# Controle de Acesso

## Norma de Controle de Acesso

**Tipo**: Norma | NRMA-0002 | **Nº Revisão**: 10.6

**Aprovação**: CGSI | **Elaboração**: Segurança da Informação | **Classificação**: Pública

| Tipo de Controle | Propriedades de Segurança da Informação | Conceitos de Segurança Cibernética | Capacidades Organizacionais | Domínios de Segurança |
|---|---|---|---|---|
| #Preventivo | #Confidencialidade<br>#Integridade<br>#Disponibilidade | #Proteger | #Gestão_de_identidade_e acesso | #Proteção |

## Sumário


- 1. Objetivo
- 2. Abrangência
- 3. Responsabilidades
  - 3.1. Gestores
  - 3.2. Colaboradores
  - 3.3. Parceiros e/ou clientes
  - 3.4. Segurança da Informação
  - 3.5. Comitê de Segurança da Informação
- 4. Diretrizes
  - 4.1. Acesso à infraestrutura de produção sob a gestão da área de infraestrutura.
  - 4.2. Contratação de colaboradores
  - 4.3. Identidades de Acesso
  - 4.4. Informações de autenticação
  - 4.5. Bloqueio de acesso
  - 4.6. Desligamento de colaboradores
  - 4.7. Redundância no serviço de acessos aos servidores
- 5. Segregação de Funções
- 6. Gerenciamento de Direitos de Acesso Privilegiados
- 7. Certificação de Acessos
- 8. Aprovação do Documento
- 9. Revisão e manutenção


## 1. Objetivo

Esta norma estabelece as diretrizes para o gerenciamento de acessos aos ativos de informação da Plusoft, em atendimento aos requisitos do Sistema de Gestão de Segurança da Informação (SGSI), visando assegurar que apenas usuários autorizados obtenham acesso às informações, sistemas e recursos de tecnologia conforme suas atribuições, prevenindo acessos não autorizados.

## 2. Abrangência

Esta norma aplica-se a todas as informações pertencentes ou sob custódia da Plusoft e deve ser observada por colaboradores, prestadores de serviços e fornecedores que possuam acesso ou sejam responsáveis pela administração de serviços que possibilitem o acesso às informações e soluções da Plusoft.

## 3. Responsabilidades

### 3.1. Gestores

São responsáveis por garantir que esta norma seja conhecida e seguida nos processos executados por seus subordinados, prestadores de serviços e ativos sob sua responsabilidade.

Devem zelar pela segurança das informações e dos ativos sob sua responsabilidade.

São responsáveis pelas alterações ou pela perda de confidencialidade das informações e/ou dados sob sua responsabilidade.

## 3.2. Colaboradores

Devem registrar eventos e manter as informações conforme descrito nesta norma, apoiando os gestores na criação de procedimentos e na gestão dos serviços da área.

### 3.3. Parceiros e/ou clientes

Não são responsáveis pela gestão das informações e/ou dados confiados à Plusoft, embora possam ser seus proprietários legais.

### 3.4. Segurança da Informação

É responsável por propor e manter atualizadas as normas aplicáveis ao tema.

Deve tratar as exceções identificadas e não previstas nesta norma.

### 3.5. Comitê de Segurança da Informação

É responsável pelas aprovações e revisões desta norma.

---

# 4. Diretrizes

O cumprimento desta norma é responsabilidade de todos aqueles abrangidos por seu escopo, devendo ser observadas as seguintes diretrizes.

a) Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada.

b) Assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades operacionais.

c) Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos em conformidade com as normas de segurança da informação vigentes.

d) Garantir a continuidade do processamento das informações críticas ao negócio.

e) Comunicar imediatamente à área de Segurança da Informação qualquer dúvida ou incidente que possa representar risco às atividades ou às informações da organização.

f) Zelar pelo bom funcionamento dos recursos colocados à sua disposição, operando-os sempre de acordo com as especificações.

Todos deverão tratar as informações de acordo com sua classificação, conforme definido na Norma de Gestão e Classificação da Informação, disponível na Intranet da Plusoft.

Todos deverão participar dos treinamentos de conscientização, normas e ações relacionadas à segurança da informação quando solicitado.

Todos devem comunicar à sua chefia imediata e/ou à área de Segurança da Informação sempre que identificarem informações ou aplicações críticas expostas ou acessíveis sem a proteção adequada, em desacordo com as normas, políticas e procedimentos vigentes de segurança da informação.

Cada membro da área de infraestrutura deve possuir uma única conta de acesso (login), pessoal e intransferível, conforme o perfil de acesso definido. A conta deve estar devidamente identificada e registrada, não sendo permitido o empréstimo ou a utilização do login de outro usuário.

