gov.br

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Modelo de Política de Gestão de Controle de Acesso

Programa de Privacidade e Segurança da Informação – PPSI

Versão 2.3
Brasília, março de 2025

MODELO DE POLÍTICA DE GESTÂO DE CONTROLE DE ACESSO

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
Amaury C. da Silveira Junior
Anderson Souza de Araújo
Eder Ferreira de Andrade
Francisco Magno Felix Nobre
Guilherme Rufino Junior
Guilherme Mendonça Medeiros
Heráclito Ricardo Ferreira Gomes
Ivaldo Jeferson de Santana Castro
Yuri Arcanjo de Carvalho
Ramon Caldas

Equipe Revisora
Marcelo de Lima
Marcus Paulo Barbosa Vasconcelos
Sumaid Andrade de Albuquerque

Equipe Técnica de Revisão – Versão 2.2
Adriano de Andrade Moura
Anderson Souza de Araújo

Francisco Magno Felix Nobre
Ivaldo Jeferson de Santana Castro
Leonard Keyzo Yamaoka Batista
Raphael César Estevão
Rogério Vinícius Matos Rocha

Equipe Técnica de Revisão – Versão 2.3
Adriano de Andrade Moura
Anderson Souza de Araújo
Andressa Vieira Bueno Popinigis
Bruno Pierre Rodrigues de Sousa
Ivaldo Jeferson de Santana Castro
Leonard Keyzo Yamaoka Batista
Marta Juvina de Medeiros
Raphael César Estevão

Histórico de versões

Data	Versão	Descrição	Autor
01/04/2022	1.0	Modelo de Política de Controle de Acesso.	Equipe Técnica de Elaboração.
05/05/2022	1.1	Modelo de Política de Controle de Acesso.	Equipe Técnica de Elaboração.
16/08/2022	1.2	Remoção das referências à NC nº 7/IN01/DSIC/GSIPR revogada pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR e ajustes nos textos que indicam que deve ser informado o nome do órgão/entidade.	Equipe Técnica de Atualização.
31/03/2022	2.0	Atualização para alinhamento com o Guia do *Framework* de Privacidade e Segurança da Informação, conforme destacado no Anexo II.	Equipe Técnica de Revisão.
14/05/2024	2.1	Atualização para melhor atender às medidas 31.3, 31.4 e 31.6 do Guia do *Framework* de Privacidade e Segurança da Informação, conforme destacado no Anexo II.	Equipe Técnica de Revisão.
18/06/2024	2.2	Atualização para melhor atender às medidas 12.5, 12.6 e 12.7 do Guia do *Framework* de Privacidade e Segurança da Informação, conforme destacado no Anexo II.	Equipe Técnica de Revisão.
31/01/2025	2.3	Atualização para padronização da diagramação do documento e ajustes pontuais do texto nas seções Introdução, Política de Controle de Acesso, Referência legal e de boas práticas e reestruturação da seção Declarações da política. Adequação do Modelo à Resolução CD/ANPD nº 18, de 16 de julho de 2024.	Equipe Técnica de Revisão.

Sumário

1 Aviso preliminar e agradecimentos 6
2 Introdução 8
3 Política de Controle de Acesso 10
4 Propósito 11
5 Escopo 12
6 Termos e definições 13
7 Referência legal e de boas práticas 14
8 Declarações da política 16
CAPÍTULO I – DO ACESSO LÓGICO 16
CAPÍTULO II – DAS CONTAS DE ACESSO LÓGICO 18
8.1 CAPÍTULO III – BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO 19
CAPÍTULO IV – ACESSO FÍSICO 20
CAPÍTULO V – MOVIMENTAÇÃO INTERNA E CONTA DE ACESSO BIOMÉTRICO 22
CAPÍTULO VI – ADMINISTRADORES 22
CAPÍTULO VII – RESPONSABILIDADES 23
CAPÍTULO VIII – DISPOSIÇÕES FINAIS 25
9 Anexo I 26
9.1 Modelo de Termo de Responsabilidade 26
10 Anexo II 28

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 Controle de Acesso, 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 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 dos dados que estão sob sua custódia. Adicionalmente, a elaboração de uma Política de Controle de Acesso visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Secretaria de Governo Digital – SGD do Ministério da Gestão e da Inovação em Serviços Públicos, 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 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, e vice-versa;
b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
c) não é coautora das publicações internacionais abordadas;
d) não assume nenhuma 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 aos requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referência Legal e de Boas Práticas” deste documento.

Um agradecimento especial deve ser registrado ao CIS, à ISO, 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 à privacidade e segurança da informação e outras referências utilizadas neste documento.

