



Modelo de Norma 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, 1 de outubro de 2026



MODELO DE NORMA 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

Anderson Souza de Araújo

Natalício Fernandes Pereira

Thainan Cardoso Rezende

EQUIPE DE REVISÃO

Marta Juvina de Medeiros



Histórico de versões

Data	Versão	Descrição	Autor
01/10/2026	1.0	Elaboração da primeira versão do modelo.	Equipe Técnica de Elaboração



Licença *Creative Commons*

Esta obra está licenciada sob a Licença *Creative Commons* Atribuição-NãoComercial-SemDerivações 4.0 Internacional¹.

Você está autorizado a copiar e redistribuir o conteúdo deste modelo para uso interno e externo à sua organização, somente para fins não comerciais, desde que (i) o devido crédito seja dado à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), e (ii) um *link* para a licença seja fornecido. Além disso, não é permitida a distribuição de obras derivadas, remixadas, transformadas ou desenvolvidas a partir deste modelo.

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 (<i>Multi-Factor Authentication</i> - 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?
6.7	O órgão centraliza o controle de acesso?
6.8	O órgão define e mantém o controle de acesso baseado em funções?
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 Norma de Gestão de Identidades e Controle de Acesso do órgão ou entidade.

Este modelo, assim como todos os modelos disponibilizados pela Diretoria de Privacidade e Segurança da Informação (DEPSI) 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, que deverão analisá-lo e adaptá-lo – **inclusão e exclusão de diretrizes** – para considerar as particularidades 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 e as **destacadas em vermelho** devem ser removidas.



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

Dispõe sobre a Norma de Gestão de Identidades e Controle de Acesso no âmbito 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 Norma de Gestão de Identidades e Controle de Acesso do [órgão ou entidade], em complemento à Política de Segurança da Informação e à Política de Gestão de Identidades e Controle de Acesso.

Art. 2º Esta Norma estabelece as regras, as responsabilidades e os requisitos para a gestão do ciclo de vida das identidades digitais e das credenciais de autenticação, bem como para a concessão, manutenção, revisão e revogação de acessos aos ativos da instituição, abrangendo os domínios de controle de acesso lógico e de controle de acesso físico.

§ 1º Os controles de acesso lógico e físico possuem finalidades e mecanismos próprios e devem observar, quando aplicável, as disposições desta Norma e dos demais normativos institucionais correlatos.

§ 2º As disposições desta Norma relativas ao controle de acesso físico restringem-se à gestão das autorizações de acesso, sem prejuízo da observância das normas específicas que disciplinem a segurança física, patrimonial, ambiental e demais controles correlatos.

[Inserir outros itens que julgar necessários].

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Aplicam-se a esta Norma os termos e as definições constantes da LGPD e da Portaria GSI/PR nº 93, de 18 de outubro de 2021, sem prejuízo das seguintes definições:

I - atividade administrativa: ação executada com privilégios elevados para instalar, configurar, parametrizar, gerenciar, monitorar ou alterar sistemas, serviços, aplicações, dispositivos, contas, credenciais, permissões ou outros recursos tecnológicos;

II - atividade de uso rotineiro: ação executada no exercício regular das atribuições do usuário que não exija privilégios elevados;

III - conta: representação lógica de uma identidade digital em um sistema de informação ou serviço de tecnologia da informação, utilizada para fins de autenticação, autorização e responsabilização;

IV - conta individual: conta associada a uma única identidade digital de pessoa natural, destinada ao uso exclusivo de seu titular e utilizada para fins de autenticação, autorização, rastreabilidade e responsabilização das ações realizadas;

V - conta privilegiada: conta que possui permissões elevadas capazes de alterar configurações, administrar recursos ou acessar ativos de informação sensíveis ou críticos;

VI - credencial de autenticação: informação, dispositivo ou mecanismo utilizado para comprovar a identidade declarada durante o processo de autenticação;

VII - gestão de acessos: conjunto de processos destinados à concessão, atualização, revisão, manutenção e revogação de direitos de acesso;

VIII - identidade digital: conjunto de atributos que permite distinguir uma pessoa natural, pessoa jurídica ou entidade não humana em determinado contexto digital;

IX - identidade não humana: identidade digital associada a aplicações, serviços, dispositivos, processos automatizados, Interfaces de Programação de Aplicações (*Application Programming Interfaces* – APIs) ou outros componentes tecnológicos que necessitem autenticar-se perante recursos computacionais; e

X - identificador da conta: informação única associada a uma conta, utilizada para distingui-la das demais contas;

[Inserir outros itens que julgar necessários].