Como as contas de acesso e senhas são pessoais e intransferíveis, seu uso indevido sujeitará o usuário às medidas aplicáveis previstas na Política Interna de Sanção Disciplinar publicada na Intranet da Plusoft.

Todos os pedidos de concessão, alteração ou revogação de acesso devem ser realizados por meio do portal interno da área responsável.

Os acessos devem ser concedidos de acordo com as atribuições e responsabilidades de cada usuário, considerando a necessidade de acesso para o desempenho de suas atividades.

## 4.1. Acesso à infraestrutura de produção sob a gestão da área de infraestrutura.

Apenas a equipe de Infraestrutura possui acesso ao console de administração do provedor de serviços em nuvem por meio da Internet, utilizando autenticação centralizada (SSO) com múltiplos fatores de autenticação (MFA).

Os administradores devem possuir uma conta de acesso (login) exclusiva para uso pessoal, de forma que suas atividades possam ser rastreadas individualmente. Os identificadores de acesso não devem indicar o nível de privilégio do usuário.

O provedor de serviços em nuvem deve permitir o controle de acesso aos serviços e recursos, possibilitando seu gerenciamento por usuário ou por grupos, de forma a facilitar a administração. Os usuários e grupos devem possuir permissões que permitam conceder ou restringir o acesso aos recursos e serviços de forma granular.

As solicitações de concessão de acesso às informações ou aos recursos de informação devem ser encaminhadas ao líder de Infraestrutura e realizadas conforme os processos de RH aplicáveis, incluindo contratação, movimentação, suspensão e desligamento.

A área de Infraestrutura é responsável pela criação, suspensão e exclusão das contas de acesso, mediante solicitação e autorização formal do gestor da informação ou em decorrência dos processos de RH aplicáveis, incluindo contratação, movimentação, suspensão e desligamento.

## 4.2. Contratação de colaboradores

A equipe de TI Interno (Service Desk) deve executar os procedimentos relacionados à concessão de acessos durante o processo de contratação de colaboradores, conforme definido na Norma de Gestão de RH, incluindo as seguintes atividades:

- Criação da credencial de acesso à VPN administrativa, quando necessária ao desempenho das atividades e responsabilidades do colaborador.
- Criação da credencial de acesso ao console de administração do provedor de serviços em nuvem, quando necessária ao desempenho das atividades e responsabilidades do colaborador.
- Disponibilização das credenciais de acesso conforme orientado no chamado de contratação aberto pela área de HX

### 4.3. Identidades de Acesso

As identidades de acesso atribuídas às pessoas com acesso às soluções Plusoft devem ser, preferencialmente, nominais e identificáveis.

A atribuição de identidades a entidades não humanas deve estar registrada em documento de controle específico (Controle de Credenciais Não Nominais), contendo, no mínimo:

- Identificação da credencial;
- Finalidade de uso;
- Tipo de acesso;
- Responsável pela credencial.

As identidades de acesso compartilhadas entre múltiplos usuários somente são permitidas quando necessárias por razões operacionais ou de negócio, devendo estar formalmente aprovadas e documentadas em controle específico, contendo, no mínimo:

- Identificação da credencial;
- Finalidade de uso;
- Tipo de acesso;
- Responsável pela credencial.

## 4.4. Informações de autenticação

As seguintes diretrizes devem ser aplicadas no processo de criação de senhas:

As senhas devem ser criadas evitando combinações de fácil dedução e observando os seguintes requisitos:

- Possuir tamanho mínimo de 8 caracteres;
- Ser compostas por combinação de caracteres alfabéticos maiúsculos e minúsculos, numéricos e especiais (%, #, $, @, &, entre outros);
- Não utilizar palavras encontradas em dicionários de qualquer idioma;
- Não utilizar números ou letras repetidos em sequência ou formando combinações óbvias, como "aaaabbbb", "12345678" ou "asdfghjk";
- Não utilizar senhas triviais ou de fácil identificação. Não devem fazer parte da senha meses do ano, dias da semana, datas, nomes de familiares, iniciais, placas de veículos, nomes relacionados à instituição, números de telefone, identificação do usuário (username), nome do usuário, grupo do usuário ou sequências numéricas com caracteres consecutivos repetidos;
- Não utilizar senhas compostas exclusivamente por caracteres alfabéticos.

Não é permitida a reutilização de senhas.

A senha deve ser alterada a cada 60 dias ou sempre que houver indicação ou suspeita de comprometimento.

Na criação da primeira senha, esta deve ser enviada ao solicitante por e-mail, conforme definido no ticket de admissão e nas diretrizes da Norma de RH, devendo ser alterada no primeiro acesso.