2 Introdução

A gestão de contas e controle de acesso é o processo de criação, provisionamento, uso e encerramento de contas e credenciais na instituição. A política de gestão de contas e controle de acesso, por sua vez, fornece os processos e procedimentos para governar o ciclo de vida da gestão das contas e credenciais.

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 Controle de Acesso no âmbito institucional.

O presente documento serve como um modelo prático a ser utilizado para auxiliar na adoção de medidas dos Controles 5, 6, 12 e 31 do Guia do *Framework* de Privacidade e Segurança da Informação[1] v1, e respectivas evoluções desta versão (1.1, 1.2 etc.), elaborado e publicado pela SGD, que assim estabelecem:

Controle 5: Gestão de Contas – Usar processos e ferramentas para atribuir e gerenciar autorização de credenciais para contas de usuário, contas de administrador, contas de serviço para ativos e softwares institucionais.

Controle 6: Gestão do Controle de Acesso – Usar processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e *software* institucionais.

Controle 12: Gestão da Infraestrutura de Redes – Estabeleça, implemente e gerencie ativamente (rastreie, reporte, corrija) os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.

Controle 31: Segurança Aplicada à Privacidade – 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.

As medidas dos Controles 5, 6, 12 e 31 que estão contempladas por este modelo são: 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 12.3, 12.5, 12.6, 12.7, 31.3, 31.4 e 31.6.

[1] Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf>. Acesso em: 21 jan. 2025.

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.

Nesse contexto, os entes federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem dados pessoais e informações 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* 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.

A proteção dos dados pessoais pelo Governo, enquanto agente de tratamento, está designada no art. 46. da Lei Geral de Proteção de Dados Pessoais, 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 a adoção deste modelo não dispensa o ente público de 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.

3 Política de Controle de Acesso

Este modelo tem por foco prover diretrizes para o controle de acesso, a fim de atender à necessidade de implementar os controles emergenciais previstos no anexo 5 do Programa de Privacidade e Segurança da Informação – PPSI. Contudo, recomenda-se que o órgão ou entidade considere, no mínimo, as diretrizes gerais estabelecidas para implementação da Política de Segurança da Informação, conforme prevê o art. 12, inciso IV, da Instrução Normativa 01/GSI/PR, em especial as diretrizes para controle de acesso (lógico e físico), referenciadas na alínea f do referido inciso.

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 especificas 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 autorização da implementação desta política]
Políticas Relacionadas	[Relacione outras políticas corporativas relacionadas dentro ou externas a este modelo, por exemplo: POSIN]
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 Gestão de Controle de Acesso

4 Propósito

Objetivo da Política conforme IN01 GSI/PR Art. 11.

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

Exemplo: A Política de Controle de Acesso objetiva estabelecer controles de autenticação, autorização e auditoria para salvaguardar as informações do [Órgão ou Entidade], estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que implique risco de destruição, alteração, perda, roubo ou divulgação indevida.

Sem controles de autenticação, autorização e auditoria, existe o risco potencial de que os ativos de informação possam ser acessados ilicitamente e que a segurança desses ativos seja comprometida.

Considera-se, portanto, que as credenciais crachá de identificação funcional e logins de acesso dos ativos de informações são pessoais e intransferíveis e representam o único método legítimo pelo qual o direito de acesso físico ou lógico podem ser exercidos.

Os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação do [Órgão ou Entidade].

5 Escopo

Amplitude: alcance da Política, conforme IN01 GSI/PR, art. 12, item I.

Defina a quem e a quais ativos esta Política se aplica. Liste os agentes públicos e 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 se aplica a todas as informações, cujo [Órgão ou Entidade] é responsável pelo tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e às dependências físicas desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento.

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].
- todos os funcionários de parceiros que acessam fisicamente as dependências ou que acessam ativos de informação do [Órgão ou Entidade].

6 Termos e definições

Glossário, conforme IN01 GSI/PR, art.12, item II.

Defina quaisquer termos-chave, siglas ou conceitos que serão utilizados na Política. Sugere-se utilizar como referência as definições apresentadas na 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:

ACESSO – ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

CONTA DE SERVIÇO – conta de acesso à rede corporativa de computadores, necessária a um procedimento automático (aplicação, *script*, entre outros) sem qualquer intervenção humana no seu uso;

CONTROLE DE ACESSO – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

MFA – sigla de autenticação de multifatores (*multi-factor authentication*).

7 Referência legal e de boas práticas

Documentos norteadores

Se for aplicável, liste quaisquer leis, regulamentos ou guias de boas práticas que regem a Política ou com os quais a Política deve estar em conformidade ou ser cumprida. Confirme com o departamento jurídico que a lista é completa e precisa.

