



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

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 1.0

Brasília, dezembro de 2023



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

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 PROTEÇÃO DE DADOS

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Ivaldo Jeferson de Santana Castro

Rafael da Silva Ribeiro

Raphael César Estevão

Equipe Revisora

Adriano de Andrade Moura

Francisco de Assis Fialho Henriques

Rogério Vinícius Matos Rocha

Sumaid Andrade de Albuquerque



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



Sumário

Aviso Preliminar e Agradecimentos	5
Introdução	6
Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação	8
Propósito [Objetivo da Política]	8
Escopo [Amplitude, alcance da Política]	8
Termos e Definições [Glossário]	9
Declarações da política [Diretrizes aplicáveis ao caso específico]	10
Disposições Gerais	10
Metas e resultados esperados	11
Papéis e Responsabilidades	11
Orçamento	12
Ações de desenvolvimento prioritárias	12
Procedimentos para solicitações de ações de desenvolvimento de pessoas	13
Afastamento para capacitação	13
Disposições finais	14
Referências Bibliográficas	15



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 da 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 determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais, deve, no âmbito de suas competências, 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 Informação¹ 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, da ABNT 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.

Finalmente, 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.

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.

¹ https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf

Introdução

Este modelo tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a elaborar sua Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação no âmbito institucional.

Os Controles 14 e 23 do Guia do Framework de Privacidade e Segurança da Informação (p. 52 e 63) estabelecem que:



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, processos, procedimentos, acordos e valores de privacidade da organização.

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 Informação v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. 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.

Cada vez mais o Governo utiliza tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.

Nesse contexto, os órgãos 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 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). As informações federais são frequentemente fornecidas ou compartilhadas, obedecendo os requisitos legais, com entes como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

O Art. 50 da Lei Geral de Proteção de Dados (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 a sensibilizar os profissionais de privacidade e segurança da informação a executar ações que mitiguem os possíveis danos a instituição, e conseqüentemente, aos titulares de dados pessoais, que possam ser causados por algum incidente de segurança da informação.

Ressaltamos ainda, que a adoção deste modelo não dispensa as instituições da Administração Pública Federal de observar e considerar as diretrizes estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD), pelo Gabinete de Segurança Institucional (GSI), pela Lei Geral de Proteção de Dados (LGPD) e outras normas vigentes.

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 de uma 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 tutelados pela organização.



Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação

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 a sua realidade.

Este modelo tem por foco prover diretrizes para a elaboração da política de desenvolvimento de pessoas em privacidade e segurança da informação.

Para usar este modelo, basta substituir o texto em cinza por informações personalizadas do seu órgão ou entidade. Quando estiver concluído, exclua todos os textos introdutórios ou de exemplo e converta todo o texto restante em preto antes do processo de aprovação.

Responsável	Nome da pessoa ou área responsável pela gestão desta política.
Aprovado por:	Nome da pessoa ou área responsável pela aprovação e 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 de Aprovação	Liste a data em que essa política entrou em vigor.
Data de revisão	Liste a data em que esta política deve passar por revisão e atualização.
Versão	Indique a versão atual desta política

Propósito [Objetivo da Política]

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

Exemplo:

A Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação tem por objetivo estabelecer diretrizes, princípios e conceitos para conscientizar e capacitar os servidores e conscientizar colaboradores que se relacionam com o(a) [Órgão ou entidade] e que em algum momento têm acesso ou 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 9.637, de 26 de dezembro de 2018.

[Acrescente aqui os objetivos para a Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação que julgar necessário.]

Escopo [Amplitude, alcance da Política]

Defina a quem e a quais sistemas esta política se aplica. Liste os agentes públicos e colaboradores necessários para cumprir ou simplesmente indique "todos" se todos devem cumprir. Também indique quaisquer exclusões ou



exceções que estejam fora de escopo, ou seja, essas pessoas, elementos ou situações que não estejam cobertas por esta política ou onde uma consideração especial possa ser feita.

Exemplo:

A Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação, deve abranger todo âmbito do(a) [Órgão ou entidade].

Esta Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação se aplica aos servidores e colaboradores do [Órgão ou entidade], incluindo gestores, prestadores de serviços, estagiários e contratados que tenham acesso e/ou utilize dados institucionais, incluindo os dados pessoais.

[Acrescente aqui mais diretrizes sobre o escopo da Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação que julgue necessárias.]