CAPÍTULO III

DO ESCOPO

Art. 4º Esta Norma aplica-se a toda pessoa natural ou entidade não humana que possua, solicite ou administre acesso a ativos de informação ou recursos de tecnologia da informação do [órgão ou entidade], abrangendo:

I - agentes públicos, independentemente da natureza do vínculo, do cargo, da função ou da forma de investidura;

II - estagiários, residentes, bolsistas e colaboradores eventuais;

III - trabalhadores de empresas contratadas, prestadores de serviços, consultores e demais colaboradores externos que possuam acesso a ativos de informação ou recursos de tecnologia da informação do [órgão ou entidade]; e

IV - identidades não humanas, inclusive contas de serviço, aplicações, APIs, integrações sistêmicas, dispositivos e demais componentes tecnológicos administrados pelo [órgão ou entidade].

[Inserir outros itens que julgar necessários].

Parágrafo único. Esta Norma aplica-se aos ativos de informação e aos recursos de tecnologia da informação administrados pelo [órgão ou entidade], independentemente da localização da infraestrutura subjacente ou do modelo de prestação do serviço, incluindo ambientes próprios, serviços em nuvem e soluções fornecidas por terceiros.

[Inserir outros itens que julgar necessários].

CAPÍTULO IV

DA GESTÃO DO CICLO DE VIDA DAS IDENTIDADES

Seção I

Da Criação das Identidades Digitais

Art. 5º A criação de identidade digital somente será permitida quando necessária ao desempenho de atribuições institucionais ou à prestação de serviços autorizados pelo [órgão ou entidade].

Parágrafo único. A solicitação para criação de identidade digital deverá identificar, no mínimo:

- I - a pessoa natural ou a entidade não humana à qual a identidade será vinculada;
- II - a justificativa para sua criação;
- III - a unidade organizacional responsável;
- IV - o responsável pela solicitação; e
- V - o período de utilização, quando aplicável.

[Inserir outros itens que julgar necessários].

Art. 6º Cada identidade digital deverá estar associada a uma única pessoa natural ou a uma única entidade não humana, sendo vedado o compartilhamento de identidades digitais.

Parágrafo único. É vedada a alteração da vinculação da identidade digital sem o registro formal da mudança e a correspondente atualização dos controles de acesso.

[Inserir outros itens que julgar necessários].

Seção II

Da Manutenção das Identidades Digitais

Art. 7º As informações associadas às identidades digitais deverão ser mantidas atualizadas durante todo o seu ciclo de vida, observadas as alterações cadastrais, funcionais ou operacionais que impactem sua utilização.

Art. 8º A alteração das informações associadas à identidade digital deverá preservar os registros históricos e as evidências necessárias à rastreabilidade das ações realizadas durante todo o seu ciclo de vida.

[Inserir outros itens que julgar necessários].

Seção III

Da Suspensão das Identidades Digitais

Art. 9º A identidade digital deverá ser suspensa nas seguintes situações:

I - sempre que ocorrer afastamento, interrupção ou indisponibilidade temporária da relação que justificou sua criação;

II - ocorrência de situação que inviabilize temporariamente sua utilização; ou

III - necessidade de mitigação imediata de riscos à segurança da informação.

[Inserir outros itens que julgar necessários].

§ 1º A suspensão não implica a exclusão da identidade digital.

§ 2º Enquanto perdurar a suspensão, deverão permanecer preservadas as informações necessárias à retomada das atividades e à realização de auditorias.

Seção IV

Do Encerramento das Identidades Digitais

Art. 10. A identidade digital deverá ser encerrada:

I - quando cessarem as condições que justificaram sua criação; ou

II - quando deixar de existir a necessidade de sua manutenção.

[Inserir outros itens que julgar necessários].

§ 1º O encerramento da identidade digital deverá ocorrer tão logo seja constatada a cessação das condições que justificaram sua criação ou manutenção.

§ 2º O encerramento da identidade digital deverá implicar a revogação dos acessos a ela vinculados, sem prejuízo da preservação dos registros necessários ao atendimento de requisitos legais, regulatórios, administrativos e de auditoria.

Art. 11. O encerramento da identidade digital deverá ser formalmente registrado, de forma a preservar a rastreabilidade das ações realizadas durante seu ciclo de vida.

Art. 12. As identidades digitais encerradas não poderão ser reassociadas a outra pessoa natural ou a outra entidade não humana.

[Inserir outros itens que julgar necessários].

CAPÍTULO V

DA GESTÃO DE CONTAS

Seção I

Disposições Gerais

Art. 13. As contas deverão ser classificadas, no mínimo:

I – quanto à sua natureza, em:

a) conta individual; ou

b) conta de serviço; e

II – quanto ao nível de acesso, em:

- a) conta privilegiada; ou
- b) conta não privilegiada.

Parágrafo único. Considera-se privilegiada a conta individual ou de serviço que possua permissões elevadas para administrar recursos, alterar configurações ou acessar ativos de informação críticos.

[Inserir outros itens que julgar necessários].

