gov.br

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Modelo de Política de Segurança da Informação

Programa de Privacidade e Segurança da Informação (PPSI)

Versão 1.0
Brasília, agosto de 2024

MODELO DE POLÍTICA DEFESAS CONTRA MALWARE

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS
Esther Dweck
Ministra

SECRETARIA DE GOVERNO DIGITAL
Rogério Souza Mascarenhas
Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO
Leonardo Rodrigo Ferreira
Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE
Julierme Rodrigues da Silva
Coordenador-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO
Loriza Andrade Vaz de Melo
Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração
Francisco Magno Felix Nobre
Ivaldo Jeferson de Santana Castro
Raphael César Estevão

Equipe Revisora
Adriano de Andrade Moura
Anderson Souza de Araújo
Bruno Pierre Rodrigues de Sousa
Rogério Vinícius Matos Rocha

Histórico de versões

Data	Versão	Descrição	Autor
22/08/2024	1.0	Modelo de Política de Segurança da Informação	Equipe Técnica de Elaboração

Sumário

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 Segurança da Informação, em atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados que estão sob sua custódia. Adicionalmente, a Elaboração de uma Política de Segurança da Informação visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação, tais como as instruções normativas do GSI/PR (Gabinete de Segurança Institucional da Presidência da República).

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[1] 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 ANPD;
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.

[1] https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, à ABNT, ao NIST e aos profissionais de privacidade e proteção de dados 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 proteção de dados ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e proteção de dados e outras referências utilizadas neste documento

2 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 Segurança da Informação no âmbito institucional.

O Controle 22 do Guia do Framework de Privacidade e Segurança da Informação (p. 62) estabelece que:

Controle 22: Políticas, Processos e Procedimentos - Definir, desenvolver, divulgar, implementar e atualizar políticas, processos e procedimentos operacionais, internos e externos que regem as ações relativas à proteção de dados pessoais e privacidade, e controles para programas, sistemas de informação ou tecnologias que envolvam o tratamento de dados pessoais.

O presente documento serve como um modelo prático a ser utilizado na implementação do controle 22 do Guia do Framework de Privacidade e Segurança da Informação v1 e respectivas evoluções desta versão (1.1, 1.2, 1.3 etc.) elaborado e publicado pela SGD. A medida do controle 22 que está contemplada por este modelo é a 22.1.

Cada vez mais o Governo utiliza a 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, obedecidos 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.

A proteção dessas informações pelo Governo, enquanto agente de tratamento, está designada no art.46. da Lei Geral de Proteção de Dados, sancionada em 14 de agosto de 2018:

> “Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou

> ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”

Importante ressaltar que adoção deste modelo não dispensa o órgão de observar e considerar as diretrizes gerais estabelecidas para implementação da Política de Segurança da Informação, conforme prevê o art.12, Inciso IV da Instrução Normativa Nº 01/GSI/PR, bem como os Capítulos III e IV da Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021, a qual dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. Adicionalmente devem ser observadas as diretrizes estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD), pela Lei Geral de Proteção de Dados Pessoais (LGPD) e outras normas vigentes.

O Modelo de Política de Segurança da Informação é um normativo institucional que tem o papel de estabelecer regras, diretrizes e práticas para a segurança da informação dentro de uma organização. Visa a garantir a confidencialidade, integridade e disponibilidade da informação, assegurando seu uso adequado e a mitigação de riscos à segurança da informação. Estipular papéis e responsabilidades claras e objetivas, definir diretrizes de segurança e estabelecer meios de monitoramento do cumprimento da política são processos muito importantes para garantir a segurança da informação.

3 Política de Segurança da Informação

IMPORTANTE: Este modelo deve ser utilizado exclusivamente como referência, devendo o órgão ou entidade considerar as particularidades técnicas especificas 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 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 preto antes do processo de aprovação.

4 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 segurança da informação. Além disso, demonstre os objetivos básicos da política e o que ela pretende alcançar.

