

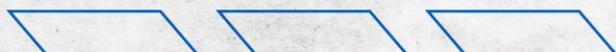


Modelo de Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação

Programa de Privacidade e
Segurança da Informação – PPSI



Versão 1.1
Brasília, abril de 2025



MODELO DE POLÍTICA DE DESENVOLVIMENTO DE PESSOAS EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra de Estado

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE

Marta Juvina de Medeiros

Coordenadora-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Anderson Souza de Araújo

Ivaldo Jeferson de Santana Castro

Rafael da Silva Ribeiro

Raphael César Estevão

Equipe Revisora

Adriano de Andrade Moura

Francisco de Assis Fialho Henriques

Rodrigo Duran Lima

Rogério Vinicius Matos Rocha

Sumaid Andrade de Albuquerque

Equipe Técnica de Revisão - Versão 1.1

Adriano de Andrade Moura

Anderson Souza de Araújo

Andressa Vieira Bueno Popinigis

Bruno Pierre Rodrigues de Souza

Ivaldo Jeferson de Santana Castro

Leonard Keyzo Yamaoka Batista

Marta Jovina de Medeiros
Raphael César Estevão



Histórico de versões

Data	Versão	Descrição	Autor
18/12/2023	1.0	Modelo de Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação.	Equipe Técnica de Elaboração.
15/04/2025	1.1	Atualização para padronização da diagramação do documento. Ajustes pontuais do texto nas seções Termos e Definições e Disposições Gerais. Reestruturação da seção Declarações da política. Adequação do Modelo à Resolução CD/ANPD N° 18, de 16 de julho de 2024.	Equipe Técnica de Revisão.



Sumário

1	Aviso preliminar e agradecimentos	6
2	Introdução	8
3	Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação	10
4	Propósito	11
5	Escopo	12
6	Termos e definições	13
7	Declarações da política	15
8	Referências bibliográficas	19
9	Anexo I	22



1 Aviso preliminar e agradecimentos

O presente modelo, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal – APF, visa a auxiliar na elaboração de uma Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação, em atendimento ao previsto no art. 50 da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais – LGPD, que estabelece que os controladores e operadores, no âmbito de suas competências, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Adicionalmente, a elaboração da Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de desenvolvimento pessoal.

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

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

- a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST;
- b) não se manifesta em nome da Autoridade Nacional de Proteção de Dados Pessoais – ANPD nem do Gabinete de Segurança Institucional da Presidência da República – GSI/PR;
- c) não é coautora das publicações internacionais abordadas;
- d) não assume responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente modelo; e
- e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referências bibliográficas” deste documento.



Um agradecimento especial deve ser registrado ao CIS, à ISO, à ABNT, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração deste documento.

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



2 Introdução

A política de desenvolvimento de pessoas em privacidade e segurança da informação é um normativo institucional complementar à Política de Desenvolvimento de Pessoas do órgão, que tem o papel de estabelecer diretrizes para o desenvolvimento pessoal dentro da organização. Estipular papéis e responsabilidades claras e objetivas, definir diretrizes de conscientização e estabelecer meios de monitoramento do cumprimento da política são processos muito importantes para garantir o desenvolvimento pessoal em privacidade e segurança da informação.

Este modelo tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e as entidades da Administração Pública Federal, direta, autárquica e fundacional a elaborar, em âmbito institucional, sua política de desenvolvimento de pessoas em privacidade e segurança da informação.

O presente documento serve como um modelo prático a ser utilizado na implementação dos controles 14 e 23 do Guia do *Framework* de Privacidade e Segurança da Informação¹ v1, e respectivas evoluções desta versão (1.1, 1.2 etc.), elaborado e publicado pela SGD, que assim estabelecem:



Controle 14: Conscientização e Treinamento de Competências sobre Segurança – Implantar e manter um programa de conscientização de segurança que possa influenciar e conscientizar o comportamento dos colaboradores, tornando-os devidamente qualificados e assim atingir o objetivo de reduzir riscos de segurança cibernética da organização.