Orientação	Seção
Decreto nº 12.198, de 2024 – Estratégia de Governo Digital 2024-2027.	Em sua íntegra
Lei nº 13.709, de 2018 – Lei Geral de Proteção de Dados Pessoais.	Arts. 46 e 50
Decreto nº 9.573 – Política Nacional de Segurança de Infraestruturas Críticas – PNSIC.	Anexo, art. 3, inciso I
Decreto nº 9.637, de 2018 – Política Nacional de Segurança da Informação – PNSI.	Art. 2, incisos III e IV, art. 3, inciso XI e art.15
Decreto nº 10.222, de 2020 – Estratégia Nacional de Segurança Cibernética – E-Ciber.	Anexo, itens 2.3.4 e 2.3.5
Decreto nº 10.046, de 2019 – Governança no Compartilhamento de Dados – GCD.	Art. 2, inciso XXIII
Instrução Normativa nº 01/GSI/PR/2020.	Art. 12, inciso IV, alínea f
ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de Segurança da Informação.	Itens 9 – 11.2.9
CIS *Critical Security Control* v8.	Capítulos 5, 6 e 12
Guia do *Framework* de Privacidade e Segurança da Informação.	Controles 5, 6, 12 e 31
Instrução Normativa nº 04/GSI/PR/2020.	Capítulo II
Portaria GSI/PR nº 93, de 2021.	Em sua íntegra
Account and Credential Management Policy Template for CIS Controls 5 and 6.	Em sua íntegra
ABNT NBR ISO/IEC 27701: 2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC	Itens 6 – 6.6.2

27002 para gestão da privacidade da informação — Requisitos e Diretrizes.	
ISO/IEC FDIS 29151:2016(E). *Information technology — Security techniques — Code of practice for personally identifiable information protection.*	Itens 9 – 9.2.2 e 9.2.3
GSI 09/2023. OSIC[2] (ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA) — Gestão de Acesso Privilegiado (*Privileged Access Management* – PAM) – parte 2 de 2.	Em sua íntegra
Resolução CD/ANPD Nº 18, de 2024.	Em sua íntegra

Quadro 2 – Referência legal e de boas práticas

[2] Disponível em: <https://www.gov.br/gsi/pt-br/ssic/osic/OSIC%2009.23>. Acesso em: 21 jan. 2025.

8 Declarações da política

Regras aplicáveis ao caso específico

Descreva as regras 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 extensão ou complexidade da política.

Art. 1º Fica aprovada, no âmbito do [Órgão ou Entidade], a Política de Gestão de Controle de Acesso para criação e administração de contas de acesso, em complemento às diretrizes estabelecidas pelo Capítulo [xxx], da Política de Segurança da Informação – POSIN do [Órgão ou Entidade].

Art. 2° O acesso aos ativos de informação do [Órgão ou Entidade] está restrito aos seus colaboradores no âmbito do exercício de suas atividades, funções e responsabilidades observando-se sempre o princípio do menor privilégio.

Parágrafo único. Para fins desta Política, os colaboradores mencionados no *caput* são considerados usuários dos recursos de tecnologia da informação e demais ativos de informação do [Órgão ou Entidade].

CAPÍTULO I – DO ACESSO LÓGICO

Art. 3º O acesso lógico aos recursos da rede local do [Órgão ou Entidade] é realizado por meio de sistema de controle de acesso.

§ 1º Compete à [Unidade responsável pela Gestão de Controle dos Acessos] administrar o acesso dos usuários baseado em suas funções e responsabilidades.

§ 2º A [Unidade responsável pela Gestão de Controle dos Acessos] deve realizar, periodicamente ou quando novas funções e ativos de informação sejam inseridos na organização, análises de controle de acesso nos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função.

Art. 4º Os acessos lógicos serão concedidos e mantidos pela [Unidade responsável pela Gestão de Controle dos Acessos], considerando o disposto no § 1º do art. 3º e o seguinte:

I. terão direito a acesso lógico aos recursos da rede local os usuários de recursos de tecnologia da informação;
II. o acesso remoto aos recursos do [Órgão ou Entidade] deve ser realizado por meio de Rede Virtual Privada (*Virtual Private Network* – VPN), após as devidas autorizações;
III. quando suportado pelo ativo, é obrigatória a utilização de Múltiplos Fatores de Autenticação – MFA para a autenticação de acessos remotos;

IV. quando suportado pelos ativos, o acesso a todas as aplicações corporativas ou de terceiros que estejam hospedadas em fornecedores deve utilizar MFA.
V. [Inserir outros itens que julgar necessários].

Art. 5º A concessão de acesso aos usuários que lidam com dados pessoais é limitada, estritamente, aos sistemas que processam esses dados e para cumprir as finalidades a que se destinam em conformidade ao princípio da necessidade mencionado na Lei Geral de Proteção de Dados Pessoais – LGPD.