Exemplo: Esta Política de Segurança da Informação tem como objetivo estabelecer os princípios, diretrizes, responsabilidades e práticas para a proteção das informações do(a) [Órgão ou Entidade]. A Política visa garantir a confidencialidade, integridade e disponibilidade das informações, assegurando o seu uso adequado e a mitigação de riscos à segurança da informação, bem como o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras normas vigentes.

[Acrescente aqui mais definições sobre o propósito da Política de Segurança da Informação que julguem necessárias]

5 Escopo

Amplitude, alcance da Política

Defina a quem e a quais ativos 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:

Instituir a Política de Segurança da Informação (PSI), no âmbito do(a) [Órgão ou Entidade], com a finalidade de estabelecer princípios e diretrizes para a implementação de ações e controles que garantam a segurança das informações e de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas.

Esta Política se aplica a todos os ativos de informação do(a) [Órgão ou Entidade], incluindo dados, sistemas, aplicativos, dispositivos e redes. A Política se aplica a todos os colaboradores, funcionários, contratados, parceiros e terceiros que acessam ou processam as informações do(a) [Órgão ou Entidade]. Esta política se aplica em todas as instalações físicas administradas ou utilizadas pelo ao(a) [Órgão ou entidade] e entidades subsidiárias.

[Acrescente aqui mais definições sobre o escopo da Política de Segurança da Informação que julguem necessárias]

6 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:

CONFIDENCIALIDADE: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

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

DADO PESSOAL SENSÍVEL: 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, quando vinculado a uma pessoa natural;

DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

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

TITULAR DO DADO: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

[Acrescente aqui mais termos-chave, siglas ou conceitos que julguem necessários]

7 Declarações da política

Regras aplicáveis ao caso específico

Descreva aqui as diretrizes ou regras que compõem a política. Normalmente, é apresentado em forma de declarações prescritivas. A divisão desta seção em subseções pode ser necessária dependendo da complexidade da política.

Art. 1º. Fica instituída a Política de Segurança da Informação do [Órgão ou entidade], com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação.

Art. 2º. Esta Política de Segurança da Informação aplica-se a todas as unidades organizacionais do(a) [Órgão ou entidade], e deverá ser observada por todos os usuários de informação, seja servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade deste(a) [Órgão ou entidade].

CAPÍTULO I - Disposições Gerais

Art. 3º. São objetivos da Política de Segurança da Informação:

I. estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;
II. estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;
III. estabelecer competências e responsabilidades quanto à segurança da informação;
IV. nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;
V. promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional do(a) [Órgão ou entidade].

[liste outros que julgar necessário]

Art. 4º. Para os efeitos desta Portaria e de suas regulamentações, aplicam-se os termos do Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

CAPÍTULO II - Dos Princípios e Diretrizes

Art. 5º. As ações de segurança da informação do(a) [Órgão ou Entidade] são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes princípios:

I. disponibilidade, integridade, confidencialidade e autenticidade das informações;
II. continuidade dos processos e serviços essenciais para o funcionamento do(a) [Órgão ou Entidade];
III. economicidade da proteção dos ativos de informação;
IV. respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;
V. observância da publicidade como preceito geral e do sigilo como exceção;
VI. responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;
VII. alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico do(a) [Órgão ou Entidade], assim como demais normas específicas de segurança da informação da Administração Pública Federal;
VIII. conformidade das normas e das ações de segurança da informação com a legislação regulamentos aplicáveis; e
IX. educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.
[liste outros que julgar necessário]

Art. 6º. Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito deste [Órgão ou Entidade] e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 7º. As normas, procedimentos, manuais e metodologias de segurança da informação do [Órgão ou Entidade] devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 8º. As ações de segurança da informação devem:

I. considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do(a) [Órgão ou Entidade];
II. ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades do(a) [Órgão ou Entidade];
III. ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;
IV. visar à prevenção da ocorrência de incidentes.
[liste outros que julgar necessário]

Art. 9º. O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos ao [Órgão ou Entidade].

Art. 10. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada no(a) [Órgão ou Entidade] compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

Parágrafo único. As informações citadas no caput, que tramitem pelo ambiente computacional do(a) [Órgão ou Entidade], são passíveis de monitoramento e auditoria pelo(a) [Órgão ou Entidade], respeitados os limites legais.

