Modelo de Política de Gestão de Identidades e Controle de Acesso

MINISTÉRIO DA
GESTÃO E DA
INOVAÇÃO EM
SERVIÇOS PÚBLICOS

Programa de Privacidade e Segurança da Informação

PPSI 2.0

Versão 1.0

Brasília, 24 de agosto de 2026

MODELO DE POLÍTICA DE GESTÃO DE IDENTIDADES E CONTROLE DE ACESSO

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
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
Natalício Fernandes Pereira
Thainan Cardoso Rezende

EQUIPE DE REVISÃO
Anderson Souza de Araújo

Histórico de versões

Data	Versão	Descrição	Autor
24/08/2026	1.0	Elaboração do Modelo.	Equipe Técnica de Elaboração

Licença *Creative Commons*

[1] Disponível em: https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.

Medidas do *framework* do PPSI 2.0 apoiadas por este documento

Id	Medida
5.1	O órgão estabelece e mantém um inventário de contas?
5.2	O órgão promove ações para evitar a reutilização de senhas?
5.3	O órgão desabilita ou exclui contas inativas?
5.4	O órgão limita os privilégios de administrador às contas de administrador dedicadas?
5.5	O órgão estabelece e mantém um inventário de contas de serviço?
5.6	O órgão centraliza a gestão de contas?
6.1	O órgão estabelece um processo de concessão de acesso?
6.2	O órgão estabelece um processo de revogação de acesso?
6.3	O órgão exige autenticação multifator (*Multi-Factor Authentication* - MFA) para soluções de software expostas externamente?
6.4	O órgão exige MFA para acesso remoto à rede?
6.5	O órgão exige autenticação MFA para acesso administrativo?
6.6	O órgão estabelece e mantém um inventário de sistemas de autenticação e autorização?
6.7	O órgão centraliza o controle de acesso?
6.8	O órgão define e mantém o controle de acesso baseado em funções?
12.3	O órgão centraliza a autenticação, a autorização e a auditoria (*Authentication, Authorization, and Accounting* - AAA) de rede?
12.7	O órgão assegura que os dispositivos remotos utilizem uma Rede Privada Virtual (*Virtual Private Network* - VPN) e se conectam em uma infraestrutura de AAA?
14.3	O órgão conscientiza os agentes públicos nas melhores práticas de autenticação?
25.7	O órgão implementa medidas técnicas e administrativas aptas a proteger os dados pessoais?

Orientações

Esta seção consigna informações básicas para a elaboração da Política de Gestão de Identidades e Controle de Acesso.

Este modelo, assim como todos os modelos disponibilizados pela Secretaria de Governo Digital (SGD) no âmbito do Programa de Privacidade e Segurança da Informação (PPSI) instituído pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, deve ser utilizado como uma referência pelos órgãos e entidades, devendo ser realizada uma análise e adaptação, **inclusão e exclusão de diretrizes,** para considerar as particularidades específicas dos seus ambientes a fim de construir diretrizes que sejam adequadas à sua realidade e às boas práticas.

As informações [destacadas em amarelo] neste modelo devem ser substituídas conforme o caso concreto. As informações explicitadas em vermelho devem ser removidas.

Modelo de Política de Gestão de Identidades e Controle de Acesso

[ATO NORMATIVO nº XX, DE XX DE XXXXXXXXX DE 20XX]

Dispõe sobre a Política de Gestão de Identidades e Controle de Acesso do [órgão ou entidade].

O [representante do órgão ou entidade], no uso da atribuição que lhe confere o [dispositivo legal], e tendo em vista o disposto na Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), no Decreto nº 11.856, de 26 de dezembro de 2023, e no Decreto nº 12.572, de 4 de agosto de 2025, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Gestão de Identidades e Controle de Acesso no âmbito do [órgão ou entidade].

Art. 2º Esta Política tem por objeto estabelecer as diretrizes estratégicas para a gestão de identidades e o controle de acesso lógico e físico aos ativos de informação, sistemas, aplicações e instalações da organização.

Art. 3º Esta Política aplica-se, no âmbito do [órgão ou entidade], a todos os agentes públicos, prestadores de serviços, colaboradores e visitantes.

