Modelo de Política de Gestão de Controle de Acesso

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 2.0

Brasília, março de 2023

MODELO DE POLÍTICA DE 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 PROTEÇÃO DE DADOS

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Amaury C. da Silveira Junior

Eder Ferreira de Andrade

Francisco Magno Felix Nobre

Heráclito Ricardo Ferreira Gomes

Ivaldo Jeferson de Santana Castro

Yuri Arcanjo de Carvalho

Ramon Caldas

Guilherme Rufino Junior

Guilherme Mendonça Medeiros

Equipe Revisora

Marcelo de Lima

Marcus Paulo Barbosa Vasconcelos

Sumaid Andrade de Albuquerque

Equipe Técnica de Revisão - Versão 2.0

Ivaldo Jeferson de Santana Castro

Julierme Rodrigues da Silva

Rogério Vinícius Matos Rocha

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 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

Sumário

Aviso Preliminar e Agradecimentos....6
Introdução....7
Política de Controle de Acesso....9
Propósito [Objetivo da Política] conforme IN01 GSI/PR art.11....9
Escopo [Amplitude, alcance da Política] conforme IN01 GSI/PR art.12 item I....10
Termos e Definições [Glossário] conforme IN01 GSI/PR art.12 item II....10
Referência legal e de boas práticas [Documentos norteadores]....10
Declarações da política [Regras aplicáveis ao caso específico]....11
ANEXO I....18
ANEXO II....20

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 a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados que estão sob sua custódia. Adicionalmente, a Elaboração de uma Política de 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 os 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.

Finalmente, 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.

Este Modelo será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas neste documento.

Introdução

Este Modelo tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a elaborar sua Política de Controle de Acesso no âmbito institucional.

Os Controles 5 e 6 do Guia do Framework de Privacidade e Segurança da Informação (p. 42) estabelecem que:

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.*

O presente documento serve como um modelo prático a ser utilizado para auxiliar na adoção dos Controles 5 e 6 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. As medidas dos Controles 5 e 6 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 e 6.8.

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 órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entes como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

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

> *"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."*

Importante ressaltar que adoção deste modelo não dispensa o órgão de 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

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 03/02/2023.

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.

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 fornece os processos e procedimentos para governar o ciclo de vida da gestão das contas e credenciais.

Política de Controle de Acesso

IMPORTANTE: Este modelo deve ser utilizado exclusivamente como referência, devendo o órgão ou entidade considerar as particularidades técnicas especificas do seu ambiente, bem como observar a boa aderência aos processos internos, a fim de construir uma política que seja adequada a sua realidade.

Este modelo tem por foco prover diretrizes para o controle de acesso, a fim de atender a 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 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), referenciado na alínea f do referido inciso.

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

Responsável	Nome da pessoa ou área responsável pela gestão desta política.
Aprovado por:	Nome da pessoa ou área responsável pela aprovação e autorização da implementação desta política.
Políticas Relacionadas	Relacione outras políticas corporativas relacionadas dentro ou externas a este modelo, por exemplo, Código de Conduta\Política de Senhas \ POSIN
Localização de armazenamento	Descreva a localização física ou digital das cópias desta política.
Data da Aprovação	Data em que essa política entrou em vigor.
Data de revisão	Data em que esta política passou por revisão e atualização.
Versão	Indique a versão atual desta política

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, afirmam os objetivos básicos da política e o que a política pretende alcançar.

Exemplo: A Política de Controle de Acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações do [Nome 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 em risco de destruição, alteração, perda, roubo ou divulgação indevida.

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

Considera-se, portanto, que as credenciais: crachá de identificação funcional e logins de acesso dos sistemas de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/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 [Nome do órgão ou entidade].