Art. 11. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Parágrafo único. É condição para acesso aos recursos de tecnologia da informação do(a) [Órgão ou Entidade] a assinatura, preferencialmente eletrônica, de Termo de Responsabilidade indicando a ciência aos termos desta Política, as responsabilidades e os compromissos em decorrência deste acesso, bem como as penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação do(a) [Órgão ou Entidade].

Art. 12. A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação do(a) [Órgão ou Entidade], devem ser divulgadas amplamente a todos os Usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º Os Usuários de Informação devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§ 2º As ações de capacitação previstas no § 1º devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Art. 13. Todos os contratos de prestação de serviços firmados pelo(a) [Órgão ou Entidade] conterão cláusula específica sobre a obrigatoriedade de atendimento à esta Política de Segurança da Informação, bem como se suas normas decorrentes.

CAPÍTULO III - Da Gestão de Segurança da Informação

Art. 14. A estrutura de Gestão de Segurança da Informação é composta por:

I. Alta Administração;
II. Comitê de Segurança da Informação;
III. Gestor de Segurança da Informação;

IV. Gestor de Tecnologia da Informação e Comunicação;
V. Encarregado pelo Tratamento de Dados Pessoais;
VI. Responsável pela Unidade de Controle Interno;
VII. Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos; e
VIII. Usuários de Informação.
[liste outros que julgar necessário]

Art. 15. Compete à Alta Administração:

I. fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação do [Órgão ou Entidade], bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados; e
II. formalizar e aprovar a Política de Segurança da Informação do [Órgão ou Entidade], bem como suas alterações e atualizações.

[liste outras que julgar necessário]

Art. 16. Compete ao Comitê de Segurança da Informação:

I. assessorar na implementação das ações de segurança da informação;
II. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
III. participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;
IV. propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;
V. deliberar sobre normas internas de segurança da informação;
VI. avaliar as ações propostas pelo gestor de segurança da informação.
[liste outros que julgar necessário]

Parágrafo único. A composição, estrutura, recursos e funcionamento do Comitê de Segurança da Informação será definido em [ato administrativo próprio] emitido pelo(a) [Órgão ou Entidade], de acordo com a legislação vigente.

Art. 17. Compete ao Gestor de Segurança da Informação:

I. coordenar o Comitê de Segurança da Informação;
II. coordenar a elaboração da Política de Segurança da Informação - PSI e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;
III. assessorar a Alta Administração na implementação da Política de Segurança da Informação;

IV. estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V. promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;

VI. incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;

VII. propor recursos necessários às ações de segurança da informação;

VIII. acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

IX. verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

XI. manter contato direto com o Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação;

[liste outros que julgar necessário]

Parágrafo único. O Gestor de Segurança da Informação do(a) [Órgão ou entidade] será designado em [ato administrativo próprio], de acordo com a legislação vigente.

Art. 18. Compete ao Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/ME nº 778, de 4 de abril de 2019, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.

[liste outras que julgar necessário]

Art. 19. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

[liste outras que julgar necessário]

Art. 20. Compete ao Responsável pela Unidade de Controle Interno, dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

[liste outras que julgar necessário]

Art. 21. Compete à Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

I. facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no(a) [Órgão ou entidade];
II. monitorar as redes computacionais;
III. detectar e analisar ataques e intrusões;
IV. tratar incidentes de segurança da informação;
V. identificar vulnerabilidades e artefatos maliciosos;
VI. recuperar sistemas de informação;
VII. promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação;
[liste outros que julgar necessário]

Parágrafo único. A composição, estrutura, recursos e funcionamento da Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos serão definidos em [ato administrativo próprio] emitido pelo(a) [entidade], de acordo com a legislação vigente.

Art. 22. Compete aos Usuários de Informação conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação do(a) [Órgão ou entidade].

Parágrafo único. Todos os Usuários de Informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

[liste outras que julgar necessário]

Art. 23. A Política de Segurança da Informação e demais normativos decorrentes desta Política integram o arcabouço normativo da Gestão de Segurança da Informação.