Controle 23: Conscientização e Treinamento – As pessoas envolvidas no tratamento de dados são instruídas e conscientizadas sobre privacidade, sendo treinadas para desempenhar suas funções e responsabilidades relacionadas à privacidade de acordo com as políticas, os processos, os procedimentos, os acordos e os valores de privacidade da organização.

As medidas dos controles 14 e 23 que estão contempladas por este modelo são: 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8, 14.9, 23.1, 23.2, 23.3 e 23.4.

Isso porque hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão, apoiado em sistemas informatizados.

¹ Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf>.

Acesso em: 21 jan. 2025.



Nesse contexto, os entes federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões de guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa).

Os dados pessoais e demais informações custodiados pelos entes públicos são frequentemente fornecidos ou compartilhados, obedecidos os requisitos legais, com entes de outras esferas e seus respectivos poderes, empresas públicas e privadas, instituições de ensino, organizações de pesquisa públicas ou independentes e organizações do terceiro setor.

O Art. 50 da LGPD estabelece que os controladores e operadores devem criar e implementar regras de boas práticas de governança para o tratamento de dados pessoais:

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

Dentre as regras de boas práticas de governança para o tratamento de dados pessoais, destaca-se para este modelo as ações educativas que visam sensibilizar os profissionais de privacidade e segurança da informação a executar ações que mitiguem os possíveis danos aos titulares de dados pessoais e, conseqüentemente, à instituição, que possam ser causados por algum incidente de segurança da informação.

Importante ressaltar que a adoção deste modelo não dispensa o ente público de considerar as diretrizes gerais estabelecidas pela Autoridade Nacional de Proteção de Dados – ANPD, pelo Gabinete de Segurança Institucional – GSI, pela LGPD, bem como pela Política Nacional de Desenvolvimento de Pessoas – PNPD e pela Política Nacional Segurança da Informação – PNSI.



3 Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação

Para usar este modelo, basta substituir o texto [com destaque amarelo] por informações personalizadas do seu órgão ou entidade. Quando estiver concluído, exclua todos os textos introdutórios ou de exemplos (em vermelho) e converta todo o texto restante em cor preta antes do processo de aprovação.

IMPORTANTE: este modelo deve ser utilizado exclusivamente como referência, devendo o órgão ou entidade considerar as particularidades técnicas específicas do seu ambiente, bem como observar a boa aderência aos processos internos a fim de construir uma política que seja adequada à sua realidade.

Responsável	[Nome da pessoa ou área responsável pela gestão desta política]
Aprovado por:	[Nome da pessoa ou área responsável pela aprovação e pela autorização da implementação desta política]
Políticas Relacionadas	[Relacione outras políticas corporativas relacionadas dentro ou externas a este modelo, por exemplo, Política Nacional de Desenvolvimento de Pessoas – PNDP / Política Nacional Segurança da Informação – PNSI]
Localização de armazenamento	[Descreva a localização física ou digital das cópias desta política]
Data da Aprovação	[Liste a data em que essa política entrou em vigor]
Data de revisão	[Liste a data em que esta política passou por revisão ou atualização]
Versão	[Indique a versão atual desta política]

Quadro 1 – Informações sobre a Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação



4 Propósito

Objetivo da Política

Levando em consideração a natureza e a finalidade do órgão ou entidade, descreva os fatores ou as circunstâncias que determinam a existência da política de desenvolvimento de pessoas. Além disso, afirme os objetivos básicos da política e o que a política pretende alcançar.

Exemplo: A Política de Desenvolvimento de Pessoas objetiva estabelecer diretrizes, princípios e conceitos para conscientizar e capacitar os servidores e conscientizar colaboradores que se relacionam com o [Órgão ou Entidade] e que em algum momento realizam operações de tratamento de dados pessoais, visando o cumprimento da Lei Geral de Proteção de Dados Pessoais – LGPD e outras normas vigentes, tais como o Decreto nº 9.991, de 28 de agosto de 2019, e o Decreto nº 9.637, de 26 de dezembro de 2018.



