem e adoção de boas práticas de proteção de dados.

Artefato nº 16

Além do documento publicado pela ANPD, recomenda-se observar as práticas propostas pelo Programa de Privacidade e Segurança da Informação (PPSI), incluindo:

01_ Nomear um Gestor de Segurança da Informação, que supervisiona as políticas e práticas de segurança.

02_ ***Instituir um Comitê de Segurança da Informação***, que coordena e monitora a implementação das diretrizes.

03_ Criar uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), que gerencia e responde a incidentes de segurança.

04_ Automatizar o registro de eventos de dados, o que inclui coleta, criação, atualização, exclusão e arquivamento.

05_ Revisar periodicamente os controles de segurança, garantindo um processo contínuo de gerenciamento de riscos.

06_ Gerenciar usuários em sistemas de dados pessoais, desde o registro até o cancelamento de acesso.

07_ Aplicar o princípio do privilégio mínimo, em que cada usuário deve ter apenas os acessos necessários.

08_ Prover autenticação robusta para o processamento de dados pessoais, especialmente dados sensíveis.

09_ Gerenciar o acesso físico a dados e dispositivos, protegendo ambientes onde há dados pessoais, especialmente dados sensíveis.

10_ Realizar transferência de dados por canais criptografados, utilizando ciphers recomendadas, como as verificadas em: **https://www.ssllabs.com/ssltest/**.

11_ Implementar controles de integridade para dados armazenados, permitindo identificar alterações não autorizadas.

12_ Adotar mecanismos de restauração de dados, para casos de perda ou corrupção.

13_ Controlar a impressão e descarte de documentos, garantindo segurança na eliminação de informações.

14_ Considerar medidas de mitigação desde o desenvolvimento de sistemas, antecipando riscos de privacidade e segurança.

15_ Registrar eventos (logs) de acesso e modificação de dados pessoais, incluindo quem acessou, quando, quais dados e as alterações realizadas.

16_ Monitorar proativamente possíveis violações de dados, para resposta rápida e eficaz.

17_ Manter sistema de registro para incidentes de segurança envolvendo dados pessoais, documentando e analisando as violações.

As medidas sugeridas devem ser vistas como boas práticas, a serem complementadas com outras ações identificadas como necessárias para promover a segurança do fluxo de informações da organização.

VEJA!

A Agência da União Europeia para a Cibersegurança (ENISA) disponibiliza o *Awareness Raising in a Box* (AR-in-a-Box), um conjunto de ferramentas projetadas para auxiliar organizações na promoção da conscientização sobre segurança cibernética. O objetivo desse material é fornecer um suporte estruturado para que empresas, órgãos públicos e instituições desenvolvam campanhas educativas e treinem colaboradores para reduzir vulnerabilidades relacionadas ao fator humano.

***"Awareness Raising in a Box"* (AR-in-a-Box)**

8.2_ Como estruturar uma Política de Segurança da Informação?

A Política de Segurança da Informação é um documento essencial para uma organização, pois estabelece as diretrizes e os princípios que regem o tratamento de assuntos relacionados à segurança, incluindo a proteção de dados pessoais. Ela define as regras e os controles que devem ser adotados para garantir a confidencialidade, integridade e disponibilidade das informações da organização, abrangendo todos os serviços, sistemas, pessoas e ambientes onde a informação é tratada.

Além disso, a política inclui a definição dos processos de gerenciamento e gestão da segurança da informação, estabelecendo as responsabilidades dos gerentes e gestores. Esses processos podem envolver a identificação de riscos, a implementação de controles de segurança, a gestão de incidentes de segurança, a conscientização e o treinamento dos funcionários, entre outros aspectos relevantes.

No que diz respeito às operações de tratamento de dados pessoais, caso exista uma tolerância ao risco organizacional definida, conforme indicado pelo PPSI, recomenda-se que essa tolerância seja claramente expressa e comunicada às partes interessadas do órgão.

ACESSE!

Para direcionar organizações que ainda não possuem uma Política de Segurança da Informação formal ou que estão em fase de elaboração, o Artefato nº 17 apresenta um modelo de Política de Segurança da Informação disponibilizado pela Secretaria de Governo Digital (SGD).

Artefato nº 17

8.3_ Anonimização e pseudonimização: quais as implicações?

A anonimização é um processo que torna impossível identificar uma pessoa usando determinados dados. Quando os dados são anonimizados, deixam de ser considerados "dados pessoais" pela Lei Geral de Proteção de Dados Pessoais (LGPD), pois não permitem mais identificar indivíduos específicos. Algumas técnicas de anonimização incluem generalização (como substituir a idade exata por faixas etárias) e supressão (remover informações diretamente identificáveis, como nome e CPF).

Já a pseudonimização é um processo reversível, onde as informações pessoais são substituídas por um código ou pseudônimo. Apesar da aparência anônima, os dados pseudonimizados continuam sendo considerados dados pessoais, pois é possível restabelecer a identificação original com a posse de informações adicionais. Técnicas comuns de pseudonimização incluem o uso de codificação numérica ou criptografia das informações pessoais. Dessa forma, se existente e disponível qualquer meio razoável de reidentificar a pessoa, o dado continuará sendo considerado como pessoal.

Diante disso, conforme estudo técnico preliminar publicado pela Autoridade Nacional de Proteção de Dados (ANPD), é recomendável que as organizações estabeleçam um processo contínuo para avaliar se os métodos utilizados na anonimização permanecem eficazes ao longo do tempo, especialmente devido à evolução tecnológica, que pode facilitar a reidentificação.

ATENÇÃO!