Art. 14. A [unidade responsável pela gestão de identidades e controle de acesso] deverá manter inventário atualizado das contas administradas pelo [órgão ou entidade], contemplando, no mínimo:

- I - o identificador da conta;
- II - sua classificação;
- III - a identidade digital ou entidade à qual esteja vinculada;
- IV - o responsável pela conta;
- V - sua finalidade;
- VI - sua situação;
- VII - as datas de criação e, quando aplicável, de suspensão, reativação ou encerramento; e
- VIII - outras informações necessárias à sua gestão e rastreabilidade.

§ 1º As contas privilegiadas e as contas de serviço deverão ser identificadas de forma específica no inventário.

§ 2º O inventário deverá ser atualizado sempre que ocorrer criação, alteração, suspensão, reativação ou encerramento de conta e submetido a revisões periódicas.

§ 3º As inconsistências identificadas no inventário deverão ser apuradas e tratadas, especialmente quando envolverem contas inativas, órfãs, duplicadas, compartilhadas, sem responsável identificado ou incompatíveis com sua finalidade.

[Inserir outros itens que julgar necessários].

Seção II

Da Criação de Contas

Art. 15. A criação de conta dependerá de solicitação formal aprovada pela [autoridade competente] e deverá observar os perfis de acesso estritamente necessários ao desempenho das atribuições da identidade digital correspondente, em conformidade com o princípio do privilégio mínimo.

Art. 16. Toda conta deverá estar vinculada a uma identidade digital previamente criada e válida.

Art. 17. Toda conta deverá possuir pessoa natural ou unidade organizacional formalmente responsável por sua utilização e gestão.

[Inserir outros itens que julgar necessários].

Seção III

Das Contas Individuais

Art. 18. As contas individuais destinam-se ao uso exclusivo da identidade digital à qual estejam vinculadas, sendo vedado seu compartilhamento ou utilização por terceiros.

Parágrafo único. O titular da identidade digital vinculada à conta individual é responsável por sua utilização adequada e pela proteção das respectivas credenciais de autenticação.

[Inserir outros itens que julgar necessários].

Seção IV

Das Contas Privilegiadas

Art. 19. As contas privilegiadas destinam-se exclusivamente à execução de atividades administrativas, de gerenciamento, de manutenção ou de operação que exijam privilégios elevados sobre ativos de informação ou recursos de tecnologia da informação.

Parágrafo único. A concessão de privilégios elevados deverá ser limitada às atividades estritamente necessárias ao desempenho das atribuições institucionais.

Art. 20. A criação, atualização, suspensão e encerramento de contas privilegiadas dependerão de autorização formal da autoridade competente, observadas as competências estabelecidas nesta Norma.

Parágrafo único. A autorização deverá indicar a finalidade da conta, o nível de privilégio concedido e sua necessidade institucional.

Art. 21. O uso de contas privilegiadas restringe-se à execução das atividades administrativas que justifiquem sua concessão.

Parágrafo único. As ações realizadas por meio de contas privilegiadas deverão ser passíveis de rastreabilidade e estar sujeitas a mecanismos de registro e monitoramento compatíveis com os riscos envolvidos.

Art. 22. As atividades que demandem privilégios administrativos deverão ser segregadas das atividades de uso rotineiro, mediante a utilização de contas distintas ou mecanismos equivalentes, sempre que tecnicamente viável e compatível com a gestão dos riscos.

Parágrafo único. Quando a segregação prevista no *caput* não puder ser implementada, deverão ser adotados controles compensatórios formalmente definidos, de forma a mitigar adequadamente os riscos identificados.

Art. 23. É vedado o compartilhamento de contas privilegiadas, salvo nas hipóteses expressamente autorizadas em norma específica e mediante a adoção de controles que assegurem a responsabilização individual.

[Inserir outros itens que julgar necessários].

Seção V

Das Contas de Serviço

Art. 24. As contas de serviço destinam-se exclusivamente à execução automatizada de aplicações, serviços, processos, integrações sistêmicas ou outros componentes tecnológicos.

Parágrafo único. É vedada a utilização de contas de serviço para autenticação interativa por usuários, salvo nas hipóteses formalmente autorizadas, tecnicamente justificadas e aprovadas pela [autoridade competente].

Art. 25. As contas de serviço deverão permanecer vinculadas à finalidade que justificou sua criação, sendo vedada sua utilização para finalidades distintas daquelas formalmente aprovadas.

[inserir outros itens que julgar necessários].

Seção VI

Da Supervisão das Contas

Art. 26. A [unidade responsável pela supervisão das contas] deverá manter mecanismos destinados ao monitoramento da utilização das contas, de forma a identificar contas cujo uso, inatividade ou padrão de utilização seja incompatível com sua classificação ou finalidade.

Art. 27. As contas que permanecerem sem utilização por período superior ao definido pela [unidade de gestão de identidades e controle de acesso] deverão ser submetidas à avaliação quanto à necessidade de sua manutenção, observadas sua classificação e finalidade.