Escopo [Amplitude, alcance da Política] conforme IN01 GSI/PR art.12 item I

Defina a quem e a quais sistemas esta política se aplica. Liste os agentes públicos e colaboradores necessários para cumprir ou simplesmente indique "todos" se todos devem cumprir. Também indique quaisquer exclusões ou exceções que estejam fora de escopo, ou seja, essas pessoas, elementos ou situações que não estejam cobertas por esta política ou onde uma consideração especial possa ser feita.

Esta Política se aplica a todas as informações, cuja o [Nome do órgão ou entidade] seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as 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 [Nome do órgão ou entidade].
- Todos os contratados e terceiros que trabalham para o [Nome do órgão ou entidade].
- Todos os funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação do [Nome do órgão ou entidade]

Termos e Definições [Glossário] conforme IN01 GSI/PR art.12 item II

Defina quaisquer termos-chave, siglas ou conceitos que serão utilizados na política. [Recomenda-se utilizar como referência as definições apresentadas na PORTARIA GSI/PRNº 93, DE 18 DE OUTUBRO DE 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da PRESIDÊNCIA DA REPÚBLICA].

Por 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 (multifactor authentication);

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 as quais a política deve estar em conformidade ou ser cumprida. Confirme com o departamento jurídico que a lista é completa e precisa.

Orientação	Secção
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II art. 50
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art.3, Inciso I

Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso XI CAPÍTULO VI - Seção IV – Art.15
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Instrução Normativa 01/GSI/PR	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 (Páginas 23 - 47)
CIS V8	CAPÍTULO 6
Guia do Framework de Privacidade e Segurança da Informação (PPSI)	Controles 5 e 6
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Account and Credential Management Policy Template for CIS Controls 5 and 6	Em sua íntegra

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 e proscritivas. A subdivisão desta seção em subseções pode ser necessária dependendo do comprimento ou complexidade da política.

Por exemplo:

Dos princípios gerais:

I. A Política de Gestão de Controle de Acesso deve estar alinhada com à Política de Segurança da Informação da [organização].
II. A Política de Gestão de Controle de Acesso deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

O PRESIDENTE DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO DO [Nome do órgão ou entidade]., no uso de suas atribuições e tendo em vista o disposto no [informar os dispositivos normativos que respaldam a legitimidade e autoridade do comitê de segurança para aprovar este documento].

R E S O L V E:

Art. 1º Fica aprovada, no âmbito do [Nome do órgão ou entidade], a Norma para Criação e Administração de contas de acesso, em complemento às diretrizes estabelecidas pelo Capítulo [X], da Política de Segurança da Informação - POSIN do [Nome do órgão ou entidade].

CAPÍTULO I

ACESSO LÓGICO

Art. 2º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela [Setor responsável pela gestão dos acessos], baseado nas responsabilidades e tarefas de cada usuário.

I. Terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.
II. Para fins desta Resolução, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade no [Nome do órgão ou entidade].

III. O acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada, após as devidas autorizações.

IV. Deve ser utilizado o MFA para a autenticação de acesso remoto.

V. O acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA.

Art. 3º O [Setor responsável pela gestão dos acessos], deve estabelecer e manter um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviço. Em caso de contas de serviço, o inventário deve conter no mínimo informações de:

a. Departamento proprietário.
b. Data de criação/última autorização de renovação de acesso;
c. O [Setor responsável pela gestão dos acessos], deve é responsável por validar todas as contas ativas do órgão, [a cada 90 (noventa), dias].

Art. 4º O [Setor responsável pela gestão dos acessos] deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

Art. 5º O [Setor responsável pela gestão dos acessos] deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

Art.6º O [Setor responsável pela gestão dos acessos] deve centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório ou provedor de SSO.

Art. 7º O [Setor responsável pela gestão dos acessos] deve definir e manter o controle de acesso dos usuários baseado em funções.

I. Deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da organização.
II. O [Setor responsável pela gestão dos acessos] deverá realizar análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização.