Termos e Definições [Glossário]

Defina quaisquer termos-chave, siglas ou conceitos que serão utilizados na política. [Recomenda-se utilizar como referência as definições apresentadas no Art. 5 da LGPD, além da PORTARIA GSI/PRNº 93, DE 18 DE OUTUBRO DE 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da PRESIDÊNCIA DA REPÚBLICA].

Exemplo:

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 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, 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;

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;

[Acrescente os termos-chave, siglas ou conceitos que podem ser utilizados na política.]

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:

Disposições Gerais

A Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação do [Órgão ou entidade] deve estar alinhada:

- com Lei Geral de Proteção de Dados Pessoais (Lei 13.709, de 14 de agosto de 2018);
- com a Política Nacional de Desenvolvimento de Pessoas (Decreto 9.991, de 28 de agosto de 2019);
- com a Política Nacional de Segurança da Informação (Decreto 9.637, de 26 de dezembro de 2018);
- com Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;
- com Instrução Normativa SGD/ME Nº 117, de 19 de novembro de 2020;
- com o Programa de Privacidade e Segurança da Informação (PPSI - Portaria SGD/MGI nº 852, DE 28 de março de 2023);
- com o plano de desenvolvimento de pessoas do órgão;
- com a política de segurança da informação do órgão;
- com a política de proteção de dados pessoais do órgão;
- com uma gestão de continuidade de negócios em nível organizacional;
- [Liste demais instrumentos que deverão estar alinhados com a Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação.]

Deve ser previsto pelo [Órgão ou entidade], um número de atividades de conscientização, tais como, campanhas (por exemplo, “Dia da Privacidade e Segurança da Informação”) e a publicação de boletins ou folhetos.

Os treinamentos do [Órgão ou entidade], devem estar alinhados com as melhores práticas de tratamento de dados pessoais, privacidade e segurança da informação, em especial as recomendações do PPSI:

- I. Melhores práticas de tratamento de dados;
- II. Como reconhecer ataques de engenharia social;
- III. Melhores práticas de autenticação;
- IV. Causas da exposição não intencional de dados;
- V. Como reconhecer e relatar incidentes de segurança;
- VI. [Liste demais temáticas que poderão ser abordadas em treinamentos previstos na Política de Desenvolvimento de Pessoas em Privacidades e Segurança da Informação.]



O [Órgão ou entidade], deve definir os níveis de conhecimento e habilidade necessários para os servidores e colaboradores executarem deveres e tarefas relacionadas a Privacidade e Segurança da Informação.

O planejamento das ações de desenvolvimento de pessoas em privacidade e segurança da informação do [Órgão ou entidade], deve estar de acordo com os princípios da economicidade e da eficiência, conforme disposto no art. 3º do Decreto nº 9.991, de 28 de agosto de 2019.

[Liste demais disposições gerais que poderão compor a Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação.]

Metas e resultados esperados

O [Órgão ou entidade], deve:

- promover o desenvolvimento pessoal em privacidade e segurança da informação;
- estabelecer metas institucionais como referência para o planejamento das ações de desenvolvimento em privacidade e segurança da informação;
- atingir um nível de conhecimento considerável em privacidade e segurança da informação, após sua conclusão;
- avaliar o desempenho e comprometimento dos servidores com as metas e necessidades institucionais ao final de cada processo de desenvolvimento;
- [Acrescente aqui demais diretrizes sobre as metas e resultados esperados da Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação.]

Papéis e Responsabilidades

Cabe a(o) [indicar o responsável] a responsabilidade de planejar e coordenar a execução das atividades de ensino em privacidade e segurança da informação.

Cabe ao Gestor de Segurança da Informação do [Órgão ou entidade], estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação, conforme previsto no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

Cabe ao Encarregado orientar os funcionários e os contratados do [Órgão ou entidade], a respeito das práticas de desenvolvimento pessoal a serem tomadas em relação à proteção de dados pessoais.

Cabe a Alta Administração do [Órgão ou entidade], capacitar os Agentes Responsáveis para o uso dos recursos criptográficos, observando as normas vigentes, os procedimentos de credenciamento de segurança, e o tratamento de informação classificada.

Todos os servidores e colaboradores do [Órgão ou entidade], têm a responsabilidade de implementar os conceitos ensinados nos programas de conscientização e treinamento em Privacidade e Segurança da Informação.

Todas as ações de capacitação, independentemente de sua fonte de recursos, devem ser acompanhadas pelo(a) [indicar o responsável pelo acompanhamento].

O(a) [indicar o responsável] deve divulgar periodicamente, por intermédio da intranet ou por outros meios, os eventos constantes no Plano Anual de Capacitação.