§ 1º A avaliação deverá considerar, entre outros aspectos:

I - a finalidade da conta;

II - sua natureza;

III - a existência de processos automatizados associados;

IV - sua utilização prevista em planos de continuidade de negócios, contingência ou recuperação de desastres; e

V - outras justificativas formalmente registradas.

[Inserir outros itens que julgar necessários].

§ 2º Verificada a inexistência de justificativa para manutenção da conta, esta deverá ser suspensa ou encerrada.

Art. 28. As contas submetidas à avaliação deverão possuir registro formal da decisão quanto à sua manutenção, suspensão ou encerramento.

[Inserir outros itens que julgar necessários].

CAPÍTULO VI

DA GESTÃO DAS CREDENCIAIS DE AUTENTICAÇÃO

Seção I

Das Disposições Gerais

Art. 29. Toda conta deverá possuir mecanismo de autenticação compatível com os riscos associados ao ativo de informação ou ao recurso de tecnologia da informação ao qual esteja vinculada.

Parágrafo único. A definição dos mecanismos de autenticação deverá considerar critérios de proporcionalidade, criticidade da informação, sensibilidade dos dados tratados e riscos associados ao acesso.

Art. 30. As credenciais de autenticação associadas a pessoas naturais deverão ser individuais, intransferíveis e mantidas sob responsabilidade exclusiva do titular da conta.

Art. 31. As credenciais associadas a identidades não humanas deverão possuir responsável formalmente designado, ser armazenadas de forma protegida e ser utilizadas exclusivamente para as finalidades que justificaram sua concessão.

Art. 32. É vedado o compartilhamento, a divulgação ou o fornecimento de credenciais de autenticação a terceiros, ainda que temporariamente.

Art. 33. O comprometimento, perda, divulgação indevida ou suspeita de comprometimento de credenciais de autenticação deverá ser comunicado imediatamente à [unidade competente].

Art. 34. As credenciais de autenticação deverão ser revogadas, substituídas ou atualizadas sempre que houver indício de comprometimento ou alteração dos requisitos que justificaram sua concessão.

[Inserir outros itens que julgar necessários].

Seção II

Das Credenciais Baseadas em Senha

Art. 35. Quando a autenticação utilizar senha como credencial, sua definição, atualização e utilização deverão observar os seguintes requisitos mínimos, sem prejuízo das disposições constantes dos procedimentos específicos editados pela [unidade responsável pela gestão de identidades e controle de acesso]:

I - possuir comprimento mínimo compatível com os riscos associados à conta e aos mecanismos de autenticação empregados, conforme definido em procedimento específico;

II - permitir a utilização de frases-senha e outras formas de combinação que favoreçam a criação de credenciais robustas e de fácil memorização pelo usuário;

III - impedir, sempre que tecnicamente viável, a utilização de senhas reconhecidamente fracas, previsíveis, amplamente utilizadas ou comprometidas em incidentes de segurança conhecidos;

IV - ser distinta do identificador da conta (login), quando suportado pelo mecanismo de autenticação adotado;

V - quando suportado pela solução de gestão de identidades ou pelo mecanismo de autenticação adotado pelo [órgão ou entidade], impedir a reutilização de quantidade mínima de senhas anteriormente utilizadas, conforme definido em procedimento específico; e

VI - observar critérios compatíveis com os riscos associados à conta, sua classificação e os mecanismos de autenticação empregados.

[Inserir outros itens que julgar necessários].

Art. 36. A gestão de credenciais deverá contemplar mecanismos destinados à identificação de credenciais comprometidas, reutilizadas indevidamente ou reconhecidamente expostas em incidentes de segurança.

§ 1º Sempre que tecnicamente viável, a verificação prevista no caput deverá ocorrer durante os processos de criação, atualização ou redefinição da credencial.

§ 2º Identificada situação de comprometimento, a credencial deverá ser substituída, revogada ou submetida a outras medidas de mitigação compatíveis com os riscos identificados.

Art. 37. Quando da criação de conta baseada em senha destinada à autenticação interativa por pessoa natural, deverá ser atribuída credencial temporária ao seu titular.

§ 1º A credencial temporária deverá ser gerada de forma aleatória, possuir prazo de utilização limitado e ser transmitida por meio que preserve sua confidencialidade.

§ 2º A credencial temporária deverá ser atualizada no primeiro acesso realizado pelo usuário.

§ 3º O disposto neste artigo não se aplica às contas de serviço, às identidades não humanas, tampouco aos mecanismos de autenticação que dispensem senha.

Art. 38. As senhas de autenticação deverão ser atualizadas:

I - por iniciativa do titular da conta, observado o disposto nesta Norma;

II - sempre que houver indícios ou confirmação de comprometimento da credencial;

III - quando da redefinição da senha pela [unidade responsável pela gestão de identidades e controle de acesso]; ou

IV - nas demais hipóteses previstas nesta Norma.

[Inserir outros itens que julgar necessários].