Parágrafo único**.** O disposto no *caput* estende-se aos ativos de informação, às informações custodiadas e às instalações físicas da instituição.

Art. 4º A gestão de identidades e o controle de acesso aos ativos de informação do [órgão ou entidade] fundamentam-se nos seguintes princípios:

I - privilégio mínimo;

II - segregação de funções;

III - necessidade de conhecer;

IV - rastreabilidade;

V - responsabilidade;

VI - proteção de dados pessoais;

VII - gestão baseada em riscos.

[Inserir outros itens que julgar necessário]

Art. 5º Para além dos princípios dispostos no art. 4º, a gestão de identidades e o controle de acesso do [órgão ou entidade] devem considerar a criticidade dos ativos de informação, os processos institucionais e os impactos decorrentes de acessos inadequados.

Art. 6º Os processos relacionados à gestão de identidades e ao controle de acesso devem integrar-se à governança de segurança da informação, com a definição clara de responsabilidades, mecanismos de supervisão e processos de tomada de decisão compatíveis com os objetivos institucionais.

[Inserir outros itens que julgar necessário]

CAPÍTULO II

DA GESTÃO DE IDENTIDADES E CONTAS

Art. 7º O gerenciamento de identidades deve abranger diferentes classes de usuários, incluindo agentes públicos, estagiários, prestadores de serviços, terceiros, contas de serviço, contas de aplicação e credenciais utilizadas por *Application Programming Interface* (API), aplicando-se regras estritas de expiração e revogação imediata de privilégios para pessoal externo após o encerramento do vínculo contratual.

Art. 8º A [unidade responsável pela gestão de identidades e acessos] deve assegurar a gestão do ciclo de vida das identidades institucionais, promovendo sua identificação inequívoca, unicidade, rastreabilidade e vinculação às respectivas contas de acesso durante todo o seu período de utilização.

Art. 9º A [unidade responsável pela gestão de identidades e acessos] deve manter inventário atualizado das contas de acesso gerenciadas e coordenar a revisão periódica de sua adequação, nos termos das normas complementares a esta Política.

[Inserir outros itens que julgar necessário]

CAPÍTULO III

DOS CONTROLES DE ACESSO

Art. 10. Os controles de acesso lógico devem restringir o acesso a sistemas, aplicações, bancos de dados, código-fonte e demais ativos de informação, observados os princípios estabelecidos no art. 4º.

Parágrafo único. A concessão de acessos lógicos que envolvam ativos de informação críticos ou dados pessoais sensíveis fica condicionada à assinatura prévia, pelo usuário, de Termo de Ciência e Responsabilidade (TCR), contendo obrigações de conduta, sigilo e restrições de uso.

Art. 11. Os controles de acesso físico devem proteger as instalações e os ativos contra acessos não autorizados, danos e interferências, definindo perímetros de segurança e controlando o acesso a áreas restritas.

Art. 12. Os mecanismos de autenticação adotados devem ser compatíveis com o grau de criticidade e com o risco associado aos ativos de informação, aplicando-se critérios de robustez técnica para a garantia da identidade do usuário.

Art. 13. Os privilégios administrativos atribuídos a contas dedicadas devem ser restritos, observando o princípio do privilégio mínimo. As contas de serviço, quando utilizadas para a execução de processos, aplicações ou serviços automatizados, também devem estar sujeitas a controles compatíveis e ao estrito atendimento de suas finalidades.

Art. 14. Os controles de acesso às redes institucionais e aos acessos remotos devem ser compatíveis com os riscos à privacidade e à segurança da informação identificados.

[Inserir outros itens que julgar necessário]

CAPÍTULO IV

DA PROTEÇÃO DE DADOS PESSOAIS

Art. 15. O acesso aos dados pessoais será concedido em estrita observância aos princípios estabelecidos no art. 6º da LGPD, em especial aos princípios da finalidade, necessidade, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Art. 16. O tratamento de dados pessoais sensíveis deve ser realizado com a adoção de medidas de segurança específicas para assegurar sua integridade, confidencialidade e proteção contra acessos não autorizados.