No caso de condução de estudos e pesquisas que envolvam a coleta e o tratamento de dados pessoais, como pesquisas acadêmicas, levantamentos estatísticos, estudos de impacto social e análises de políticas públicas, recomenda-se que eventual divulgação de resultados ou de qualquer excerto não revele, em nenhuma hipótese, informações que possibilitem a identificação direta ou indireta dos indivíduos envolvidos.

Para isso, é possível a aplicação de técnicas adequadas de anonimização, garantindo que os dados divulgados não possam ser revertidos para identificar os titulares. A pseudonimização, quando utilizada, deve ser complementada por controles adicionais, pois, diferentemente da anonimização, ainda permite a reidentificação caso informações complementares sejam acessadas.

8.4_ Como garantir o comprometimento dos colaboradores com as diretrizes?

A segurança das informações e dos dados pessoais não depende apenas de tecnologias e políticas internas, mas também do comprometimento dos colaboradores. Para reforçar esse compromisso, é recomendável a formalização de um **Termo de Responsabilidade para Colaboradores**, onde podem ser definidas diretrizes claras sobre o manuseio de dados e informações dentro da organização.

O Termo de Responsabilidade, apesar de não ser documento obrigatório, tem como objetivo garantir que os colaboradores compreendam suas obrigações no tratamento de dados pessoais, respeitando a Política de Segurança da Informação, bem como demais diretrizes internas da instituição sobre segurança da informação e proteção de dados pessoais.

ACESSE!

No Artefato nº 18, disponibilizamos uma sugestão do documento de Termo de Responsabilidade para colaboradores que pode ser adaptado às particularidades de cada organização.

Artefato nº 18

PPSI

O Método RNP foi desenvolvido com o objetivo de apoiar instituições no fortalecimento da governança e da gestão de conformidade para proteção de dados pessoais. Para reforçar sua aderência a práticas reconhecidas nacionalmente, cada módulo do Método RNP foi mapeado em relação aos controles previstos no Programa de Proteção à Segurança da Informação (PPSI), uma iniciativa estruturante da Secretaria de Governo Digital que orienta órgãos e entidades da Administração Pública Federal na implementação de medidas de segurança e proteção de dados. Confira a seguir os controles do PPSI abordados neste módulo:

TABELA 14_ COMPARATIVO ENTRE O MÓDULO MEDIDAS DE SEGURANÇA E O *FRAMEWORK* DO PPSI

CONTROLES DO PPSI	ID DE IDENTIFICAÇÃO
Controle 20_ *Finalidade e legitimidade*	*20.7; 20.8*
Controle 22_ *Políticas, processos e procedimentos*	*22.1; 22.3; 22.6*
Controle 24_ *Minimização dos dados*	*24.7; 24.8; 24.9; 24.11; 24.12*
Controle 25_ *Gestão do tratamento*	*25.1; 25.9*
Controle 31_ *Segurança aplicada a privacidade*	*31.1; 31.2; 31.3; 31.4; 31.5; 31.6; 31.7; 31.8; 31.9; 31.10; 31.13; 31.14; 31.15; 31.16; 31.17*

Fonte: elaboração própria.

MÓDULO RESPOSTA A INCIDENTES

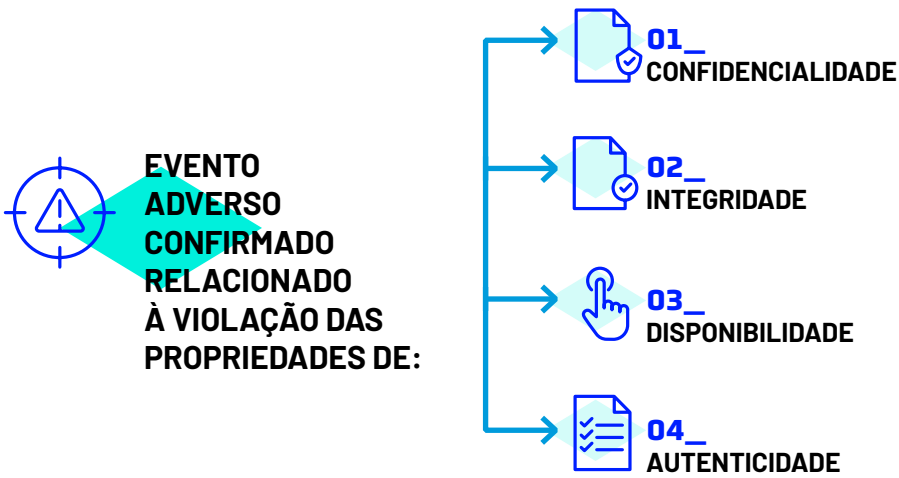
Neste módulo você encontrará respostas para as seguintes perguntas:

Artefatos relacionados:

ARTEFATO Nº 19_ *Formulário de Comunicação de Incidente de Segurança com Dados Pessoais da ANPD*

A ANPD, por meio do Regulamento de Comunicação de Incidente de Segurança (RCIS), define incidente de segurança como:

FIGURA 20_ INCIDENTE DE SEGURANÇA



Fonte: adaptado do art. 3º de Autoridade Nacional de Proteção de Dados (2024c).

O QUE SÃO ESSAS PROPRIEDADES?

CONFIDENCIALIDADE

Refere-se à proteção dos dados contra acessos não autorizados, garantindo que apenas pessoas ou sistemas autorizados possam visualizar ou utilizar as informações.

Exemplo de violação:

Um banco de dados contendo dados pessoais é exposto na internet sem proteção, permitindo que qualquer pessoa acesse os dados sem permissão.

INTEGRIDADE

Diz respeito à garantia de que os dados não sejam alterados, manipulados ou corrompidos de forma indevida, seja acidentalmente ou por ação maliciosa.