CAPÍTULO II

CONTA DE ACESSO LÓGICO E SENHA

Art. 8º Para utilização das estações de trabalho do [Nome do órgão ou entidade], será obrigatório o uso de uma única identificação (*login*) e de senha de acesso, fornecidos pela [Setor responsável pela gestão dos acessos], mediante solicitação formal pelo titular da unidade do requisitante.

I. O formulário de solicitação de acesso se encontra disponível para preenchimento na Intranet do [Nome do órgão ou entidade].

II. Os privilégios de acesso dos usuários à Rede Local devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

III. Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para a [Setor responsável pela gestão de acessos] que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 9º O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pelo [Setor responsável pela gestão de acessos] quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 10º O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, João.silva.

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, o [Setor responsável pela gestão dos acessos] realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 11º O padrão adotado para o formato da senha é o definido pelo [Setor responsável pela gestão dos acessos], que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

I. A formação da senha da identificação (*login*) de acesso à Rede Local deve seguir as regras de:

a) Possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números, para contas que utilizam MFA e 14 caracteres para contas que não utilizam MFA;
b) Recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

c) Não ser formada por 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;

d) Não utilizar termos óbvios, tais como: Brasil, senha, usuário, *password* ou *system*.

e) Não reutilizar as últimas [05 (cinco)] senhas.

II. O [Setor responsável pela gestão dos acessos] fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

Art. 12º As senhas de acesso serão renovadas a cada [90 (noventa)] dias, devendo o usuário ser informado antecipadamente a fim de que ele próprio efetue a mudança.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que a nova senha seja configurada.

CAPÍTULO III

BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 13º A conta de acesso será bloqueada nos seguintes casos:

I. Após [5 (cinco)] tentativas consecutivas de acesso errado;

II. Solicitação do superior imediato do usuário com a devida justificativa;

III. Quando da suspeita de mau uso dos serviços disponibilizados pelo [Nome do órgão ou entidade] ou descumprimento da Política de Segurança da Informação – POSIN e normas correlatas em vigência.

IV. Após [45 (quarenta e cinco)] dias consecutivos sem movimentação pelo usuário.

Art. 14º O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário ao [Setor responsável pela gestão dos acessos].

Art. 15º Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou do [Setor responsável pela Gestão de Pessoas].

Art. 16º A conta de acesso não utilizada há mais de [180 (cento e oitenta)] dias poderá ser cancelada.

Art. 17º O [Setor responsável pela Tecnologia da Informação], deve configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido. Tal prazo pode ser específico para cada tipo de ativo.

Art. 18º O [Setor responsável pela Tecnologia da Informação] deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

CAPÍTULO IV

MOVIMENTAÇÃO INTERNA

Art. 19º Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à Rede Local devem ser revogados.

I. O novo superior imediato ou o [Setor responsável pela Gestão de Pessoas] deve realizar a solicitação de novos acessos de acordo com novo setor / função do usuário.

II. Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato ou do [Setor responsável pela Gestão de Pessoas].

CAPÍTULO V

CONTA DE ACESSO BIOMÉTRICO

Art. 20º A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores.

Parágrafo único. O [Nome do órgão ou entidade] deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VI

ADMINISTRADORES

Art. 21º A utilização de identificação (*login*) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

I. Somente os técnicos da [Setor responsável pela Tecnologia da Informação], devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

II. Na necessidade de utilização de *login* com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para o [Setor responsável pela gestão dos acessos], que poderá negar os casos em que entender desnecessária a utilização.

III. 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 do [Setor responsável pela Tecnologia da Informação].

IV. Caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

V. 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.

VI. Salvo para atividades específicas da área responsável pela gestão da 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.

VII. Excepcionalmente, poderão ser concedidas identificações (*login*) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação do [Setor ou pessoa/função Responsável] por meio da [Setor responsável pela gestão dos acessos].

VIII. O [Setor responsável pela gestão dos acessos] deve implementar o MFA para todas as contas de administrador.

IX. O [Setor responsável pela gestão dos acessos] deve restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador não consiga realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário.