Parágrafo único. Ao atribuir ou revogar os direitos de acesso, a [Unidade Responsável pela Gestão de Controle dos Acessos] deve:

I. verificar se o nível de acesso concedido é apropriado às operações de tratamento de dados pessoais, além de ser consistente com outros requisitos, tal como a segregação de funções;
II. assegurar que os direitos de acesso não foram ativados antes que o procedimento de autorização esteja completo;
III. manter um registro preciso e atualizado dos perfis de acesso criados, incluindo a relação dos usuários autorizados e as matrizes de acesso correspondentes a cada um, em relação ao respectivo ativo de informação;
IV. manter atualizados os direitos de acesso dos usuários que tenham mudado de função ou de atividades, e imediata remoção ou bloqueio dos direitos de acesso dos usuários que não estão mais vinculados ao [Órgão ou Entidade];
V. analisar criticamente os direitos de acesso em intervalos regulares.
VI. [Inserir outros itens que julgar necessários].

Art. 6º A [Unidade responsável pela Gestão de Controle dos Acessos] deverá manter um inventário de todas as contas gerenciadas, incluindo contas de usuário, administrativas, de testes e de serviço.

§ 1º O inventário das contas de serviço deve abranger no mínimo, informações sobre:

I. unidade organizacional gestora do serviço;
II. data de criação/última autorização de renovação de acesso.
III. [Inserir outros itens que julgar necessários].

§ 2º Compete à [Unidade responsável pela Gestão de Controle dos Acessos] validar todas as contas ativas do [Órgão ou Entidade], [a cada 90 (noventa) dias].

Art. 7º A [Unidade Responsável pela Gestão de Controle dos Acessos] deverá manter um inventário dos sistemas de autenticação e autorização do [Órgão ou Entidade], revisado periodicamente.

Art. 8º Quando suportadas a autenticação, a autorização e a auditoria (AAA) dos ativos de informação da infraestrutura de rede do [Órgão ou Entidade] devem ser geridas de forma centralizada, se possível, por meio de um serviço de diretório ou provedor de autenticação única, como o *Single Sign-On* – SSO.

Art. 9º O acesso à rede local do [Órgão ou Entidade] dever assegurar que apenas colaboradores e dispositivos autorizados possam interagir com partes específicas da rede, dentre elas, não se limitando:

I. a segmentação de rede;
II. a protocolos de comunicação e redes seguros.
III. [Inserir outros itens que julgar necessários].

CAPÍTULO II – DAS CONTAS DE ACESSO LÓGICO

Art. 10. Para a utilização das estações de trabalho do [Órgão ou Entidade], é obrigatório o uso de uma conta de acesso lógico (login) e senha, fornecidos pela [Unidade Responsável pela Gestão de Controle dos Acessos] mediante solicitação formal do gestor da unidade ao qual o usuário está vinculado.

§ 1º O formulário de solicitação de criação de conta de acesso se encontra disponível para preenchimento no [local] do [Órgão ou Entidade];

§ 2º Os privilégios de acesso dos usuários à rede local são definidos pela unidade à qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas atribuições.

§ 3º Na necessidade de utilização de perfil diferente do disponibilizado, o gestor da unidade à qual o usuário está vinculado deverá encaminhar solicitação para a [Unidade Responsável pela Gestão dos Acessos] que a examinará, podendo negá-la nos casos em que entender desnecessária.

Art. 11. O login e a senha são de uso pessoal e intransferível, sendo vedado o seu compartilhamento e a sua divulgação, estando sujeitos ao bloqueio imediato pela [Unidade Responsável pela Gestão de Controle dos Acessos] se constatado o uso indevido ou qualquer irregularidade que possa prejudicar a segurança do [Órgão ou Entidade].

Parágrafo único. No caso do bloqueio citado no *caput*, para retomar o acesso à rede, deverá ser formalizada nova requisição de desbloqueio pelo gestor da unidade à qual o usuário está vinculado.

Art. 12. Preferencialmente, o padrão a ser adotado para o formato da conta de acesso do usuário é a sequência do primeiro nome + ponto + último sobrenome do usuário.

§ 1º Caso seja constatada a existência de uma conta de acesso em uso com o mesmo nome do novo usuário, a [Unidade Responsável pela Gestão de Controle dos Acessos] realizará uma

combinação distinta utilizando as outras possibilidades de sobrenome que conste no nome completo do usuário para o qual a conta está sendo criada.

§ 2º A [Unidade Responsável pela Gestão de Controle dos Acessos] fornecerá uma senha temporária para cada conta de acesso criada, que deverá ser alterada pelo usuário quando do primeiro acesso à rede local.