Exemplo de violação:

Um hacker invade um sistema financeiro e modifica os valores das transações para desviar dinheiro para outra conta.

DISPONIBILIDADE

Assegura que os dados estejam acessíveis sempre que necessário. Se a disponibilidade for comprometida, usuários legítimos podem ser impedidos de acessar suas informações.

Exemplo de violação:
Um ataque de negação de serviço (DDoS) sobrecarrega os servidores de um serviço de e-mail, impedindo que os usuários enviem ou recebam mensagens.

AUTENTICIDADE

Relaciona-se à garantia de que os dados são legítimos e não foram adulterados ou falsificados.

Exemplo de violação:
Um criminoso cria uma página falsa de um banco para induzir clientes a inserirem seus dados de login, *permitindo o roubo de credenciais.*

Como visto acima, um incidente de segurança pode ocorrer de diversas formas, como acessos indevidos, vazamento de dados, ataques cibernéticos, exclusão acidental de informações ou falhas técnicas que comprometam a privacidade dos titulares. A resposta rápida e eficiente a esses eventos é essencial para reduzir impactos e manter a conformidade com a LGPD.

9.1_ Como instituir um Plano de Resposta a Incidentes?

A implementação de um **Plano de Resposta a Incidentes** é essencial para garantir que as organizações estejam preparadas para lidar com eventos que possam comprometer a segurança dos dados pessoais. Um plano bem estruturado permite uma resposta rápida e eficaz, minimizando danos aos titulares e garantindo conformidade com a LGPD.

Neste plano, sugerimos a inclusão, no mínimo, de:

TABELA 15_ SUGESTÃO BÁSICA PARA O PLANO DE RESPOSTA A INCIDENTES

DEFINIÇÃO DE RESPONSABILIDADES	*Designar pessoas e/ou equipes responsáveis por cada obrigação relacionada ao gerenciamento e resposta a incidentes, garantindo uma abordagem multidisciplinar.*
PROCEDIMENTOS DE DETECÇÃO E AVALIAÇÃO	*Diretrizes claras para detectar e avaliar possíveis violações das propriedades que caracterizam um incidente. Isso envolve a implementação de ferramentas de monitoramento, auditorias periódicas e mecanismos para que colaboradores possam relatar suspeitas de incidentes de maneira segura.*

FLUXOS DE CONTENÇÃO E MITIGAÇÃO	*Uma vez identificado um incidente, é fundamental contar com diretrizes para conter o impacto e mitigar os danos, definindo ações imediatas e os responsáveis pela condução.*
PROCEDIMENTOS DE COMUNICAÇÃO	*Quem será o responsável por avaliar se a comunicação é necessária, prazos e formato para a comunicação à ANPD e aos titulares, bem como as informações mínimas necessárias nessas comunicações.*
PLANO DE RECUPERAÇÃO E LIÇÕES APRENDIDAS	*Fluxos para restaurar os sistemas e reforçar as medidas de segurança, bem como a realização de uma análise pós-incidente, identificando falhas e oportunidades de melhoria para prevenir novas ocorrências.*
TESTES E AVALIAÇÕES CONTÍNUAS	*Uma boa prática é a realização de treinamentos e **simulação de incidentes**. Capacitar os colaboradores é essencial para garantir que saibam como reagir rapidamente a um incidente de segurança.*

Fonte: elaboração própria.

ACESSE!

A Secretaria de Governo Digital (SGD) disponibiliza o Guia de Resposta a Incidentes de Segurança. Este guia apresenta boas práticas para que instituições e profissionais de segurança da informação tratem incidentes cibernéticos, com foco específico em incidentes que envolvem dados pessoais.

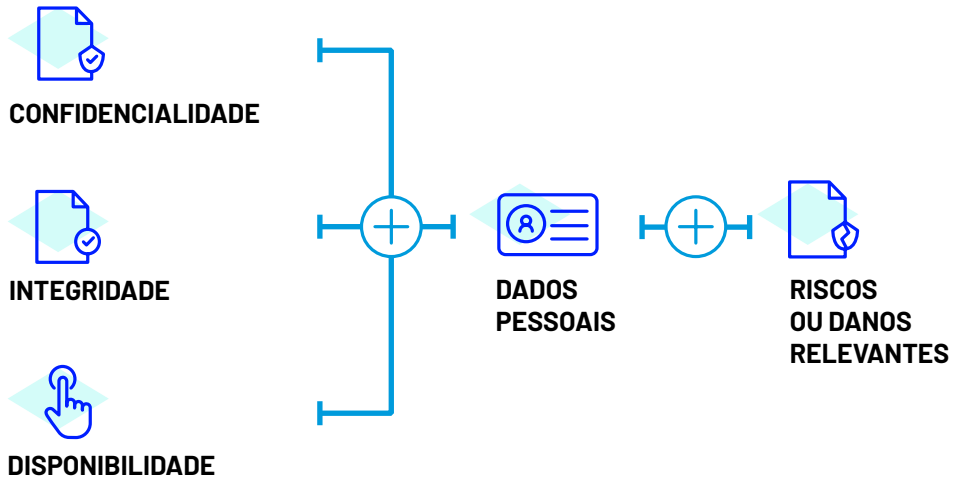
Guia de Resposta a Incidentes de Segurança

9.2_ Quando comunicar um incidente envolvendo dados pessoais?

A Lei Geral de Proteção de Dados Pessoais (LGPD), em seu **artigo 48º**, estabelece a obrigação para o controlador de comunicar incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais.

No **Regulamento de Comunicação de Incidente de Segurança (RCIS)**, esclarece-se que a comunicação à ANPD e aos titulares deve ocorrer quando três condições cumulativas forem atendidas.