Sempre que tecnicamente suportado, os acessos devem utilizar autenticação multifator (MFA), associando o uso de senha a um mecanismo adicional de autenticação seguro e confiável.

O acesso à VPN administrativa e ao console de administração do provedor de serviços em nuvem deve ser realizado por meio de autenticação centralizada (SSO) e MFA, garantindo um ponto único de controle. O perfil de superadministrador, classificado nesta norma como acesso privilegiado, é tratado como exceção a esse modelo.

Sempre que houver autenticação por senha, esta deve ser apresentada de forma mascarada.

O provedor de serviços em nuvem deve suportar os requisitos de gerenciamento de senhas definidos neste item.

## 4.5. Bloqueio de acesso

A equipe de TI Interno (Service Desk), sob a gestão da área de Infraestrutura, deve bloquear o acesso dos administradores ao ambiente de produção nos seguintes casos:

- Afastamento;
- Desligamento.

As permissões de acesso atribuídas às contas devem ser revogadas nas seguintes situações:

a) Afastamentos por período superior a 15 dias, conforme diretrizes da Norma de RH.

b) Término do contrato de trabalho ou da autorização de concessão de acesso.

c) Transferência do colaborador para outra função ou área. Nesses casos, os acessos vigentes devem ser revogados e novos acessos concedidos de acordo com a nova função exercida.

Após 5 (cinco) tentativas consecutivas e malsucedidas de autenticação, o login será bloqueado. Essa configuração é realizada diretamente no serviço de autenticação centralizada (SSO).

Para o desbloqueio, o colaborador deverá solicitar ao seu gestor a abertura de um ticket no portal interno para análise e tratativa.

### 4.6. Desligamento de colaboradores

Independentemente de o desligamento ter sido solicitado pelo colaborador ou realizado pela empresa, a área de Infraestrutura e/ou a área de Segurança da Informação deverá ser comunicada imediatamente para realizar o bloqueio dos acessos, por meio da abertura de tarefa no sistema interno ou por comunicação direta, em razão da criticidade do processo.

Todos os acessos, incluindo VPN administrativa, acesso aos servidores, console de administração do provedor de serviços em nuvem e demais acessos relacionados às atividades do colaborador, deverão ser cancelados em até 2 horas úteis após a abertura do chamado.

Devem ser observados os procedimentos de desligamento definidos na Norma de Gestão de RH

### 4.7. Redundância no serviço de acessos aos servidores

O acesso dos colaboradores aos servidores da infraestrutura de produção é realizado por meio da VPN PfSense. Em caso de incidente que resulte na indisponibilidade desse serviço, o acesso poderá ser realizado por meio da VPN Sophos, garantindo a continuidade do acesso aos servidores da infraestrutura de produção

---

## 5. Segregação de Funções

Parar reduzir as oportunidades de modificação não autorizada ou não intencionada ou o uso indevido dos ativos da organização, somente os colaboradores com a função de administrador do ambiente de infraestrutura tem acesso ao ambiente hospedado no provedor de serviços em nuvem. Esse acesso é tratado como Acesso Privilegiado.
Dentro de processos ou atividades que possam ter funções conflitantes, a segregação deve estar definida no documento ou por meio de fluxo de trabalho ou por meio de Responsabilidades para cada área envolvida.

As diretrizes para o controle da segregação das funções no processo de mudança estão documentadas na Norma de Gestão de Mudanças.

As diretrizes para o controle da segregação das funções no processo de desenvolvimento que apoia esse sistema, estão documentadas na Norma de Desenvolvimento Seguro.

---

## 6. Gerenciamento de Direitos de Acesso Privilegiados

Somente os administradores do ambiente de infraestrutura estão autorizados a possuir acessos privilegiados aos ambientes hospedados no provedor de serviços em nuvem, exceto nos casos de ambientes de laboratório devidamente autorizados.

Toda solicitação de acesso privilegiado deve ser formalmente aprovada pelo Gestor da Informação e concedida pela equipe de Infraestrutura ou TI Interna, responsável pela gestão e controle de segurança do ambiente.

As atividades de administração do ambiente interno de rede devem ser executadas exclusivamente pela equipe de TI Interna, utilizando credenciais administrativas específicas.

Os usuários que possuírem acessos privilegiados devem utilizá-los somente para as atividades que exijam essas permissões, utilizando suas credenciais de uso comum para as demais atividades do dia a dia.

Os colaboradores das equipes de Infraestrutura e TI Interna que possuírem acessos administrativos devem formalizar o aceite do Termo de Acesso de Administrador, mantido no respectivo registro da área de TI Interna.

Os colaboradores da equipe de Desenvolvimento que possuírem privilégios de instalação de softwares em suas estações de trabalho, quando necessários ao desempenho de suas atividades, também devem formalizar o aceite do Termo de Acesso de Administrador, mantido no respectivo registro da área de TI Interna.