[Inserir outros itens que julgar necessário]

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 17. Compete a [unidade responsável pela gestão de identidades e acessos] a implementação e manter dos controles e medidas previstas nesta Política, gerir o ciclo de vida das contas de acesso e a manter dos registros de acesso.

Art. 18. Compete ao superior imediato do usuário de informação solicitar formalmente a criação, alteração ou cancelamento de contas de acesso de seus subordinados e comunicar tempestivamente à unidade responsável qualquer movimentação interna ou desligamento do usuário.

Art. 19. Compete aos usuários utilizar suas credenciais de forma responsável e conforme as diretrizes constantes desta Política, manter sigilo sobre elas, comunicar qualquer suspeita de comprometimento à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) e responder por todas as ações realizadas com suas credenciais.

Art. 20. Compete à [unidade de tecnologia da informação] implementar e manter as medidas técnicas de controle de acesso e monitorar a utilização da rede e dos sistemas do [órgão ou entidade].

Art. 21. Compete à ETIR investigar incidentes relacionados a acessos não autorizados e ao descumprimento desta Política.

Art. 22. Compete à [unidade de tecnologia da informação], em conjunto com as instâncias de segurança da informação, assegurar a rastreabilidade e a auditabilidade dos acessos lógicos realizados nos sistemas institucionais, nos termos das normas complementares a esta Política.

[Inserir outros itens que julgar necessário]

CAPÍTULO VI

DA REVISÃO PERIÓDICA E DA AUDITORIA

Art. 23. Os direitos de acesso concedidos devem ser revisados periodicamente, ou sempre que houver mudança de função, movimentação interna ou desligamento de usuários e colaboradores, a fim de validar a adequação dos privilégios.

Art. 24. A [unidade de tecnologia da informação] deve assegurar a geração e a proteção de registros de auditoria e de acesso a sistemas, aplicações e instalações físicas, garantindo sua integridade e disponibilidade e protegendo-os contra alterações não autorizadas.

Art. 25. Os critérios de retenção e de revisão dos registros de auditoria para fins de identificação de comportamentos anômalos serão disciplinados em ato normativo complementar a esta Política.

[Inserir outros itens que julgar necessário]

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 26. O Gestor de Segurança da Informação e o Encarregado pelo Tratamento de Dados Pessoais do [órgão ou entidade], cada qual no âmbito de suas competências, devem promover a conscientização e a capacitação dos agentes públicos, usuários e colaboradores sobre as disposições desta Política e das normas e procedimentos a ela correlatos.

Art. 27. Incidentes de segurança relacionados a acessos não autorizados devem ser comunicados imediatamente à ETIR para investigação e tratamento.

Art. 28. O descumprimento das disposições desta Política sujeitará o agente público às sanções administrativas previstas na Lei nº 8.112, de 11 de dezembro de 1990, e demais normas disciplinares aplicáveis, sem prejuízo das responsabilidades civis e penais cabíveis.

Art. 29. Quaisquer exceções, temporárias ou definitivas, às regras estabelecidas nesta Política devem ser formalmente justificadas pela unidade demandante, submetidas à análise de risco da [unidade de segurança da informação] e aprovadas pela autoridade competente, observado o âmbito da matéria envolvida.

§ 1º As exceções relacionadas à segurança da informação devem ser aprovadas pelo Gestor de Segurança da Informação, enquanto aquelas que envolvam tratamento de dados pessoais devem contar com a manifestação do Encarregado pelo Tratamento de Dados Pessoais, sem prejuízo da definição das competências decisórias em normativo específico.

§ 2º Devem ser adotados controles e medidas de privacidade e segurança da informação compensatórias e compatíveis com os riscos identificados.

Art. 30. Os casos omissos serão resolvidos pelo [Comitê de Segurança da Informação ou instância ou equivalente] ou pelo [Comitê de Proteção de Dados Pessoais ou instância equivalente] para questões relacionadas a dados pessoais.

Art. 31. Esta Política será revisada, no mínimo, a cada dois anos, ou sempre que houver alterações significativas no contexto institucional, regulatório, tecnológico ou estratégico que justifiquem sua atualização.

[Inserir outros itens que julgar necessário]

gov.br

Dúvida?

Entre em contato conosco

Sítio do PPSI:
PPSI 2.0 — Governo Digital