FIGURA 21_ CRITÉRIOS CUMULATIVOS PARA COMUNICAR UM INCIDENTE



Fonte: Autoridade Nacional de Proteção de Dados (2022b).

O QUE CARACTERIZA RISCO OU DANO RELEVANTE AOS TITULARES?

AFETAR SIGNIFICATIVAMENTE OS INTERESSES E DIREITOS FUNDAMENTAIS DOS TITULARES

Situações em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

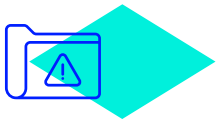
ENVOLVER, PELO MENOS, UM DOS SEGUINTES CRITÉRIOS:

- **DADOS PESSOAIS SENSÍVEIS**
- **DADOS DE CRIANÇAS, DE ADOLESCENTES OU DE IDOSOS**
- **DADOS FINANCEIROS**
- **DADOS DE AUTENTICAÇÃO EM SISTEMAS**
- **DADOS PROTEGIDOS POR SIGILO LEGAL, JUDICIAL OU PROFISSIONAL**
- **DADOS EM LARGA ESCALA***

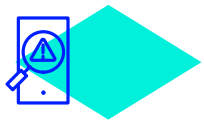
*considerando-se número significativo de titulares, volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.

FIGURA 22_ EXEMPLOS DE INCIDENTES CAPAZES DE GERAR RISCO OU DANO RELEVANTE AOS TITULARES

A invasão de uma rede de computadores de uma instituição financeira por um agente malicioso que realize a cópia não autorizada de uma base de dados contendo dados pessoais dos correntistas, tais como extratos bancários, números de cartões de crédito e senhas viola o sigilo bancário dos titulares e os expõe a risco de fraudes e danos morais e materiais.



A indisponibilidade prolongada de um sistema utilizado por uma rede hospitalar em razão de um incidente de sequestro de dados, impedindo o acesso aos dados dos pacientes ou a realização de procedimentos médicos, pode expor dados pessoais sensíveis dos titulares e causar-lhes riscos ou danos à saúde.



A perda ou roubo de documentos ou dispositivos de armazenamento de dados que contenham dados pessoais protegidos por sigilo profissional, cópia de documentos de identificação oficial e dados de contato dos titulares pode expô-los a riscos reputacionais e de sofrer fraudes financeiras.

Fonte: Autoridade Nacional de Proteção de Dados (2022b).

Conforme o artigo 6º e o artigo 9º do Regulamento de Comunicação de Incidente de Segurança, a comunicação à ANPD e ao(s) titular(es) deverá ser realizada pelo controlador no prazo de **(3) três dias úteis**, ressalvada a existência de prazo para comunicação previsto em legislação específica. Esse prazo é contado em dobro para agentes de pequeno porte.

Se não for possível dispor de informações completas a respeito do incidente, a comunicação à ANPD poderá ser realizada em etapas: **preliminar e complementar**.

A impossibilidade de realizar a comunicação completa deve ser devidamente justificada pela instituição. **As informações podem ser complementadas, de maneira fundamentada, no prazo de 20 (vinte) dias úteis, a contar da data da comunicação**. A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar, por meio de petição intercorrente.

Assim, em caso de incidentes de segurança envolvendo dados pessoais, é fundamental que as organizações tenham um processo bem definido, testado e validado para gerenciar essas situações.

9.3_ Como comunicar um incidente à ANPD?

A comunicação de incidentes de segurança à ANPD deve ser realizada pelo Encarregado ou por um representante legalmente constituído do controlador, por:

Peticionamento eletrônico no sistema SEI da ANPD

A ANPD possui um **portal específico sobre comunicação de incidentes de segurança** onde é possível encontrar orientações e um passo a passo do procedimento de peticionamento.

Comunicação de incidentes de segurança

ACESSE!

No Artefato nº 19, disponibilizamos o Formulário de Comunicação de Incidente de Segurança com Dados Pessoais disponibilizado pela ANPD. Ali, é possível compreender todos os elementos necessários no conteúdo da comunicação.

Artefato nº 19

9.4_ Como comunicar um incidente aos titulares afetados?

A comunicação de um incidente deve ser feita em **linguagem simples e de fácil entendimento**, de forma **individual** e **diretamente** aos titulares, sempre que possível. Pode ser realizada por quaisquer meios tais como e-mail, SMS, carta ou mensagem eletrônica e, preferencialmente, através do canal já habitualmente utilizado pelo agente para se comunicar com o titular.

Se, apesar de confirmada a ocorrência do incidente, não for possível individualizar os titulares afetados, pode ser necessário comunicar a todos cujos dados estejam presentes na base de dados violada ou comunicar a ocorrência do incidente de forma ampla pelos meios de divulgação disponíveis (sítio eletrônico, aplicativos, mídias sociais e canais de atendimento ao titular), mantendo-a pelo período de, no mínimo, três meses.

Informações mínimas que devem estar contidas na comunicação ao(s) titular(es):

01_ Descrição da natureza e da categoria de dados pessoais afetados;

02_ Medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

03_ Riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

04_ Motivos da demora, no caso de a comunicação não ter sido no prazo;

05_ Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;

06_ Data do conhecimento do incidente de segurança; e

07_ Contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

9.5_ Como elaborar um relatório de tratamento de incidente?

O **Relatório de Tratamento de Incidente** é documento elaborado pelo controlador que contém cópias, em meio físico ou digital, de dados e informações relevantes para descrever o incidente e as providências adotadas para reverter ou mitigar os seus efeitos.