[Liste demais responsáveis e seus papéis dentro da Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação]

Orçamento

O [Órgão ou entidade], deve:

- somente realizar despesas com ações de desenvolvimento de pessoas em privacidade e segurança da informação, após aprovação do PDP, conforme disposto no art. 16 do Decreto nº 9.991, de 28 de agosto de 2019;
- racionalizar e utilizar de modo efetivo os recursos orçamentários destinados ao desenvolvimento de pessoas em privacidade e segurança da informação;
- publicar na internet, de forma transparente e objetiva, todas as despesas com as ações de desenvolvimento de pessoas em privacidade e segurança da informação, conforme disposto no art. 16 do Decreto nº 9.991, de 28 de agosto de 2019;
- analisar o custo-benefício das despesas realizadas no exercício anterior com as ações de desenvolvimento de pessoas em privacidade e segurança da informação, conforme disposto no art. 3º do Decreto nº 9.991, de 28 de agosto de 2019;
- [Acrescente aqui demais diretrizes sobre o orçamento da Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação.]

Ações de desenvolvimento prioritárias

Durante a realização do planejamento das ações prioritárias de desenvolvimento de pessoas deve-se criar um quadro com a programação das atividades, no qual contenha para cada ação de desenvolvimento do servidor e/ou colaborador do [Órgão ou entidade]:

Exemplo:

- I. nome do evento ou ação;
- II. a carga horária;
- III. tipo de atividade;
- IV. forma de realização;
- V. [Liste o que mais achar necessário ser acrescentado no quadro de atividades.]

[Liste diretrizes a serem observadas ao que diz respeito as ações de desenvolvimento prioritárias dentro da Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação.]

As ações de desenvolvimento prioritárias do [Órgão ou entidade] devem ser definidas dentre as relacionadas a seguir:

- I. ações que visam ao atendimento às necessidades diagnosticadas com base em avaliações da instituição e, ou, de seu planejamento estratégico do [Órgão ou entidade];
- II. curso introdutório financiado pelo [Órgão ou entidade], abordando os princípios básicos de Privacidade e Segurança da Informação na administração pública, entre outros;
- 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;
- V. ações que busquem elevar a maturidade e a resiliência do [Órgão ou entidade], em termos de privacidade e segurança da informação que estejam alinhadas com o PPSI;



- VI. as 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 e/ou pessoas físicas direcionado a segurança da informação, privacidade e proteção de dados pessoais, conforme as funções das pessoas envolvidas 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 servidor e/ou colaborador designando papéis e responsabilidades;
- XI. [Liste as demais ações que julgue prioritárias no desenvolvimento da Política].

Procedimentos para solicitações de ações de desenvolvimento de pessoas

Os procedimentos para solicitações de ações de desenvolvimento de pessoas em privacidade e segurança da informação devem estar previstos no Plano de Desenvolvimento de Pessoas do órgão.

A solicitação para participação de servidor do [Órgão ou entidade], em ações de desenvolvimento deve ser feita mediante a instrução do processo correspondente no Sistema Eletrônico de Informações (SEI), com posterior envio à unidade de gestão de pessoas.

A participação em ação de desenvolvimento que implicar em despesas diárias e passagens somente pode ser realizada se o custo total da ação for inferior ao custo da participação em evento similar na própria localidade de exercício do interessado, podendo ser aprovada, mediante justificativa, pela [autoridade competente].

[Liste aqui mais diretrizes sobre os procedimentos para solicitações de ações de desenvolvimento pessoal da Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação.]

Afastamento para capacitação

É considerado afastamento para participação em ações de desenvolvimento do [Órgão ou entidade] a:

- I. licença para capacitação, nos termos do disposto no art. 87 da Lei nº 8.112, de 11 de dezembro de 1990;
- II. participação em programa de pós-graduação stricto sensu no País, conforme o disposto no art. 96-A da Lei nº 8.112, de 11 de dezembro de 1990;
- III. realização de estudo no exterior, conforme o disposto no art. 95 da Lei nº 8.112, de 1990.



Os afastamentos podem ser concedidos pelo [Órgão ou entidade], entre outros critérios, quando a ação de desenvolvimento:

- I. estiver prevista no PDP do órgão ou da entidade do servidor;
- II. estiver alinhada ao desenvolvimento do servidor nas competências relativas ao Art. 19, II do Decreto Nº 9.991, de 28 de agosto de 2019;
- III. dispor de horário ou o local que inviabilize o cumprimento das atividades previstas ou a jornada semanal de trabalho do servidor;

Os afastamentos podem ser interrompidos, a qualquer tempo, a pedido do servidor ou no interesse da administração do [Órgão ou entidade].