§ 1º Poderá ser estabelecido prazo máximo de validade para as senhas de autenticação, considerando, entre outros fatores, a análise de riscos, a criticidade dos ativos de informação, os mecanismos de autenticação empregados, os requisitos regulatórios aplicáveis e as capacidades da solução de gestão de identidades adotada.

§ 2º Quando adotado prazo máximo de validade, o usuário deverá ser comunicado previamente acerca da necessidade de atualização da senha.

§ 3º Expirado o prazo de validade sem que a senha tenha sido atualizada, a credencial poderá ter seu uso restringido ou bloqueado temporariamente até a conclusão do procedimento de redefinição da senha.

§ 4º A inexistência de prazo máximo de validade para senhas não dispensa a obrigatoriedade de sua atualização nas hipóteses previstas nos incisos II, III e IV deste artigo.

[Inserir outros itens que julgar necessários].

Seção III

Das Credenciais Não Baseadas em Senha

Art. 39. Os mecanismos de autenticação não baseados em senha deverão observar critérios de segurança, interoperabilidade, disponibilidade e proporcionalidade aos riscos envolvidos.

[Inserir outros itens que julgar necessários].

CAPÍTULO VII DA AUTENTICAÇÃO

Seção I Dos Princípios Gerais

Art. 40. A autenticação deverá assegurar nível de confiança compatível com a criticidade do ativo de informação ou do recurso de tecnologia da informação, considerados os riscos associados ao acesso.

Art. 41. Os processos de autenticação deverão preservar a vinculação entre a identidade digital e a entidade autenticada, de modo a assegurar a rastreabilidade e a responsabilização das ações realizadas.

[Inserir outros itens que julgar necessários].

Seção II Da Autenticação Multifator

Art. 42. A autenticação multifator deverá ser adotada sempre que a criticidade do ativo de informação, a classificação da informação ou os riscos associados ao acesso exigirem nível adicional de confiança na autenticação.

§ 1º A obrigatoriedade de autenticação multifator deverá considerar, no mínimo:

- I - o nível de privilégio da conta;
- II - a sensibilidade das informações acessadas;
- III - a exposição do serviço a redes externas; e
- IV - os riscos associados ao acesso.

[Inserir outros itens que julgar necessários].

§ 2º A autenticação multifator deverá ser obrigatoriamente adotada para:

- I - o acesso a soluções expostas a redes externas;
- II - o acesso remoto à infraestrutura tecnológica da organização; e
- III - o acesso administrativo ou por meio de contas privilegiadas.

[Inserir outros itens que julgar necessários].

§ 3º A utilização de autenticação multifator não dispensa a observância dos requisitos aplicáveis à gestão de contas, credenciais de autenticação e controle de acesso previstos nesta Norma.

Art. 43. Quando a autenticação multifator não puder ser implementada em situações nas quais sua adoção seja exigida, deverão ser adotados controles compensatórios compatíveis com os riscos identificados.

[Inserir outros itens que julgar necessários].

CAPÍTULO VIII

DA GESTÃO DE ACESSOS

Seção I

Da Concessão

Art. 44. A concessão de direitos de acesso deverá observar os princípios da necessidade de conhecer, do privilégio mínimo, da segregação de funções, da proporcionalidade e da rastreabilidade.

Art. 45. Os direitos de acesso deverão ser concedidos exclusivamente na medida necessária ao desempenho das atribuições institucionais da identidade digital à qual estiverem vinculados.

Parágrafo único. É vedada a concessão de direitos de acesso por conveniência administrativa, vínculo hierárquico ou qualquer outro fundamento dissociado da necessidade institucional.

Art. 46. A concessão, atualização, suspensão e revogação de direitos de acesso dependerão de autorização formal da [autoridade competente], observadas as competências estabelecidas nesta Norma.

Parágrafo único. A concessão de direitos de acesso deverá ser precedida da definição do perfil de acesso adequado por parte da [autoridade competente].

[Inserir outros itens que julgar necessários].

Seção II

Da Segregação de Funções

Art. 47. É vedada a concessão de direitos de acesso que possam resultar em conflitos de interesse ou comprometer a adequada segregação de funções, salvo mediante justificativa formal e adoção de controles compensatórios.

Art. 48. Sempre que tecnicamente viável, deverão ser adotados mecanismos destinados à prevenção, detecção ou sinalização de conflitos de segregação de funções nos sistemas de informação.

[Inserir outros itens que julgar necessários].

Seção III

Da Revisão dos Direitos de Acesso

Art. 49. Os direitos de acesso deverão ser revisados periodicamente para verificar se permanecem compatíveis com as atribuições desempenhadas pela pessoa natural vinculada à identidade digital ou com a finalidade para a qual a identidade não humana foi criada.

§ 1º A periodicidade das revisões deverá ser formalmente estabelecida pela [unidade responsável pela gestão de identidades e controle de acesso], observados os riscos associados, a criticidade dos ativos e as categorias de acesso existentes.