É importante que a instituição mantenha o registro de incidentes de segurança ocorridos, **inclusive daqueles não comunicado à ANPD e aos titulares**, pelo prazo mínimo de **5 (cinco) anos**, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

De acordo com o Regulamento de Comunicação de Incidente de Segurança, o registro do incidente precisa conter, no mínimo:

01_ A data de conhecimento do incidente;

02_ A descrição geral das circunstâncias em que o incidente ocorreu;

03_ A natureza e a categoria de dados afetados;

04_ O número de titulares afetados;

05_ A avaliação do risco e os possíveis danos aos titulares;

06_ As medidas de correção e mitigação dos efeitos do incidente, quando aplicável;

07_ A forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e

08_ Os motivos da ausência de comunicação, quando for o caso.

PPSI

O Método RNP foi desenvolvido com o objetivo de apoiar instituições no fortalecimento da governança e da gestão de conformidade para proteção de dados pessoais. Para reforçar sua aderência a práticas reconhecidas nacionalmente, cada módulo do Método RNP foi mapeado em relação aos controles previstos no Programa de Proteção à Segurança da Informação (PPSI), uma iniciativa estruturante da Secretaria de Governo Digital que orienta órgãos e entidades da Administração Pública Federal na implementação de medidas de segurança e proteção de dados. Confira a seguir os controles do PPSI abordados neste módulo:

TABELA 16_ COMPARATIVO ENTRE O MÓDULO RESPOSTA A INCIDENTES E O *FRAMEWORK* DO PPSI

CONTROLES DO PPSI	ID DE IDENTIFICAÇÃO
Controle 22_ *Políticas, processos e procedimentos*	*22.10; 22.11*
Controle 29_ *Abertura, transparência e notificação*	*29.12*
Controle 31_ *Segurança aplicada a privacidade*	*31.18*

Fonte: elaboração própria.

CONCLUSÃO

O Método RNP de conformidade à LGPD foi desenvolvido para oferecer um caminho estruturado e acessível para que instituições possam implementar um Programa de Governança em Privacidade alinhado às melhores práticas nacionais e internacionais. O Método RNP é dinâmico e adaptável, permitindo que cada organização avance conforme sua maturidade em proteção de dados.

O Método RNP busca incentivar uma cultura de privacidade e proteção de dados dentro das instituições. A conformidade com a LGPD vai além do cumprimento de obrigações legais; trata-se de um diferencial estratégico para organizações que desejam construir relações de confiança com titulares de dados, parceiros e órgãos reguladores.

Reforçamos a importância da melhoria contínua e do compromisso institucional para garantir que a proteção de dados seja uma prioridade sustentável e integrada à estratégia organizacional.

ACESSE!

O ANEXO comparativo do Método RNP com o PPSI

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Banner de cookies da página da ANPD.** Brasília, DF:ANPD, [202-]. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Centrais de conteúdo**. Brasília, DF:ANPD, 2025a. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo. Acesso em: 30 jan. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Checklist de medidas de segurança para agentes de tratamento de pequeno porte**. Brasília, DF: ANPD, 2021a. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Comunicação de incidente de segurança**, Brasília, DF: ANPD, 2022b. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Denúncias ou Petições de titular**, Brasília, DF: ANPD, 2024a. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-peticao-de-titular. Acesso em: 30 jan. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Glossário ANPD**. Brasília, DF: ANPD, 2025b. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/glossario-anpd. Acesso em: 30 jan. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo cookies e proteção de dados pessoais**. Brasília, DF: ANPD, 2022c. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo hipóteses legais de tratamento de dados pessoais legítimo interesse**. Brasília, DF: ANPD, 2024b. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Brasília, DF: ANPD, 2022d. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte**. Brasília, DF: ANPD, 2021b. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo tratamento de dados pessoais pelo poder público**. Brasília, DF: ANPD, 2023b. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas**. Brasília, DF: ANPD, 2023a. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Modelo de Registro de operações de tratamento de dados pessoais para Agentes de Tratamento de Pequeno Porte (ATPP)**. [2021]. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/modelo_de_ropa_para_atpp.pdf. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais**. Brasília, DF: ANPD, 2023c.Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd/relatorio-de-impacto-a-protecao-de-dados-pessoais/#p9. Acesso em: 06 fev. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. Brasília, DF: ANPD, 2023d. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 23 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 1, de 28 de outubro de 2021.** Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Brasília, DF: ANPD, 2021c. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021#:~:text=Aprova%20o%20Regulamento%20do%20Processo,Nacional%20de%20Prote%C3%A7%C3%A3o%20de%20Dados.&text=OUTUBRO%20DE%202021-,Aprova%20o%20Regulamento%20do%20Processo%20de%20Fiscaliza%C3%A7%C3%A3o%20e%20do%20Processo,Nacional%20de%20Prote%C3%A7%C3%A3o%20de%20Dados. Acesso em: 30 jan. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 15, de 24 de abril de 2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança. Brasília, DF: ANPD, 2024c. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 18, de 16 de julho de 2024**. Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. Brasília, DF: ANPD, 2024d. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 19, de 23 de agosto de 2024**. Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das

cláusulas-padrão contratuais. Brasília, DF: ANPD, 2024e. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: ANPD, 2022e. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 04 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.** Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Brasília, DF: ANPD, 2023e. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 30 jan. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 7, de 17 de agosto de 2023.** Aprova a Política de Comunicação Social da Autoridade Nacional de Proteção de Dados. Brasília, DF: ANPD, 2023f. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/ResoluoCD.ANPD.7AprovaaPolticadeComunicaoSocial.pdf. Acesso em: 30 jan. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução nº 23, de 9 de dezembro de 2024.** Aprova a Agenda Regulatória da ANPD para o biênio 2025-2026. Brasília, DF: ANPD, 2024f. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/governanca/governanca-estrategica/resolucao-no-23-de-9-12-2024-agenda-regulatoria-2025-2026.pdf. Acesso em: 30 jan. 2025.