A licença para capacitação do [Órgão ou entidade], deve observar a Lei Nº 8.112, de 11 de dezembro de 1990, o que consta no decreto Nº 9.991, de 28 de agosto de 2019 e demais normas correlatas.

[Liste diretrizes se necessárias, para compor as formas que o afastamento para capacitação será concedido.]

Disposições finais

Esta política deverá ser revisada no período de [definir o prazo para revisão da política], a partir do início de sua vigência.

[Acrescente aqui as demais disposições que julgue necessário.]

Esta política entra em vigor na data de sua publicação.



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

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 8.112, de 11 de dezembro de 1990. **Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais**. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm >. Acesso em: 28 set. 2023

BRASIL. 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: 28 set. 2023

BRASIL. 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: 28 set. 2023

BRASIL. 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: 28 set. 2023

BRASIL. 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: 28 set. 2023.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 9.991, de 28 de agosto de 2019. **Dispõe sobre a Política Nacional de Desenvolvimento de Pessoas da Administração Pública Federal Direta, Autárquica e Fundacional**. Disponível em: < https://www.planalto.gov.br/ccivil_03/ato2019-2022/2019/decreto/d9991.htm >. Acesso em: 28 set. 2023.

BRASIL. 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: 28 set. 2023.

BRASIL. 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: 28 set. 2023.

BRASIL. 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: 28 set. 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria GSI/PR nº 93, 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: 28 set. 2023

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Instrução Normativa nº 01, maio de 2020. **Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da**



Administração Pública Federal. Disponível em: <https://www.gov.br/gsi/pt-br/dsic/legislacao/copy_of_IN01_consolidada.pdf>. Acesso em: 28 set. 2023

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Instrução Normativa nº 03, maio de 2021. **Dispõe sobre os processos relacionados à Gestão de Segurança da Informação nos Órgãos e nas Entidades da Administração Pública Federal.** Disponível em: < https://www.gov.br/gsi/pt-br/dsic/legislacao/copy_of_IN03_consolidada.pdf >. Acesso em: 28 set. 2023

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Norma Complementar nº 17, abril de 2013. **Dispõe sobre a Atuação e Adequações para Profissionais a Área de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.** Disponível em: < <https://www.gov.br/gsi/pt-br/dsic/legislacao/NC17.pdf> >. Acesso em: 28 set. 2023

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Norma Complementar nº 18, abril de 2013. **Dispõe sobre as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.** Disponível em: < <https://www.gov.br/gsi/pt-br/dsic/legislacao/NC18.pdf> >. Acesso em: 28 set. 2023

BRASIL. Ministério do Meio Ambiente. Portaria 100, março de 2012. **Dispõe sobre diretrizes e objetivos relativos à Política de Desenvolvimento dos Servidores do Ministério do Meio Ambiente.** Disponível em: < <https://www.ibama.gov.br/component/legislacao/?view=legislacao&legislacao=126824> >. Acesso em: 28 set. 2023.

BRASIL. Secretaria de Governo Digital. Portaria SGD/MGI nº 852, março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI. Disponível em: < <https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908> >. Acesso em: 28 set. 2023.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação. Novembro 2022.** Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf>. Acesso em: 28 set. 2023.

UNIVERSIDADE DE FEDERAL DA BAHIA. SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO. **Plano de conscientização em segurança da informação. Março de 2023.** Disponível em: < <https://sti.ufba.br/plano-de-conscientizacao-em-seguranca-da-informacao> >. Acesso em: 28 set. 2023.

BRASIL. Ministério de Gestão e da Inovação em Serviços Públicos. **Norma Complementar nº 18, abril de 2013. D Plano de Desenvolvimento de Pessoas 2023.** Disponível em: < https://www.gov.br/servidor/pt-br/aceso-a-informacao/servidor/carreiras/eppgg/sobre-a-carreira/desenvolvimento-profissional-1/arquivos/formularios/plano_de_desenvolvimento_de_pessoas_2023.pdf >. Acesso em: 28 set. 2023

MINISTÉRIO DA ECONOMIA. Instrução Normativa SGD/ME nº117, 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: 28 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: 28 set. 2023

CENTER INTERNET SECURITY. **Security Awareness Skills Training Policy Template for CIS Control 14.** março 2023. Disponível em: < <https://www.cisecurity.org/insights/white-papers/security-awareness-skills-training-policy-template-for-cis-control-14> > . Acesso em: 28 set 2023.

_____. **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.

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: 28 set 2023.