§ 2º As revisões deverão contemplar, no mínimo, as contas privilegiadas e os direitos de acesso a informações classificadas, a dados pessoais, a ativos considerados críticos ou a recursos acessíveis por meio de redes externas.

§ 3º Para as contas privilegiadas, as revisões deverão considerar, entre outros aspectos:

I - as atribuições atualmente desempenhadas;

II - a necessidade institucional da manutenção dos privilégios; e

III - a observância dos princípios do privilégio mínimo e da segregação de funções.

[Inserir outros itens que julgar necessários].

§ 4º Verificada a inexistência de necessidade para manutenção dos privilégios, estes deverão ser revogados ou adequados em prazo compatível com os riscos identificados.

[Inserir outros itens que julgar necessários].

Seção IV

Dos Perfis de Acesso

Art. 50. Os direitos de acesso deverão ser concedidos por meio de perfis de acesso previamente definidos pela [unidade responsável], ressalvadas as hipóteses devidamente justificadas.

[Inserir outros itens que julgar necessários].

CAPÍTULO IX

DO MONITORAMENTO E DA CONFORMIDADE

Seção I

Das Disposições Gerais

Art. 51. A gestão de identidades e o controle de acesso deverão contemplar mecanismos de monitoramento contínuo destinados a verificar a efetividade dos controles estabelecidos nesta Norma, identificar desvios, apoiar a resposta a incidentes de segurança da informação e subsidiar a melhoria contínua dos processos.

Art. 52. O monitoramento deverá observar os princípios da necessidade, da finalidade e da proporcionalidade, bem como o respeito aos direitos dos titulares, observadas as normas aplicáveis de transparência, proteção de dados pessoais e segurança da informação.

[Inserir outros itens que julgar necessários].

Seção II

Do Registro de Eventos

Art. 53. Os eventos relacionados à criação, manutenção, atualização, suspensão, reativação e encerramento de identidades digitais, bem como à administração de contas, autenticação e gestão de acessos, deverão ser registrados de forma a possibilitar sua rastreabilidade.

Art. 54. Os registros de eventos deverão preservar, sempre que aplicável:

- I - a identificação da identidade digital envolvida;
- II - a data e o horário da ocorrência;
- III - o recurso de tecnologia da informação afetado;
- IV - a ação realizada;
- V - o resultado da operação; e
- VI - outras informações necessárias à rastreabilidade do evento.

[Inserir outros itens que julgar necessários].

Art. 55. Os registros de eventos deverão ser protegidos contra alteração, destruição, acesso não autorizado e perda de integridade durante todo o período de retenção estabelecido pela [unidade responsável pela gestão de identidades e controle de acesso], observados os requisitos legais, regulatórios, contratuais e as necessidades de auditoria, investigação, resposta a incidentes e continuidade das operações.

§ 1º O período de retenção dos registros deverá ser formalmente estabelecido pela [unidade responsável pela gestão de identidades e controle de acesso], considerando, entre outros aspectos:

- I - a criticidade dos ativos;
- II - a classificação das informações;
- III - os requisitos legais, regulatórios e contratuais;
- IV - as necessidades de auditoria;
- V - as atividades de investigação e resposta a incidentes; e
- VI - os requisitos de continuidade das operações.

[Inserir outros itens que julgar necessários].

§ 2º Encerrado o período de retenção, os registros deverão ser eliminados ou anonimizados, quando aplicável, de forma segura e em conformidade com a legislação vigente, inclusive com as normas institucionais de gestão documental e de proteção de dados pessoais.

[Inserir outros itens que julgar necessários].

Seção III

Do Monitoramento dos Acessos

Art. 56. Os eventos relacionados ao controle de acesso lógico deverão ser monitorados, sempre que tecnicamente viável e proporcionalmente aos riscos envolvidos, incluindo:

- I - o uso de contas privilegiadas;
- II - as tentativas de autenticação malsucedidas;
- III - a elevação de privilégios;
- IV - os acessos lógicos a ativos de informação críticos; e
- V - outros eventos considerados relevantes para a segurança da informação.

[Inserir outros itens que julgar necessários].

Parágrafo único. A definição dos eventos sujeitos a monitoramento deverá observar critérios de criticidade, classificação da informação, riscos associados ao acesso e capacidades técnicas dos mecanismos utilizados.

Art. 57. Sempre que identificados indícios de utilização indevida de identidades digitais, contas, credenciais, direitos de acesso ou autorizações de acesso físico, deverão ser adotadas medidas compatíveis com a criticidade da situação, observados os procedimentos institucionais de resposta a incidentes de segurança da informação e, quando aplicável, os procedimentos relacionados à segurança física.

[Inserir outros itens que julgar necessários].