AUTORITÉ DE PROTECTION DES DONNÉES. **Vision et mission**. c2025. Disponível em: https://www.autoriteprotectiondonnees.be/professionnel/l-autorite/vision-et-mission. Acesso em: 30 jan. 2025.

BRASIL. Decreto-Lei nº 4.657, de 4 de setembro de 1942. **Diário Oficial da União:** seção 1, Brasília, DF, 9 set. 1942. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm. Acesso em: 30 jan. 2025.

BRASIL. Decreto nº 8.936, de 19 de dezembro de 2016. Institui a Plataforma de Cidadania Digital. **Diário Oficial da União**: seção 1, Brasília, DF, 20 dez. 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8936.htm. Acesso em: 30 jan. 2025.

BRASIL. Emenda Constitucional º 115, de 10 de fevereiro de 2022. **Diário Oficial da União**: seção 1, Brasília, DF, p. 2, 11 fev. 2022a. Disponível em: https://www.in.gov.br/en/web/dou/-/emenda-constitucional-n-115-379516387. Acesso em: 30 jan. 2025.

BRASIL. Instrução Normativa nº 1, de 27 de maio de 2020. **Diário Oficial da União**: seção 1, Brasília, DF, p. 13, 28 mai. 2020b. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215. Acesso em: 30 jan. 2025.

BRASIL. Instrução Normativa nº 3, de 09 de junho de 2017. **Diário Oficial da União**: seção 1, Brasília, DF, 12 jun. 2017. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/19111706/do1-2017-06-12-instrucao-normativa-n-3-de-9-de-junho-de-2017-19111304. Acesso em: 30 jan. 2025.

BRASIL. Instrução Normativa nº 117, de 19 de novembro de 2020. **Diário Oficial da União**: seção 1, Brasília, DF, 20 nov. 2020c. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596. Acesso em: 06 fev. 2025.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011**.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. **Diário Oficial da União**: seção 1, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 30 jan. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. **Diário Oficial da União:** seção 1, Brasília, DF, edição 157, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/L13709compilado.htm. Acesso em: 04 out. 2024.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. **Encarregado pelo Tratamento de Dados Pessoais**. Brasília, DF: MCTI, 2024a. Disponível em: https://www.gov.br/mcti/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd/encarregado. Acesso em: 27 set. 2024.

BRASIL. Ministério da Economia. Comitê Central de Governança de Dados. **Guia de Boas Práticas:** Lei Geral de Proteção de Dados Pessoais. Brasília, DF: ME, 2020a. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 04 out. 2024.

BRASIL. Ministério da Economia. Comitê Central de Governança de Dados. **Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília, DF: ME, 2022b. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 30 jan. 2025.

BRASIL. Ministério da Economia. Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022. Dispõe sobre as contratações de Tecnologia da Informação e Comunicação no âmbito da administração pública federal. **Diário Oficial da União**, Brasília, DF, 29 dez. 2022c. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/instrucao-normativa-sgd-me-no-94-de-23-de-dezembro-de-2022. Acesso em: 30 jan. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de resposta a incidentes de segurança**. Brasília, DF: SGD, 2024d. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf. Acesso em: 04 out. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia sobre privacidade desde a concepção e por padrão**. Brasília, DF: SGD, 2024e. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_privacidade_concepcao.pdf. Acesso em: 04 out. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Inventário de dados pessoais**. Brasília, DF: SGD, 2023a. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_inventario_dados_pessoais.pdf. Acesso em: 04 out. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 852. **Diário Oficial da União:** Seção 1, Brasília, DF, n. 62, p. 92, 30 mar. 2023c. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. Acesso em: 30 jan. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria MGI nº 7.601. **Diário Oficial da União:** Seção 1, Brasília, DF, n. 224, p. 36, 27 nov. 2023d. Disponível em: https://pesquisa.in.gov.br/imprensa/servlet/INPDFViewer?jornal=515&pagina=36&data=27/11/2023&captchafield=firstAccess. Acesso em: 06 fev. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Programa de Governança em Privacidade.** Brasília, DF: SGD, 2024g. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_programa_governanca_privacidade.pdf. Acesso em: 04 out. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Programa de Privacidade e Segurança da Informação (PPSI)**. Brasília, DF: SGD, 2024h. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/programa-de-privacidade-e-seguranca-da-informacao-ppsi. Acesso em: 04 out. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. Brasília, DF: SGD, 2024i. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_template_ripd.docx. Acesso em: 04 out. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Modelo de Política de Segurança da Informação.** Brasília, DF: SGD, 2024f. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_politica_seguranca_informacao.pdf. Acesso em: 30 jan. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Termo de uso e Política de Privacidade**. Brasília, DF: SGD, 2023e. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_termo_uso_politica_privacidade.pdf. Acesso em: 04 out. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Modelo de Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação**. Brasília, DF: SGD, 2023b. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_politica_desenvolvimento_pessoas.pdf. Acesso em: 30 jan. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de Requisitos e Obrigações Quanto a Privacidade e à Segurança da Informação.** Brasília, DF: SGD, 2024c. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_requisitos_obrigacoes.pdf. Acesso em: 30 jan. 2025.

BRASIL. Supremo Tribunal Federal. **Guia de Elaboração de Inventário de Dados Pessoais**. Brasília, DF: STF, 2024b. Disponível em: https://bibliotecadigital.stf.jus.br/xmlui/handle/123456789/6396. Acesso em: 22 out. 2024.