Art. 13. O padrão adotado para o formato da senha é o definido pela [Unidade Responsável pela Gestão de Controle dos Acessos], considerando o seguinte:

I. a obrigatoriedade do uso de letras maiúsculas, minúsculas e números, com tamanho mínimo de oito caracteres para contas que utilizam MFA e 14 caracteres para as contas que não utilizam MFA;
II. a recomendação de utilização de letras maiúsculas, minúsculas e caracteres especiais (ex: $, %, &);
III. a não utilização de sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações, ou ainda termos óbvios, tais como: Brasil, senha, usuário, *password* ou *system;*
IV. a não reutilização das últimas [5 (cinco)] senhas.
V. [Inserir outros itens que julgar necessários].

Art. 14. As senhas de acesso possuem validade de [90 (noventa)] dias, devendo o usuário efetuar a troca ao ser notificado.

Parágrafo único. Caso a mudança da senha não seja efetuada no prazo estabelecido, o login será bloqueado, impossibilitando seu acesso à rede local até que seja realizada solicitação de desbloqueio e uma nova senha seja atribuída.

8.1 CAPÍTULO III – BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 15. A conta de acesso será bloqueada nos seguintes casos:

I. após [5 (cinco)] falhas consecutivas de tentativas de acesso;
II. mediante solicitação do superior imediato do usuário, com a devida justificativa;
III. quando da suspeita de uso indevido dos serviços disponibilizados pelo [Órgão ou Entidade] ou de descumprimento da POSIN e normas correlatas em vigência;
IV. após [45 (quarenta e cinco)] dias consecutivos sem utilização pelo usuário.
V. [Inserir outros itens que julgar necessários].

Art. 16. O desbloqueio da conta de acesso à rede local será realizado mediante solicitação formal, com justificativa, do gestor imediato ao qual o usuário está vinculado à [Unidade Responsável pela Gestão de Controle dos Acessos].

Art. 17. Quando do afastamento temporário do usuário, a conta de acesso deverá ser bloqueada a pedido do superior imediato ou da [Unidade de Gestão de Pessoas].

Art. 18. A conta de acesso não utilizada há mais de [180 (cento e oitenta)] dias deverá ser cancelada.

Art. 19. O processo formal de cancelamento de usuários que administram ou operam sistemas e serviços é estabelecido pela [Unidade Responsável pela Gestão de Controle dos Acessos] e deve incluir:

I. a desativação ou exclusão imediata de usuário que tenha deixado o [Órgão ou Entidade];
II. em caso de usuários com acesso privilegiado, a [Unidade Responsável pela Gestão de Controle dos Acessos] prioriza a revogação ou a desativação de contas com o objetivo de manter dados e *logs* para possíveis auditorias.
III. [Inserir outros itens que julgar necessários].

Art. 20. A [Unidade de Tecnologia da Informação] deve configurar bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido.

Parágrafo único. O período de inatividade de que trata o *caput* é específico para cada tipo de ativo e deve considerar [diretrizes].

CAPÍTULO IV – ACESSO FÍSICO

Art. 21. A [Unidade Responsável pela Gestão de Controle dos Acessos] estabelece perímetros de segurança para proteger ambientes e ativos contra acesso físico não autorizado, danos e interferências, com base nas diretrizes a seguir dispostas:

I. indicação da localização e resistência dos perímetros de acordo com os requisitos de segurança da informação relacionados aos ativos que se encontre dentro dos perímetros;
II. proteção dos ambientes seguros contra acessos não autorizados por meio de mecanismos de controle de acesso, como fechaduras tradicionais ou digitais, que possibilitem autenticação por biometria, senhas, PIN (*Personal Identification Number*) ou cartões de acesso;
III. execução de testes nos mecanismos de controle de acesso em períodos pré-definidos para assegurar a funcionalidade total dos equipamentos;
IV. monitoramento dos mecanismos de controle de acesso por parte da [Unidade ou Equipe Responsável pela Monitoração];
V. estabelecimento de uma área de recepção ou outros meios de controle de acesso físico a ambientes em que não for conveniente a implementação de mecanismos de controle de acesso.
VI. [Inserir outros itens que julgar necessários].

Art. 22. O acesso físico a ambientes seguros ou ativos de tratamento e armazenamento de dados do [Órgão ou Entidade] é destinado apenas a pessoal autorizado.

Parágrafo único. A [Unidade Responsável pela Gestão de Controle dos Acessos] mantém um processo de gestão de acessos para fornecimento, revisão periódica, atualização e revogação das autorizações.

Art. 23. A [Unidade Responsável pela Gestão de Controle dos Acessos] retém e mantém seguro os *logs* ou registros de todos os acessos físicos aos ativos de informação.