Seção IV

Da Avaliação da Conformidade

Art. 58. A gestão de identidades e os processos de controle de acesso lógico e físico deverão ser submetidos a avaliações periódicas de conformidade em relação às políticas institucionais, aos normativos internos, à legislação aplicável e aos referenciais normativos e técnicos adotados.

Art. 59. As não conformidades identificadas deverão ser registradas, analisadas e tratadas de forma compatível com os riscos envolvidos, observadas as responsabilidades definidas nos normativos institucionais aplicáveis.

[Inserir outros itens que julgar necessários].

CAPÍTULO X

DAS RESPONSABILIDADES

Art. 60. Compete à alta administração do [órgão ou entidade]:

I - assegurar o apoio institucional necessário à implementação da Norma de Gestão de Identidades e Controle de Acesso;

II - assegurar a disponibilização dos recursos necessários à implementação e à manutenção dos controles previstos nesta Norma; e

III - acompanhar os riscos e as não conformidades relevantes relacionadas à gestão de identidades e ao controle de acesso.

[Inserir outros itens que julgar necessários].

Art. 61. Compete ao Comitê de Segurança da Informação ou estrutura equivalente:

I - aprovar esta Norma e suas alterações;

II - acompanhar a implementação desta Norma e a efetividade dos controles nela estabelecidos;

III - acompanhar os riscos e as não conformidades relevantes relacionadas à gestão de identidades e ao controle de acesso; e

IV - deliberar sobre as exceções à Norma submetidas à sua apreciação.

[Inserir outros itens que julgar necessários].

Parágrafo único. Quando a matéria envolver tratamento de dados pessoais, o Comitê de Proteção de Dados Pessoais ou estrutura equivalente deverá ser previamente consultado, observadas suas competências institucionais.

Art. 62. Compete à [unidade responsável pela segurança da informação]:

- I - coordenar a implementação e a revisão desta Norma;
- II - estabelecer requisitos, critérios e orientações para a gestão de identidades, contas, credenciais, autenticação e direitos de acesso;
- III - apoiar a avaliação dos riscos relacionados ao controle de acesso lógico e físico;
- IV - acompanhar a conformidade dos controles disciplinados por esta Norma; e
- V - propor medidas destinadas ao aprimoramento dos controles de gestão de identidades e de controle de acesso.

[Inserir outros itens que julgar necessários].

Art. 63. Compete à [unidade responsável pela gestão de identidades e controle de acesso]:

- I - executar a criação, manutenção, suspensão, reativação e encerramento de identidades digitais e contas, mediante solicitação devidamente autorizada;
- II - manter o inventário de contas e demais registros necessários à gestão do ciclo de vida das identidades;
- III - assegurar a vinculação entre cada identidade digital, suas contas e o respectivo responsável;
- IV - implementar os perfis e os direitos de acesso aprovados pelos gestores competentes;
- V - executar os procedimentos de concessão, atualização, revisão e revogação de acessos previstos nesta Norma; e
- VI - identificar contas inativas, órfãs, duplicadas, compartilhadas ou incompatíveis com sua finalidade.

[Inserir outros itens que julgar necessários].

Art. 64. Compete aos gestores das unidades organizacionais:

- I - definir e manter atualizados os perfis e os requisitos de acesso sob sua responsabilidade;
- II - autorizar, rejeitar, revisar ou solicitar a revogação dos direitos de acesso aos ativos sob sua gestão;
- III - assegurar que os acessos concedidos sejam compatíveis com as atribuições dos usuários e limitados ao mínimo necessário; e
- IV - comunicar tempestivamente as alterações de lotação, atribuições, vínculo, afastamento ou desligamento que exijam adequação dos direitos de acesso.

[Inserir outros itens que julgar necessários].

Art. 65. Compete ao gestor de segurança da informação:

- I - acompanhar a implementação dos controles previstos nesta Norma;
- II - monitorar os riscos relacionados à gestão de identidades e ao controle de acesso;
- III - apoiar a análise e o tratamento de não conformidades relacionadas aos controles disciplinados por esta Norma;

IV - reportar ao Comitê de Segurança da Informação ou estrutura equivalente situações relevantes relacionadas à gestão de identidades e ao controle de acesso;

V - promover a articulação entre as unidades responsáveis pela implementação dos controles previstos nesta Norma; e

VI - promover a conscientização e a capacitação dos agentes públicos, usuários e colaboradores sobre as disposições desta Norma e demais procedimentos a ela correlatos.

[Inserir outros itens que julgar necessários].

Art. 66. Compete ao encarregado pelo tratamento de dados pessoais, sem prejuízo das atribuições previstas na legislação e em normas complementares:

I - orientar os agentes públicos e o controlador quanto às práticas de proteção de dados pessoais aplicáveis à gestão de identidades e ao controle de acesso;

II - prestar orientação no tratamento de incidentes que envolvam acesso não autorizado ou indevido a dados pessoais; e

III - promover a conscientização e a capacitação dos agentes públicos, usuários e colaboradores sobre a proteção de dados pessoais no âmbito desta Norma e dos demais procedimentos correlatos.