Art. 24. A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

I. tratamento da informação;
II. segurança física e do ambiente;
III. gestão de incidentes em segurança da informação;
IV. gestão de ativos;
V. gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;
VI. controles de acesso;
VII. gestão de riscos;
VIII. gestão de continuidade;
IX. auditoria e conformidade;
[liste outros que julgar necessário]

§ 1º O Comitê de Segurança da Informação poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

§ 2º Para cada um dos processos que constituem a Gestão de Segurança da Informação, deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o seu entendimento em conformidade com a legislação vigente e boas práticas de segurança de informação.

Art. 25. As políticas, normas, procedimentos, orientações ou manuais de que trata o §2º do art. 16 devem abordar, no mínimo, aspectos relacionados:

I. a conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidas pela ANPD;
II. a classificação da informação de acordo com seu nível de confidencialidade e criticidade, entre outros fatores, com vistas a determinar os controles de segurança adequados;
III. a proteção dos dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;
IV. ao uso aceitável da informação e a utilização de mídias de armazenamento;
V. a entrada e saída de ativos de informação das instalações da organização;
VI. aos perímetros de segurança da organização;
VII. aos controles de acesso baseados no princípio do menor privilégio;
VIII. as etapas de identificação, contenção, erradicação e recuperação e atividades pós incidente;
IX. aos critérios para a comunicação de incidentes aos titulares de dados pessoas e a ANPD;
X. ao Plano de Gestão de Incidentes de Segurança, de forma a considerar diferentes cenários;
XI. a Política de Gestão de Ativos da organização, abordando aspectos relacionados à proteção dos ativos, sua classificação de acordo com a criticidade do ativo para o a organização; a manutenção de inventario atualizado de ativos da organização, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança; uso aceitável de ativos, vedado o uso para fins particulares de seu responsável; o mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências; o monitoramento de ativos, de acordo com os princípios legais de Segurança da Informação e privacidade; a investigação de sua operação e uso quando houver indícios de quebra de segurança e/ou privacidade;
XII. a utilização adequada dos recursos operacionais e de comunicações fornecidos pelo [Órgão ou entidade], a serem utilizados para fins profissionais, relacionados às atividades do(a) [Órgão ou entidade], em conformidade com os princípios éticos e profissionais do(a) [Órgão ou entidade], evitando comportamentos antiéticos,

discriminatórios, ofensivos ou que possam comprometer a reputação do(a) [Órgão ou entidade];

XIII. aos procedimentos para o uso de e-mail, o envio de informações confidenciais, a instalação de software antivírus e a abertura de anexos de e-mail;

XIV. o acesso à internet, o download de arquivos da internet, vedado o uso de sites inadequados e a instalação de software não autorizado;

XV. o uso de mídias sociais, a divulgação de informações nas mídias sociais, o uso de contas pessoais para fins profissionais e a interação com estranhos nas mídias sociais;

XVI. as políticas e procedimentos para o uso da computação em nuvem, a seleção de provedores de serviços em nuvem, a segurança dos dados na nuvem e a conformidade com as leis e regulamentos aplicáveis;

XVII. as políticas e procedimentos para o controle de acesso, tais como o uso de Múltiplo Fator de Autenticação (MFA), controles de autorização, baseados no princípio do menor privilégio, controles de segregação de funções, trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para os ativos de informação, desligamento ou afastamento de colaboradores e parceiros que utilizam ou operam os ativos de informação do(a) [Órgão ou entidade];

XVIII. as políticas e procedimentos para a gestão dos riscos de segurança da informação que possam afetar seus ativos de informação, abordando a análise do ambiente do(a) [Órgão ou entidade], dos seus ativos de informação e das ameaças à segurança da informação; a adoção de uma metodologia estruturada para identificar riscos, a documentação dos riscos identificados, incluindo sua descrição, origem, impacto potencial e probabilidade de ocorrência; a avaliação de riscos, de forma a determinar o risco a se concretizar e o impacto potencial nos ativos de informação, bem como quais riscos devem ser priorizados para tratamento; o tratamento dos riscos identificados e avaliados, o que pode incluir a mitigação de riscos, por meio da implementação de controles de segurança, ou a aceitação de riscos;