Art. 24. O acesso por fornecedores ou prestadores de serviços a ambientes seguros ou ativos de tratamento e armazenamento de dados que estão nas dependências do [Órgão ou Entidade] será concedido somente quando necessário e de acordo com as seguintes diretrizes:

I. para fins específicos e autorizados;
II. com autorização concedida pela [Unidade Responsável pela Gestão de Controle dos Acessos ou Responsável pelo Ativo];
III. com supervisão e monitoramento.
IV. [Inserir outros itens que julgar necessários].

Art. 25. Os ativos de armazenamento e tratamento de dados que se encontrem fora do [Órgão ou Entidade] devem ser protegidos contra perda, roubos, danos e acesso físico não autorizados, conforme as seguintes diretrizes:

I. manter sempre o ativo em constante vigilância quando em locais públicos e inseguros;
II. proteger o ativo contra riscos associados a visualização de informações por outra pessoa;
III. implementar as funcionalidades de rastreamento e limpeza remota.
IV. [Inserir outros itens que julgar necessários].

Art. 26. A gestão de mídias de armazenamento compete à [Unidade Responsável pela Gestão de Controle dos Acessos] e deve ser realizada de acordo com as seguintes diretrizes:

I. exigir autorização para a saída de mídias de armazenamento do [Órgão ou Entidade];
II. armazenar mídias em local seguro de acordo com a classificação de suas informações;
III. criptografar as mídias de acordo com a classificação de suas informações;
IV. manter cópias de segurança de mídias de acordo com a classificação de suas informações.
V. [Inserir outros itens que julgar necessários].

Art. 27. As condições e restrições pertinentes ao acesso físico nos dispositivos de trabalho remoto são as definidas pela [Unidade Responsável pela Gestão de Controle dos Acessos], levando em consideração as seguintes diretrizes:

I. segurança física do local de trabalho remoto;
II. regras e orientações quanto ao acesso de familiares e visitantes ao dispositivo.
III. [Inserir outros itens que julgar necessários].

CAPÍTULO V – MOVIMENTAÇÃO INTERNA E CONTA DE ACESSO BIOMÉTRICO

Art. 28. Nos casos em que houver transferência de usuário entre setores ou ocupação de nova função pelo usuário, os direitos de acesso à rede local serão revogados.

§ 1º Cabe ao novo superior imediato ou à [Unidade de Gestão de Pessoas] realizar a solicitação de novos acessos de acordo com o novo setor ou a nova função do usuário.

§ 2º Os direitos de acesso antigos serão imediatamente cancelados conforme solicitação do antigo superior imediato ou da [Unidade de Gestão de Pessoas].

Art. 29. Ao implementar as contas de acesso biométrico, quando possível, estas serão vinculadas às contas de acesso lógico e ambas poderão ser utilizadas para se obter um acesso com autenticação multifatores.

Parágrafo único. Os dados biométricos serão tratados como dados com acesso restrito, preferencialmente utilizando-se de criptografia que atenda à legislação vigente.

CAPÍTULO VI – ADMINISTRADORES

Art. 30. A utilização de identificação (login) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas da administração de ativos de informação.

Art. 31. Somente os técnicos da [Unidade de Tecnologia da Informação], devidamente identificados e habilitados, poderão ter senha com privilégios de administrador nos equipamentos locais e na rede.

Art. 32. Em caso de necessidade de utilização de login com privilégio de administrador do equipamento local, o usuário encaminhará a solicitação para a [Unidade Responsável pela Gestão de Controle dos Acessos], a qual poderá negar os casos em que entender desnecessária a utilização.

§ 1º Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal da [Unidade de Tecnologia da Informação].

§ 2º Caso constatada alguma irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

§ 3º A identificação (login) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante.

Art. 33. Salvo para atividades específicas da área responsável pela gestão da [Unidade de Tecnologia da Informação] do órgão, não será concedida, para um mesmo usuário, identificação

(login) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede.

Art. 34. Excepcionalmente, poderá ser concedida identificação (login) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação da [Unidade ou pessoa/função Responsável] por meio da [Unidade Responsável pela Gestão de Controle dos Acessos].

Art. 35. A [Unidade Responsável pela Gestão de Controle dos Acessos] deve implementar o MFA para todas as contas de administrador.

Art. 36. A [Unidade Responsável pela Gestão de Controle dos Acessos] deve gerenciar os privilégios das contas locais de administrador nos ativos de informação de forma que o usuário com privilégio administrativo não consiga realizar atividades gerais de computação, como navegação na Internet, uso do e-mail e do pacote de produtividade.

Parágrafo único. Estas atividades devem ser executadas preferencialmente a partir da conta primária e não privilegiada.