5 Escopo

Amplitude: alcance da Política

Defina a quem e a quais sistemas esta Política se aplica. Liste os agentes públicos e os colaboradores necessários para cumprir ou simplesmente indique se todos devem cumprir. Também assinale quaisquer exclusões ou exceções que estejam fora de escopo, ou seja, pessoas, elementos ou situações que não estejam cobertas por esta política ou onde uma consideração especial possa ser feita.

Exemplo:

Esta política deve abranger todo o âmbito do [Órgão ou Entidade].

Especificamente, inclui:

- todos os funcionários, sejam servidores efetivos ou temporários, do [Órgão ou Entidade];
- todos os contratados e terceiros que trabalham para o [Órgão ou Entidade].



6 Termos e definições

Glossário

Defina quaisquer termos-chave, siglas ou conceitos que serão utilizados na política. Sugere-se utilizar como referência as definições apresentadas no Art. 5 da LGPD, além da Portaria GSI/PR nº 93, de 18 de outubro de 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

Exemplo:

AGENTES DE TRATAMENTO: o controlador e o operador;

ATIVOS DE INFORMAÇÃO: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tenha valor para um indivíduo ou organização;

CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

CONSCIENTIZAÇÃO: atividade que tem por finalidade orientar o que é segurança da informação, levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade, para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros;

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável;

ENCARREGADO: pessoa indicada pelo controlador e operador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

ENGENHARIA SOCIAL: técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto da segurança da informação, é considerada uma prática de má-fé para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de indivíduos, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes;

GESTOR DE SEGURANÇA DA INFORMAÇÃO: responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

LGPD: sigla de Lei Geral de Proteção de Dados Pessoais;

OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;



PDP: sigla de Plano de Desenvolvimento Pessoal;

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – POSIN: documento autorizado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança de informação.

TRATAMENTO: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;



7 Declarações da política

Diretrizes aplicáveis ao caso específico

Descreva as diretrizes que compõem a política. Isso normalmente toma a forma de uma série de breves declarações prescritivas. A subdivisão desta seção em subseções pode ser necessária dependendo da complexidade da política.

Exemplo:

Art. 1º Fica aprovada, no âmbito do [Órgão ou Entidade], a Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação.

Art. 2º Esta Política abrange todos os colaboradores, servidores, empregados públicos, terceirizados, estagiários e demais profissionais que atuam no [Órgão ou Entidade] e que tenham acesso a dados pessoais e informações institucionais.

Art. 3º Esta Política estabelece diretrizes para o desenvolvimento contínuo de competências em privacidade e segurança da informação, alinhadas ao Decreto nº 9.991/2019, que regula a Política Nacional de Desenvolvimento de Pessoas – PNDP, e aos dispositivos legais e normativos a seguir:

- I. à Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- II. ao Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação;
- III. à Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
- IV. ao Programa de Privacidade e Segurança da Informação – PPSI, estabelecido pela Portaria SGD/MGI nº 852, de 28 de março de 2023;
- V. às regulamentações emitidas pela Autoridade Nacional de Proteção de Dados – ANPD;
- VI. ao Plano de Desenvolvimento de Pessoas do [Órgão ou Entidade];
- VII. à Política de Segurança da Informação do [Órgão ou Entidade];
- VIII. à Política de Proteção de Dados Pessoais do [Órgão ou Entidade].
- IX. [Incluir outros itens que considerar necessários].