XIX. as políticas e procedimentos para Gestão de Continuidade de Negócios da organização, incluindo o Plano de Continuidade para garantir que o(a) [Órgão ou entidade] possa continuar suas atividades em caso de um incidente de segurança da informação e a realização de testes e exercícios periódicos baseados no Plano de Continuidade para garantir sua eficácia;

XX. as políticas e procedimentos para a Gestão de Mudanças nos ativos de informação da organização, respaldado pelas informações dos relatórios de avaliação e tratamento de risco de segurança da informação, com a designação de papéis e responsabilidades para a avaliação, aprovação e implementação de mudanças e a criação de um processo formal para solicitação e documentação de mudanças;

XXI. as políticas e procedimentos para a auditoria e conformidade da organização, abordando o Plano de Verificação de Conformidade, que considere as unidades abrangidas, os aspectos para verificação da conformidade, as ações e atividades a serem realizadas,

os documentos necessários para a fundamentação da verificação de conformidade e as responsabilidades e o Relatório de Avaliação de Conformidade, que considere o detalhamento das ações e das atividades com identificação do responsável, o parecer de conformidade e as recomendações.

[liste outros que julgar necessário]

§ 1º As unidades organizacionais do(a) [Órgão ou entidade] devem realizar periodicamente auditorias internas de sua segurança da informação para assegurar que ela esteja em conformidade com esta Política e com outros requisitos de segurança da informação aplicáveis.

§ 2º Todas as ações, realizadas pelas unidades do(a) [Órgão ou entidade], que envolvem a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis à esta temática.

§ 3º As atividades, produtos e serviços desenvolvidos no(a) [Órgão ou entidade] devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes

CAPÍTULO IV - Das Vedações e Disposições Finais

Art. 26. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pelo [Órgão ou entidade] para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 27. São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pelo [Órgão ou entidade].

Art. 28. É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

Art. 29. É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

[liste outros que julgar necessário]

Art. 30. A unidades organizacionais do(a) [Órgão ou entidade] devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

Art. 31. As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através dos seguintes canais:

[inserir lista de canais de denúncia]

Art. 32. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados pelo(a) [Órgão ou entidade] periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 33. A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Art. 34. Esta Política será revisada periodicamente, pelo menos a cada quatro anos, ou com mais frequência se necessário, para refletir as mudanças no ambiente do(a) [Órgão ou entidade], nos riscos à segurança da informação e nas melhores práticas de segurança da informação.

Art. 35. Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e seus documentos devem ser submetidas ao Comitê de Segurança da Informação.

[liste outras que julgar necessário]

Referências Bibliográficas

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27001:2022: **Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos**. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27002:2022: **Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação— Requisitos**. Rio de Janeiro, 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: 02 jul. 2024.

BRASIL. Presidência da República. Casa Civil. Instituto Nacional de Tecnologia da Informação. **Portaria N° 79, de 31 de dezembro de 2018. Política de Segurança da Informação e Comunicações do Instituto Nacional de Tecnologia da Informação**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015- 2018/2018/Lei/L13709.htm. Acesso em: 02 jul. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **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.html. Acesso em: 17 jun. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional**. Portaria nº 93, de 26 de setembro de 2019. Glossário de Segurança da Informação**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-%20219115663. Acesso em: 01 jul. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa nº 01, de 27 de maio de 2020. Brasília, DF, GSI/PR, 2020**. Disponível em: https://www.gov.br/gsi/ptbr/composicao/SSIC/dsic/legislacao/copy_of_IN01_consolidada.pdf. Acesso em: 01 jul. 2024.

BRASIL. 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: 01 jul. 2024.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação. Março 2024**. Disponível em:https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf . Acesso em: 25 jun. 2024.

BRASIL. Presidência da República. Agência Nacional de Proteção de Dados - ANPD. **Guia Orientativo - Tratamento de dados pessoais pelo Poder Público. Junho 2023.** Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 01 jul. 2022.