---

## 7. Certificação de Acessos

Trimestralmente, a área de Segurança da Informação realiza a certificação dos acessos.

A área de Segurança da Informação é responsável por avaliar as contas existentes nos ambientes sob sua gestão e validar, junto ao Gestor da Informação, a adequação dos acessos concedidos. Caso seja identificado qualquer desvio, o acesso deverá ser removido imediatamente após a aprovação do Gestor da Informação.

Todo o processo deve ser documentado pelo Gestor da Informação e verificado pela área de Governança, responsável por solicitar os ajustes necessários e manter sob sua custódia as evidências coletadas.

---

## 8. Aprovação do Documento

As aprovações deste documento são formalmente registradas na **Ata do Comitê de Segurança da Informação**, servindo como evidência da validação e concordância dos participantes.

---

## 9. Revisão e manutenção

Este documento deverá ser revisado quando alguma mudança ocorrer na organização que mude o contexto atual.

## 9.1 Histórico de revisões

| Versão | Data | Autor | Comentários |
|---|---|---|---|
| 1.0 | 04/08/2017 | Daniel Sabatini Freitas | Versão final. |
| 2.0 | 04/09/2017 | Daniel Sabatini Freitas | Mudança de modelo. |
| 3.0 | 06/11/2017 | Daniel Sabatini Freitas | Inclusão controles ISO27017. |
| 4.0 | 06/11/2017 | Anderson Crispim | Revisão do Documento. |
| 5.0 | 04/09/2019 | Anderson Crispim | Revisão do documento e atualização do item 8. APROVAÇÃO DO DOCUMENTO |
| 5.1 | 25/11/2019 | Patricia Albuquerque | Inclusão do item de 6. Segregação de funções para melhor esclarecimento, apontado na Auditoria Interna de 2019.<br><br>Alteração da sequência a partir desse item 6. |
| 5.2 | 07/08/2020 | Denise Paiva | Atualização do item 9. APROVAÇÃO DO DOCUMENTO |
| 5.3 | 20/08/2020 | Patricia Albuquerque | Adequação para Grupo Plusoft. |
| 5.4 | 23/09/2020 | Patricia Albuquerque | Revisão do documento. |
| 6.0 | 05/10/2020 | Patricia Albuquerque | Revisão do documento. |
| 6.1 | 01/06/2021 | Alexandre Alcantara | Revisão do documento. |
| 7.0 | 14/09/2021 | Patricia Albuquerque | Revisão, adequação ao novo layout |
| 8.0 | 20/09/2021 | Lucas Nogueira | Atualização de índice/ sumário, hiperlinks e item 8 (aprovações) |
| 8.1 | 10/11/2021 | Lucas Nogueira | Atualização do item 4,3 sobre a identificação das credenciais de acesso. |
| 9.0 | 07/10/2022 | Alexandre Alcantara | Revisão do documento. |
| 9.1 | 23/11/2022 | Patricia Albuquerque | Correção do texto do item 4.4 |
| 9.2 | 14/08/2023 | Patricia Albuquerque | Adequação a ISO27001/2022. |
| 9.3 | 14/08/2023 | Patricia Albuquerque, Alexandre Cruz | Revisão das adequações acima. |
| 9.4 | 12/09/2023 | Helio Shimosako<br><br>Alexandre Alcantara | Adicionado documento de onboarding no item 4.2 Contratação de colaboradores |
| 9.5 | 29/09/2023 | Comitê de SI | Aprovação 2023 |
| 9.6 | 05/09/2024 | Alexandre Alcantara | Revisão 2024 |
| 9.7 | 04/10/2024 | Comitê de SI | Aprovação 2024 |
| 9.8 | 21/04/2025 | Patricia Albuquerque e Henrique Pinheiro | Mudança para classificação = pública e revisão para essa mudança |

| | | | |
|---|---|---|---|
| 9.9 | 24/09/2025 | Lucas Nogueira | Revisão 2025 |
| 10.0 | 03/10/2025 | Comitê de SI | Aprovação 2025 |
| 10.1 | 07/10/2025 | Alexandre Alcantara | Revisão 2025 |
| 10.2 | 06/11/2025 | SI | Inclusão do descritivo de acessos privilegiados relacionados a itens de controle de rede. |
| 10.3 | 07/11/2025 | Comitê de SI | Aprovação para publicação |
| 10.4 | 03/09/2026 | Patricia Albuquerque | Ajustes de texto, gramática e concordância. |
| 10.5 | 30/10/2026 | Comitê de SI | Aprovação 2026 |
| 10.6 | 23/10/2026 | Helio Shimosako | Revisão 2026 |