Art. 4º São objetivos da Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação do [Órgão ou Entidade]:

- I. promover a capacitação periódica para adaptação às novas tecnologias e ameaças digitais;
- II. atender aos dispositivos dispostos no art. 3º e demais normas e legislação correlatas;
- III. viabilizar a adequada proteção dos ativos de informação contra ameaças internas e externas;

- IV. promover a cultura organizacional de privacidade e segurança da informação;
- V. incentivar a adoção de boas práticas de privacidade e segurança da informação.
- VI. **[Incluir outros itens que considerar necessários].**

Art. 5º Para fins do cumprimento desta Política, o Plano de Desenvolvimento de Pessoas – PDP do **[Órgão ou Entidade]** deve contemplar as ações de desenvolvimento, capacitação ou treinamentos relacionados à privacidade e segurança da informação, em especial as recomendações oriundas do PPSI quanto aos temas:

- I. ataques de engenharia social;
- II. boas práticas de autenticação;
- III. causas da exposição não intencional de dados;
- IV. como reconhecer e relatar incidentes de segurança;
- V. gestão de riscos e boas práticas de segurança digital;
- VI. tratamento de dados pessoais.
- VII. **[Inserir outros itens que considerar necessários].**

Art. 6º Compete à **[Unidade de Gestão de Pessoas ou Outra Unidade Delegada pela Autoridade Máxima do Órgão ou Entidade]** em conjunto com o gestor de segurança da informação e o encarregado pelo tratamento de dados pessoais, com apoio da **[Unidade de Tecnologia da Informação]**, promover o levantamento das necessidades de desenvolvimento em privacidade e segurança da informação junto às unidades organizacionais do **[Órgão ou Entidade]**.

Parágrafo único. As necessidades de que trata o *caput* devem:

- I. estar alinhadas com os objetivos e metas institucionais, bem como com a estratégia do **[Órgão ou Entidade]**;
- II. atender às necessidades administrativas operacionais, táticas e estratégicas, vigentes e futuras;
- III. preparar os servidores para as mudanças de cenários internos e externos ao **[Órgão ou Entidade]**;
- IV. preparar os servidores para substituições decorrentes de afastamentos, impedimentos legais ou regulamentares do titular e da vacância do cargo;
- V. acompanhar o desenvolvimento do servidor durante sua vida funcional.
- VI. **[Inserir outros itens que considerar necessários].**

Art. 7º Compete ao gestor de segurança da informação em conjunto com o encarregado pelo tratamento de dados pessoais, com apoio da **[Unidade de Tecnologia da Informação]**:

- I. definir os níveis de conhecimento e habilidade necessários para os servidores e colaboradores executarem deveres e tarefas relacionadas à privacidade e segurança da informação;
- II. validar as necessidades de desenvolvimento em privacidade e segurança da informação do **[Órgão ou Entidade]**;



- III. planejar as ações de desenvolvimento, capacitação ou treinamento em privacidade e segurança da informação que comporão o PDP do [Órgão ou Entidade];
- IV. planejar as ações de conscientização e a publicação de boletins ou folhetos sobre privacidade e segurança da informação;
- V. comunicar as necessidades validadas para a unidade de gestão de pessoas do [Órgão ou Entidade].
- VI. [Inserir outros itens que considerar necessários].

Parágrafo único. O planejamento das ações de desenvolvimento, capacitação ou treinamento em privacidade e segurança da informação que comporão o PDP do [Órgão ou Entidade] de que trata o inciso II do *caput* deve:

- I. estar de acordo com os princípios da economicidade e da eficiência;
- II. ofertar ações de desenvolvimento de maneira equânime aos servidores.
- III. [Inserir outros itens que considerar necessários].

Art. 8º São tipos de ações de desenvolvimento, capacitação ou treinamento de pessoas em privacidade e segurança da informação:

- I. ações que visam ao atendimento das necessidades diagnosticadas com base em avaliações da instituição e do planejamento estratégico do [Órgão ou Entidade];
- II. curso introdutório abordando os princípios básicos de privacidade e segurança da informação na administração pública;
- III. treinamentos obrigatórios previstos em legislação específica sobre a temática de privacidade e segurança da informação;
- IV. ações destinadas ao desenvolvimento gerencial e reconhecimento de responsabilidades sobre proteção de dados pessoais;
- V. ações que busquem elevar a maturidade e a resiliência do [Órgão ou Entidade] em termos de privacidade e segurança da informação e que estejam alinhadas com o PPSI;
- VI. ações de treinamento e conscientização realizadas pelo [Órgão ou Entidade] que visam a manter os servidores e/ou colaboradores atualizados sobre os desenvolvimentos no ambiente regulatório, contratual e tecnológico que possam afetar a conformidade de privacidade e de segurança da informação da organização;
- VII. cursos de caráter permanente coordenados e realizados em parceria com as escolas de governo, outras instituições ou pessoas físicas direcionados à segurança da informação, privacidade e proteção de dados pessoais, conforme as funções dos profissionais envolvidos com o tratamento de dados pessoais;
- VIII. exercícios práticos de conscientização de segurança da informação que simulam ataques cibernéticos;
- IX. conscientização de segurança da informação sobre reconhecimento e relato de potenciais indicadores de ameaça interna;
- X. treinamento em privacidade e segurança da informação baseado em funções para o profissional, designando papéis e responsabilidades.



XI. [Inserir outros itens que considerar necessários].

Art. 9º Compete ao gestor de segurança da informação do [Órgão ou Entidade]:

- I. estimular ações de desenvolvimento, capacitação ou treinamento e de profissionalização de recursos humanos em temas relacionados à segurança da informação, conforme disposto no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;
- II. acompanhar a realização e o bom andamento das ações de desenvolvimento, capacitação ou treinamento em segurança da informação.
- III. [Inserir outros itens que considerar necessários].

Art. 10. Compete ao encarregado pelo tratamento de dados pessoais do [Órgão ou Entidade]:

- I. orientar os colaboradores, servidores, empregados públicos, terceirizados, estagiários e demais profissionais que atuam no [Órgão ou Entidade] a respeito das práticas de desenvolvimento pessoal a serem tomadas em relação à proteção de dados pessoais, conforme disposto no inciso III do § 2º do art. 41 da LGPD;
- II. acompanhar a realização e o bom andamento das ações de desenvolvimento, capacitação ou treinamento em privacidade.
- III. [Inserir outros itens que considerar necessários].

Art. 11. Compete aos colaboradores, servidores, empregados públicos, terceirizados, estagiários e demais profissionais que atuam no [Órgão ou Entidade] a aplicação dos conceitos, normas, procedimentos e demais conhecimentos adquiridos com a participação nas ações de desenvolvimento, capacitação ou treinamento em privacidade e segurança da informação.

Art. 12. As despesas com ações de desenvolvimento, capacitação ou treinamento em privacidade e segurança da informação só serão realizadas após aprovação do PDP, conforme disposto no art. 16 do Decreto nº 9.991, de 28 de agosto de 2019.



8 Referências bibliográficas

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

_____. ABNT NBR ISO/IEC 27002:2013: **Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação**. Rio de Janeiro, 2013.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Conselho Diretor. **Resolução CD/ANPD nº 18, de 16 de julho de 2024. Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais**. 2024. Disponível em: <<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074>>. Acesso em: 09 set. 2024.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 8.112, de 11 de dezembro de 1990**. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm>. Acesso em: 09 set. 2024.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação – LAI**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 09 set. 2024.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 09 set. 2024

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 09 set. 2024.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 9.637, de 26 de dezembro de 2018. Política Nacional de Segurança da Informação – PNSI**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm>. Acesso em: 09 set. 2024.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 9.991, de 28 de agosto de 2019**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9991.htm>. Acesso em: 09 set. 2024.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm>. Acesso em: 09 set. 2024.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 10.641, de 2 de março de 2021. Altera a Política Nacional de Segurança da Informação – PNSI.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10641.htm>. Acesso em: 09 set. 2024.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm>. Acesso em: 09 set. 2024.

_____. Presidência da República. Gabinete de Segurança Institucional. **Portaria GSI/PR nº 93, de 18 de outubro de 2021. Aprova o glossário de segurança da informação.** Disponível em: <<https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370>>. Acesso em: 09 set. 2024.