Art. 37. Ao tratar dados pessoais, o [Órgão ou Entidade] observará o princípio da necessidade como regra, para garantir que o usuário receba apenas os direitos mínimos necessários para executar suas atividades; para tanto, podem ser realizadas as seguintes ações:

a. remover os direitos de administrador nos dispositivos finais;
b. remover todos os direitos de acesso *root* ou *admin* aos servidores e utilizar tecnologias que permitam a elevação granular de privilégios conforme a necessidade, ao mesmo tempo em que fornecem recursos claros de auditoria e monitoramento;
c. eliminar privilégios permanentes (privilégios que estão “sempre ativos”) sempre que possível;
d. limitar a associação de uma conta privilegiada ao menor número possível de pessoas;
e. minimizar o número de direitos para cada conta privilegiada.

CAPÍTULO VII – RESPONSABILIDADES

Art. 38. Compete ao superior imediato do usuário comunicar formalmente à [Unidade de Gestão de Pessoas] e à [Unidade Responsável pela Gestão de Controle dos Acessos] o desligamento ou saída do usuário do [Órgão ou Entidade], para que as permissões de acesso à rede local sejam revogadas ou canceladas.

Art. 39. Compete à [Unidade de Gestão de Pessoas] a comunicação imediata à [Unidade Responsável pela Gestão de Controle dos Acessos] sobre desligamentos, férias e licenças de servidores e funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio temporário ou revogação definitiva da permissão de acesso do usuário aos recursos de rede.

Art. 40. Compete à [Unidade de Tecnologia da Informação] realizar o monitoramento da utilização de recursos de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente e sem aviso prévio, o usuário e a estação de trabalho em que esteja realizando atividade que coloque em risco a segurança e integridade da rede, até que seja verificado o caso concreto e descartada qualquer hipótese de dano à infraestrutura tecnológica do [Órgão ou Entidade].

Art. 41. O usuário é responsável por todos os acessos realizados por sua conta de login e por possíveis danos causados à rede local e aos recursos de tecnologia custodiados ou de propriedade do [Órgão ou Entidade].

§ 1º O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, em casos de ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou encerrar a sessão da estação, para coibir acessos indevidos.

§ 2º A utilização simultânea da conta de acesso à rede local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário, titular da conta de acesso, os riscos que a utilização paralela implica.

§ 3º É vedado ao usuário transferir ou compartilhar com outrem sua conta de acesso, e respectiva senha, à rede local.

Art. 42. O usuário deverá informar à [Unidade de Tecnologia da Informação] qualquer situação da qual tenha conhecimento e que configure violação de sigilo ou que possa colocar em risco a privacidade e segurança, inclusive de terceiros.

Art. 43. É dever do usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para o [Órgão ou Entidade], a saber:

I. não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;
II. evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de ativos de informações internos e externos;
III. interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completar suas atividades ou quando se ausentar do local de trabalho por qualquer motivo;
IV. não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenha sido dada autorização de acesso;
V. não divulgar a terceiros dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;
VI. utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e as medidas preventivas estabelecidas;
VII. não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

VIII. assinar o Termo de Responsabilidade (Modelo – Anexo I) quanto à utilização da respectiva conta de acesso.

IX. [Inserir outros itens que julgar necessários].

CAPÍTULO VIII – DISPOSIÇÕES FINAIS

Art. 44. No caso de ciência ou suspeita de algum evento que seja contra o cumprimento desta Política, bem como da Política de Segurança da Informação e das normas de segurança vigentes, o usuário deve comunicar à [Unidade de Tecnologia da Informação].

Art. 45. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a [Unidade de Tecnologia da Informação] realizará uma investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

Art. 46. Nos casos em que o ator da quebra de segurança for um usuário, a [Unidade de Tecnologia da Informação] comunicará os resultados ao seu superior imediato para a adoção de medidas cabíveis.

Art. 47. Ações que violem a POSIN ou que quebrem os controles de segurança da informação serão passíveis de sansões civis, penais e administrativas, conforme a legislação vigente, que podem ser aplicadas isoladamente ou cumulativamente.

Art. 48. Processo administrativo disciplinar específico poderá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela POSIN.

Art. 49. A resolução de casos de violação ou transgressões omissas nas legislações correlatas será resolvida pelo Comitê de Segurança da Informação – CSI do [Órgão ou Entidade].

Art. 50. Esta [Portaria] entra em vigor na data de sua publicação.