BRASIL. Supremo Tribunal Federal. STF intensifica medidas para cumprimento da Lei Geral de Proteção de Dados: Presidente da Corte designou encarregado de dados e criou grupo de trabalho para apoiar as atividades do Tribunal no cumprimento da norma. **Notícias,** Brasília, DF, 08 ago. 2024j. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-intensifica-medidas-para-cumprimento-da-lgpd/. Acesso em: 29 set. 2024.

CAVOUKIAN, Ann. **Privacy by Design:** The 7 Foundational Principles. [2010]. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design—-foundational-principles.pdf. Acesso em: 28 out. 2024.

CONSELHO FEDERAL DE QUÍMICA. **Contratação de empresa para prestação de serviços de consultoria especializada no levantamento e mapeamento de processos e sistemas que tratam dados pessoais visando à construção de programa de conformidade à lei Geral de Proteção de Dados – LGPD, contemplando o monitoramento do plano de ação, uma vez que deverá haver cronograma de execução para a implantação da LGPD por todos os entes do Sistema CFQ/CRQs**. [Termo de Referência]. Brasília, DF: CFQ, 2021. Disponível em: https://cfq.org.br/wp-content/uploads/2021/06/Termo-de-Refer%C3%AAncia-LGPD.pdf. Acesso em: 01 out. 2024.

CONTROLADORIA-GERAL DA UNIÃO. **Enunciado nº 4/2022 – CGU.** Interpretação da Controladoria-Geral da União sobre a aplicação da Lei Geral de Proteção de Dados (LGPD) na administração pública. Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/decisoes/enunciado-no-4-2022-cgu/view. Acesso em: 30 jan. 2025.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. **Cursos**. Brasília, DF: ENAP, 2024. Disponível em: https://www.enap.gov.br/pt/cursos. Acesso em: 27 set. 2024.

EUROPEAN DATA PROTECTION BOARD. **Guidelines on Transparency under Regulation 2016/679.** 2018. Disponível em: https://ec.europa.eu/newsroom/article29/items/622227/en. Acesso em: 30 jan. 2025.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **AR-in-a-Box:** Awareness Raising in a Box. c2025. Disponível em: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/ar-in-a-box. Acesso em: 30 jan. 2025.

FINANCIADORA DE ESTUDOS E PROJETOS. **Pregão Eletrônico FINEP 09/2021**. Contratação de fornecedores de serviços de Consultoria para atender às necessidades de adequação da Finep à Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), em conformidade com as especificações, os padrões técnicos de desempenho e de qualidade estabelecidos no Termo de Referência (TR) e seus anexos. Brasília, DF: FINEP, 2021. Disponível em: http://www.finep.gov.br/licitacoes-e-contratos/cadastrodelicitaes/523. Acesso em: 01 out. 2024.

FUNDAÇÃO OSWALDO CRUZ. **LGPD**: Fale com os encarregados de dados. [2022]. Disponível em: https://portal.fiocruz.br/lgpd-fale-com-os-encarregados-de-dados#:~:text=A%20encarregada%20titular%20de%20Dados,Rodrigo%20Murtinho%20de%20Martinez%20Torres. Acesso em: 28 set. 2024.

FUTURE OF PRIVACY FORUM. **Privacy metrics report**. Washington, D.C.: Future of Privacy Forum, 2022. Disponível em: https://fpf.org/wp-content/uploads/2022/03/FPF-PrivacyMetricsReport-R9-Digital.pdf. Acesso em: 30 jan. 2025.

INFORMATION COMMISSIONER'S OFFICE. **Best interests of the child**. London: ICO, [2021]. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/ Acesso em: 28 set. 2024.

INFORMATION COMMISSIONER'S OFFICE. **Information Commissioner's Annual Report and Financial Statements**: 2015/16. London: ICO, 2016.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Governança Corporativa**. São Paulo. [2023]. Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 30 jan. 2025

INSTITUTO FEDERAL DO PARANÁ. **Cursos e vídeos**. Paraná: IFP, 2023. Disponível em: https://ifpr.edu.br/acesso-a-informacao/lei-geral-de-protecao-de-dados/cursos-e-videos/. Acesso em: 29 set. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27701:2019 – **Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.** Geneva: ISO, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001**:2022. Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Genebra: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **Standards**. Disponível em: https://www.iso.org/standards.html. Acesso em: 30 jan. 2025.

ISACA. **COBIT 2019 Framework:** Introduction and Methodology. Estados Unidos, 2018.

MATO GROSSO DO SUL. Governo do Estado. **Modelo de termo de referência para projeto de adequação à lei geral de proteção de dados para órgãos e entidades do poder executivo estadual**. Mato Grosso do Sul, [2023]. Disponível em: https://www.lgpd.ms.gov.br/wp-content/uploads/2023/01/Minuta-de-Termo-de-Referencia-LGPD-MS.pdf. Acesso em: 01 out. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Nist Cybersecurity Framework**. U.S. Department of Commerce, 2025. Disponível em: https://www.nist.gov/cyberframework. Acesse: 30 jan. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Nist Privacy Framework:** a tool for improving privacy through enterprise risk management, version 1.0. U.S. Department of Commerce, 2020. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf. Acesso em: 30 jan. 2025.

PARÁ DE MINAS. Câmara Municipal. **Contratação de empresa especializada na prestação de serviço técnico especializado de desenvolvimento e assessoria para implementação de programa/projeto de adequação à Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, de 14 de agosto de 2018 e demais alterações**. [Termo de Referência]. Pará de Minas, MG, 2022. Disponível em: https://www.parademinas.mg.leg.br/app-home/arquivos/licitacoes/330/1528/1207136420.pdf. Acesso em: 01 out. 2024.