[Inserir outros itens que julgar necessários].

Art. 67. Compete à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), ou estrutura equivalente:

I - analisar eventos e indícios de comprometimento de identidades, contas, credenciais ou direitos de acesso;

II - solicitar, em caráter emergencial, a suspensão de identidades, contas, credenciais ou acessos, quando necessária à contenção de incidente;

III - preservar e analisar os registros e as evidências relacionados aos incidentes;

IV - coordenar, no âmbito de suas competências, as ações de contenção, erradicação e recuperação;

V - comunicar as unidades responsáveis e recomendar medidas corretivas; e

VI - registrar as lições aprendidas e apoiar o aprimoramento dos controles.

[Inserir outros itens que julgar necessários].

Art. 68. Compete aos usuários:

I - assinar o Termo de Ciência e Responsabilidade (TCR) e cumprir as obrigações nele estabelecidas, inclusive as relativas à conduta, ao sigilo e às restrições de uso;

II - utilizar identidades, contas, credenciais e direitos de acesso exclusivamente para finalidades institucionais autorizadas;

III - proteger suas credenciais de autenticação e impedir sua utilização por terceiros;

IV - não compartilhar contas, credenciais, dispositivos de autenticação ou meios de acesso físico; e

V - comunicar imediatamente a perda, o comprometimento, o uso indevido ou a suspeita de comprometimento de credenciais e meios de acesso.

[Inserir outros itens que julgar necessários].

Art. 69. Compete à unidade de gestão de pessoas:

I - promover a ciência dos agentes públicos quanto às disposições desta Norma e aos compromissos dela decorrentes;

II - manter evidências da ciência e concordância dos agentes públicos quanto às suas responsabilidades;

III - manter atualizado o repositório de agentes públicos ativos, refletindo adequadamente o quadro funcional da organização; e

IV - comunicar eventos de admissão, movimentação, afastamento e desligamento que exijam ajustes de acesso.

[Inserir outros itens que julgar necessários].

CAPÍTULO XI

DISPOSIÇÕES FINAIS

Art. 70. Esta Norma deverá ser revisada e atualizada a cada [2 (dois)] anos ou sempre que ocorrerem uma das seguintes situações:

I - alteração significativa nos riscos, na legislação, na estrutura organizacional ou nas tecnologias empregadas pelo órgão ou entidade;

II - incidente grave relacionado ao seu objeto;

III - identificação de achado de auditoria relevante; ou

IV - alteração em política ou normativo de nível superior.

Art. 71. O descumprimento das disposições desta Norma sujeita o responsável às consequências previstas na legislação e nos regimes disciplinar e contratual aplicáveis, sem prejuízo das responsabilidades civis e penais cabíveis.

Art. 72. As exceções às disposições desta Norma deverão ser formalmente documentadas, justificadas e aprovadas pela [autoridade competente], observadas as competências institucionais e a criticidade dos riscos envolvidos.

§ 1º As exceções consideradas relevantes, em razão de sua criticidade, impacto ou abrangência, deverão ser submetidas à deliberação do Comitê de Segurança da Informação ou estrutura equivalente.

§ 2º Quando a exceção puder impactar a proteção de dados pessoais ou resultar em aumento de riscos aos titulares dos dados, deverá ser previamente submetida à manifestação do Comitê de Proteção de Dados Pessoais ou estrutura equivalente.

§ 3º A solicitação de exceção deverá conter, no mínimo:

I - justificativa técnica;

II - prazo de vigência;

III - plano de adequação, quando aplicável;

IV - indicação do responsável;

V - definição dos controles compensatórios adotados; e

VI - aceitação formal do risco.

[Inserir outros itens que julgar necessários].

§ 4º As exceções não poderão afastar obrigações previstas em lei, regulamento ou decisão de autoridade competente.

Art. 73. Os casos omissos e as dúvidas decorrentes da aplicação desta Norma serão analisados pela [unidade responsável pela gestão de identidades e controle de acesso], observadas as competências institucionais e a legislação aplicável.

§ 1º Quando a matéria envolver aspectos relacionados à segurança da informação, à proteção de dados pessoais, à segurança física, à gestão de pessoas ou a outros temas especializados, deverão ser previamente consultadas as unidades competentes.

§ 2º Os casos de maior relevância, que envolvam conflitos de competência, elevado impacto institucional ou interpretação de dispositivos desta Norma com repercussão transversal, poderão ser submetidos à apreciação do Comitê de Segurança da Informação ou de estrutura equivalente e, quando houver impacto sobre a proteção de dados pessoais, à apreciação do Comitê de Proteção de Dados Pessoais ou de estrutura equivalente.

[Inserir outros itens que julgar necessários].



Dúvida?

Entre em contato
conosco

Sítio do PPSI:

[PPSI 2.0 — Governo Digital](#)