_____. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa nº 01, maio de 2020.** Disponível em: <https://www.gov.br/gsi-pt-br/ssic/legislacao/copy_of_IN01_consolidada.pdf>. Acesso em: 28 set. 2023.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa nº 03, de 28 de maio de 2021.** Brasília-DF, GSI/PR, 2021. Disponível em: <https://www.gov.br/gsi-pt-br/ssic/legislacao/copy_of_IN03_consolidada.pdf>. Acesso em: 09 set. 2024.

_____. Presidência da República. Gabinete de Segurança Institucional. **Norma Complementar nº 17, abril de 2013.** Disponível em: <<https://www.gov.br/gsi-pt-br/dsic/legislacao/NC17.pdf>>. Acesso em: 09 set. 2024.

_____. Presidência da República. Gabinete de Segurança Institucional. **Norma Complementar nº 18, abril de 2013.** Disponível em: <<https://www.gov.br/gsi-pt-br/dsic/legislacao/NC18.pdf>>. Acesso em: 09 set. 2024.

_____. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Portaria SGD/MGI nº 852, de 28 de março de 2023.** Disponível em: <<https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908>>. Acesso em: 09 set. 2024.

_____. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Diretoria de Privacidade e Segurança da Informação. **Guia do Framework de**

Privacidade e Segurança da Informação. 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf>. Acesso em: 09 set. 2024.

_____. Ministério da Economia. **Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020. Dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.** 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: 09 set. 2024.

CENTER INTERNET SECURITY. **Security Awareness Skills Training Policy Template for CIS Control 14.** mar. 2023. Disponível em: <<https://www.cisecurity.org/insights/white-papers/security-awareness-skills-training-policy-template-for-cis-control-14>>. Acesso em: 09 set. 2024.

_____. ISO/IEC 29151:2017: **Information technology – Security techniques – Code of practice for personally identifiable information protection.** Genebra, 2017.

_____. NIST Special Publication 800-50: **Building an Information Technology Security Awareness and Training Program.** Gaithersburg, 2003.

_____. NIST Special Publication 800-53 revisão 4: **Security and Privacy Controls for Information Systems and Organizations.** Gaithersburg, 2013. Acesso em: 29 set. 2023.

GOVERNO DO RIO GRANDE DO SUL. Subsecretaria de Gestão e Desenvolvimento de Pessoas. **Política de Gestão e Desenvolvimento de Pessoas.** Disponível em: <<https://gestaodepessoas.rs.gov.br/politica-de-gestao-de-pessoas/>>. Acesso em: 09 set. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Public Draft: **The NIST Cybersecurity Framework 2.0, 2023.** Disponível em: <<https://www.nist.gov/cyberframework/framework>>. Acesso em: 09 set. 2024.

UNIVERSIDADE DE FEDERAL DA BAHIA. Superintendência de Tecnologia da Informação. **Plano de conscientização em segurança da informação.** mar. 2023. Disponível em: <<https://sti.ufba.br/plano-de-conscientizacao-em-seguranca-da-informacao>>. Acesso em: 09 set. 2024.



9 Anexo I

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nas versões do Modelo de Política de Desenvolvimento de Pessoas e Segurança da Informação em comparação com o documento originalmente publicado em dezembro de 2023.

Mudanças da Versão 1.1.

As mudanças inseridas nesta versão, em comparação com a anterior, visam à padronização da diagramação do documento, ajustes nas seções Termos e Definições e Disposições Gerais, adequação do modelo com a Resolução CD/ANPD nº 18, de 16 de julho de 2024, e reestruturação da seção Declarações da política.

Destacam-se as seguintes alterações:

- adição do termo “agente de tratamento” e adequação da definição do termo “encarregado” na seção Termos e Definições;
- inclusão de um tópico no primeiro parágrafo da subseção Disposições Gerais, que estabelece a necessidade de a Política de Desenvolvimento de Pessoas e Segurança da Informação estar alinhada aos normativos e publicações da ANPD;
- inclusão da Resolução CD/ANPD nº 18, de 16 de julho de 2024, nas referências bibliográficas.