SEBRAE. **Encarregado de Proteção de Dados Pessoais**. Brasília, DF, SEBRAE, 2024. Disponível em: https://sebrae.com.br/sites/PortalSebrae/LGPD#encarregados. Acesso em: 28 set. 2024.

TRAINING DATA PROTECTION AUTHORITIES AND DATA PROTECTION OFFICERS – T4DATA. **The DPO Handbook**. 2019. Disponível em: https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf. Acesso em: 06 fev. 2025.

UNIVERSIDADE FEDERAL DE OURO PRETO. **Proteção de dados pessoais – LGPD**. Ouro Preto: UFOP, [2021]. Disponível em: https://lgpd.ufop.br/contato. Acesso em: 28 set. 2024.

UNIVERSITY STANFORD. University Privacy Office serves as an advocate for the responsible use of personal data. **Stanford Report**, Stanford, 19 fev. 2021. Disponível em: https://news.stanford.edu/stories/2021/02/university-privacy-office-serves-advocate-responsible-use-personal-data. Acesso em: 28 set. 2024.

ANEXO _

COMPARATIVO COM O *FRAMEWORK* DO PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

	MÓDULO GOVERNANÇA	MÓDULO MAPEAMENTO DE DADOS	MÓDULO GESTÃO DE RISCOS	MÓDULO TRANSPARÊNCIA NO TRATAMENTO DE DADOS PESSOAIS	MÓDULO GESTÃO DE TERCEIROS	MÓDULO ATENDIMENTO DE TITULARES	MÓDULO SENSIBILIZAÇÃO, EDUCAÇÃO E TREINAMENTO	MÓDULO MEDIDAS DE SEGURANÇA	MÓDULO RESPOSTA A INCIDENTES
CONTROLE 19_ INVENTÁRIO E MAPEAMENTO		19.1; 19.2; 19.3; 19.4; 19.5; 19.6; 19.7; 19.8; 19.9; 19.10; 19.11; 19.12; 19.13; 19.14							
CONTROLE 20_ FINALIDADE E HIPÓTESES LEGAIS		20.6; 20.9	20.1; 20.2; 20.3; 20.4; 20.5; 20.14	20.10; 20.11; 20.12; 20.13				20.7; 20.8	
CONTROLE 21_ GOVERNANÇA	21.1; 21.2; 21.3; 21.4; 21.6; 21.7; 21.9; 21.10		21.8		21.5				
CONTROLE 22_ POLÍTICAS, PROCESSOS E PROCEDIMENTOS	22.2; 22.5; 22.8; 22.12	22.9	22.7		22.4			22.1; 22.3; 22.6	22.10; 22.11
CONTROLE 23_ CONSCIENTIZAÇÃO E TREINAMENTO							23.1; 23.2; 23.3; 23.4		
CONTROLE 24_ MINIMIZAÇÃO DE DADOS			24.1; 24.2; 24.3; 24.4; 24.5; 24.6; 24.10	24.13; 24.14; 24.15				24.7; 24.8; 24.9; 24.11; 24.12	
CONTROLE 25_ GESTÃO DO TRATAMENTO		25.5; 25.6; 25.7; 25.8	25.2; 25.3			25.4		25.1; 25.9	

	MÓDULO GOVERNANÇA	MÓDULO MAPEAMENTO DE DADOS	MÓDULO GESTÃO DE RISCOS	MÓDULO TRANSPARÊNCIA NO TRATAMENTO DE DADOS PESSOAIS	MÓDULO GESTÃO DE TERCEIROS	MÓDULO ATENDIMENTO DE TITULARES	MÓDULO SENSIBILIZAÇÃO, EDUCAÇÃO E TREINAMENTO	MÓDULO MEDIDAS DE SEGURANÇA	MÓDULO RESPOSTA A INCIDENTES
CONTROLE 26_ ACESSO E QUALIDADE			26.8; 26.9; 26.10		26.12	26.1; 26.2; 26.3; 26.4; 26.5; 26.6; 26.7; 26.11			
CONTROLE 27_ COMPARTILHAMENTO, TRANSFERÊNCIA E DIVULGAÇÃO		27.1; 27.2; 27.5			27.3; 27.4				
CONTROLE 28_ SUPERVISÃO EM TERCEIROS					28.1; 28.2; 28.3; 28.4; 28.5; 28.6; 28.7; 28.8; 28.9; 28.10; 28.11; 28.12; 28.13				
CONTROLE 29_ ABERTURA, TRANSPARÊNCIA E NOTIFICAÇÃO				29.1; 29.2; 29.3; 29.4; 29.5; 29.6; 29.7; 29.8; 29.9; 29.10; 29.11					29.12
CONTROLE 30_ AVALIAÇÃO DE IMPACTO, MONITORAMENTO E AUDITORIA	30.9; 30.10; 30.11; 30.12	30.8	30.1; 30.2; 30.3; 30.4; 30.5; 30.6; 30.7						
CONTROLE 31_ SEGURANÇA APLICADA A PRIVACIDADE			31.11; 31.12					31.1; 31.2; 31.3; 31.4; 31.5; 31.6; 31.7; 31.8; 31.9; 31.10; 31.13; 31.14; 31.15; 31.16; 31.17	31.18

Fale conosco, capacite suas equipes e impulsione o processo de conformidade da sua instituição.

RNP 0800 722 0216
www.rnp.br

ESSE MATERIAL AJUDOU VOCÊ?
COMPARTILHE ESSE E-BOOK
E NOS ACOMPANHE EM
NOSSAS REDES SOCIAIS.