CAPÍTULO VII

RESPONSABILIDADES

Art. 22º É de responsabilidade do superior imediato do usuário comunicar formalmente à [Setor responsável pela Gestão de Pessoas] e o [Setor responsável pela gestão dos acessos] o desligamento ou saída do usuário do [Nome do órgão ou entidade]. para que as permissões de acesso à Rede Local sejam canceladas.

Art. 23º Caberá ao [Setor responsável pela Gestão de Pessoas] do [Nome do órgão ou entidade] a comunicação imediata ao [Setor responsável pela gestão dos acessos] sobre desligamentos, férias e licenças de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

Art. 24º É responsabilidade do [Setor responsável pela gestão de mão-de-obra terceirizada] do [Nome do órgão ou entidade] a comunicação imediata ao [Setor responsável pela gestão dos acessos] da Informação sobre desligamentos, férias e licenças de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.

I. Os serviços serão filtrados por programas de *antivírus*, *anti-phishing* e *anti-spam* e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente.

II. Nenhum técnico do [Nome do órgão ou entidade] terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores do [Nome do órgão ou entidade].

Art. 25º É de responsabilidade do [Setor responsável pela Tecnologia da Informação] o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do [Nome do órgão ou entidade].

Art. 26º O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade do [Nome do órgão ou entidade].

I. O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

II. 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.

III. O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 27º O usuário deve informar ao [Setor responsável pela Tecnologia da Informação] qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 28º É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, 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 informações internas e externas;

III. Interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV. Não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V. Não divulgar a terceiros ou a outros usuários 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 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 a utilização da respectiva conta de acesso.

CAPÍTULO VIII

DISPOSIÇÕES GERAIS

Art. 29º Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários ao [Setor responsável pela Tecnologia da Informação].

Art. 30º Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, o [Setor responsável pela Tecnologia da Informação] fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

I. Nos casos em que o ator da quebra de segurança for um usuário, o [Setor responsável pela Tecnologia da Informação] comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.

II. 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 em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

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

IV. A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Segurança da Informação - CSI do [Nome do órgão ou entidade].

Art. 31º Esta Resolução entra em vigor na data de sua publicação.

ANEXO I

Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL
[Nome do órgão ou entidade].

TERMO DE RESPONSABILIDADE

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

I. Tratar o(s) ativo(s) de informação como patrimônio do [Nome do órgão ou entidade];

II. Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do [Nome 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, do Gabinete de Segurança Institucional da Presidência da República, de 27 de maio de 2020, 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 [Nome do órgão ou entidade].;

V. Responder, perante o [Nome do 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/ou utilização de e-mail, somente com autorização (usuário/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/ou utilização de e-mail;

VII. Utilizar o correio eletrônico (*e-mail*) colocado a minha disposição 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/ou utilização de 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 estação de trabalho, bem como encerrar a seção 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/ou 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 pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Local, UF, _____de _____de _____.

_____
Assinatura
Nome do usuário e seu setor organizacional

_____
Nome da autoridade responsável pela autorização do acesso

ANEXO II

Mudanças da Versão 2.0

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Modelo de Política de Controle de Acesso.

Primeiramente, ressalta-se que as mudanças inseridas nesta versão em comparação com a anterior visam a 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 que controle 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 citadas a seguir:

No capítulo II:

- No artigo 2º, inclusão dos incisos IV e V.
- Inclusão do artigo 3º.
- Inclusão do artigo 4º.
- Inclusão do artigo 5º.
- Inclusão do artigo 6º.
- Inclusão do artigo 7º.

No capítulo II foram realizadas as seguintes inclusões:

- Atualizado o item “a” do artigo 11.

No capítulo III

- Inclusão do artigo 17.
- Inclusão do artigo 18.

No capítulo IV

- Atualização do artigo 19.

No capítulo VI

- Inclusão do inciso VIII do artigo 21.
- Inclusão do inciso IX do artigo 21.