9 Anexo I

9.1 Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL

[Órgão ou Entidade]

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo(a) _____, em _____, e lotado no(a)_____deste [Órgão ou Entidade], DECLARO , sob pena das sanções cabíveis nos termos da _____ (legislação vigente), que assumo a responsabilidade por:

I. tratar os ativos de informação como patrimônio do [Órgão ou Entidade];

II. utilizar as informações, em qualquer suporte sob minha custódia, exclusivamente no interesse do serviço do [Órgão ou Entidade];

III. contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IV. utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do [Órgão ou Entidade];

V. responder, perante o [Órgão ou Entidade], pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

VI. acessar a rede corporativa, computadores, Internet e e-mail somente com autorização (usuário e senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e e-mail;

VII. utilizar o correio eletrônico (e-mail) somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e e-mail;

VIII. não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

IX. manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

X. não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (browser), bloquear a estação de trabalho, bem como encerrar a sessão do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;

XI. não revelar minha senha de acesso à rede corporativa, computadores, Internet e do correio eletrônico (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

XII. responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam colocar em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações e dados a que tenha acesso.

[Local], [UF], _____de _____de _____.

_____

Assinatura

[Nome do usuário e seu setor organizacional]

_____

[Nome da autoridade responsável pela autorização do acesso]

10 Anexo II

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nas versões do Modelo de Política de Gestão de Controle de Acesso, em comparação com o documento originalmente publicado em abril de 2022.

Mudanças da Versão 2.3

As mudanças inseridas nesta versão em comparação com a anterior visam promover a adequação do presente modelo com a Resolução CD/ANPD Nº 18, de 16 de julho de 2024, a reestruturação das informações nas seções: Introdução, Política de Controle de Acesso, Referência legal e de boas práticas e Declarações da Política.

Mudanças da Versão 2.2

As mudanças inseridas nesta versão em comparação com a anterior visam a adequação do Modelo com o Controle 12 do Guia do *Framework* de Privacidade e Segurança da Informação.

Destacam-se as seguintes alterações:

- inclusão do controle 12 e respectivas medidas à Introdução;
- inclusão de novas referências adicionando o controle 12 do Guia de *Framework* de Privacidade e Segurança da Informação e a Instrução Normativa Nº 04/GSI/PR;
- inclusão do art. 2º, seção dos princípios gerais, visando atender à medida 12.3 do Controle 12;
- ajustes do texto do Capítulo I, seção sobre Acesso Lógico, para dar ênfase ao gerenciamento de infraestrutura de redes atendendo ao Controle 12, conforme descrito abaixo:
    - inciso I do art. 3º, em atenção à medida 12.6;
    - inciso VI do art. 3º, em atenção à medida 12.5;
    - inciso VIII do art. 3º, em atenção à medida 12.3.

Mudanças da Versão 2.1

As mudanças inseridas nesta versão em comparação com a anterior visam a adequação do Modelo com o Controle 31 do Guia do *Framework* de Privacidade e Segurança da Informação.

Foram realizadas as seguintes inclusões de:

- menção do controle 31 e suas medidas atendidas da Introdução;
- na seção referência legal e de boas práticas, foram inseridas as referências usadas para a atualização dessa versão.

Além disso, foram realizadas as seguintes inclusões, para alinhamento com as medidas 31.3, 31.4 e 31.6 do Controle 31 do Guia do *Framework* de Privacidade e Segurança da informação, citadas a seguir:

- no capítulo I:
    - inclusão do inciso III no art. 7º;
    - inclusão do art. 8º e consequente renumeração dos artigos posteriores.
- no capítulo III:
    - inclusão do art. 18.
- no capítulo IV:
    - inserção de um novo Capítulo IV para atender ao acesso físico e consequente renumeração dos capítulos e artigos seguintes.
- no capítulo VII:
    - inclusão do inciso X do art. 31.

Mudanças da Versão 2.0

Primeiramente, ressalta-se que as mudanças inseridas nesta versão em comparação com a anterior visam à adequação com o Guia do *Framework* de Privacidade e Segurança da Informação v1, elaborado e publicado pela SGD em novembro de 2022.

Foram realizadas inclusões de: seção sobre aviso preliminar e agradecimentos; e referência de quais controles e medidas do *Framework* de Privacidade e Segurança da Informação são atendidos pelo Modelo de Política de Controle de Acesso.

Além disso, foram realizadas as seguintes inclusões para alinhamento com as medidas do Guia do *Framework* de Privacidade e Segurança da informação:

no capítulo II:

- no art. 2º, inclusão dos incisos IV e V.
- inclusão do art. 3º.
- inclusão do art. 4º.
- inclusão do art. 5º.
- inclusão do art. 6º.
- inclusão do art. 7º.

no capítulo II, foram realizadas as seguintes inclusões:

- atualização da alínea “a” do art. 11.

no capítulo III:

- inclusão do art. 17.
- inclusão do art. 18.

no capítulo IV:

- atualização do art. 19.

no capítulo VI:

- inclusão do inciso VIII do art. 21.
- inclusão do inciso IX do art. 21.