Controle de Acesso

Norma de Controle de Acesso

Tipo: Norma | NRMA-0002 | **Nº Revisão**: 10.0

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 #Integridade #Disponibilidade	#Proteger	#Gestão_de_identidade_e acesso	#Proteção

Sumário

1. Objetivo

Este documento fornece diretrizes para a gestão de acessos, atendendo aos requisitos de um sistema de gestão de segurança da informação (SGSI), garantindo que usuários autorizados obtenham acesso quando necessário evitando o acesso não autorizado aos sistemas de informações.

2. Abrangência

Este documento aplica-se a todas as informações pertencentes ou sob custódia da Plusoft. Portanto, deve ser observado por todos os colaboradores, prestadores de serviços e fornecedores de serviços que tenham acesso ou gerenciem qualquer tipo de serviço que permite o acesso a qualquer tipo de informação das soluções Plusoft.

3. Responsável

3.1. Gestores

São responsáveis por avaliar e garantir que esta norma seja conhecida e seguida em procedimentos executados por seus subordinados, prestadores de serviços ou ativos correspondentes as suas alçadas.

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

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

3.2. Colaboradores

Registrar eventos e manter as informações conforme descrito na norma, apoiar os gestores na criação dos procedimentos ou na gestão de serviços da área.

3.3. Parceiros e/ou clientes

Não podem ser responsáveis pela gerência das informações e/ou dados confiados a Plusoft, embora sejam os seus proprietários legais.

3.4. Segurança da Informação

Propor e manter atualizadas as normas aplicáveis à matéria.

Tratar as exceções encontradas, não previstas nesta norma.

3.5. Comitê de Segurança da Informação

Realizar as aprovações e revisões propostas nesta norma.

---

4. Diretrizes

É de responsabilidade dos COLABORADORES, o uso e o sigilo das informações, de sua competência ou não, conforme a Política de Segurança da Informação - PSI e o Termo de Compromisso, Sigilo e Confidencialidade, devidamente assinados, onde se comprometem sobre toda e qualquer informação que venham a ser divulgadas por pessoas ou instituições inadvertidamente.

O cumprimento dessa norma é compromisso de todos e devem obedecer às 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 acessados e protegidos em conformidade com as normas de segurança da informação vigente.

d) Garantir a continuidade do processamento das informações críticas aos negócios.

e) Comunicar imediatamente a área de Segurança da Informação, quando ocorrer qualquer tipo de dúvida ou incidente, podendo ou não causar algum risco as suas atividades.

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

Todos deverão dar o tratamento adequado às informações de acordo com sua classificação conforme a Norma de Gestão e Classificação da Informação, disponíveis na Intranet da Plusoft.

Todos deverão participar dos treinamentos sobre conscientização, normas e ações proativas sobre segurança da informação quando solicitado.

Todos devem comunicar a sua chefia imediata e/ou a Segurança da Informação quando informações ou aplicações críticas estiverem expostas ou de fácil acesso, não protegida conforme as recomendações, normas, políticas e procedimentos de segurança da informação vigentes.

Cada membro da área de infraestrutura deve possuir uma única conta/login (username) pessoal e intransferível, conforme o perfil de acesso definido, devendo ser identificado e registrado não sendo permitido o empréstimo ou a utilização do login de outro usuário. Na medida em que o usuário está ciente de que sua conta/login e senha são pessoais e intransferíveis o uso indevido do mesmo sujeitará o usuário a medidas aplicáveis conforme Política interna de sanção disciplinar, publicada na Intranet da Plusoft.

Todos os pedidos de novos acessos, mudança ou revogação, deverão ser feitos através do Portal interno da área.

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

Apenas a equipe de infraestrutura possui acesso a console de administração do provedor do serviço em nuvem através da Internet, sendo o método de autenticação através de SSO com MFA.

Os administradores devem ter um identificador de conta de acesso (login) exclusivo para seu uso pessoal, de modo que as atividades possam ser rastreadas até o responsável individual. Os identificadores de conta de acesso (login) não devem dar nenhuma indicação do nível de privilégio do usuário, por exemplo, gerente ou coordenador.

O provedor de serviços em nuvem deve permitir o controle do acesso aos serviços e/ou recursos, podendo gerenciá-los por usuário ou através de grupos que facilitem a administração. Os usuários ou grupos devem possuir permissões que possibilitem conceder ou negar acesso aos recursos e /ou serviços de forma granular.

Os pedidos de concessão de acesso às informações ou aos recursos de informação, encaminhados ao líder de infraestrutura, devem ser realizados após os processos de RH (contratação, movimentação, suspensão e desligamento).

A área de infraestrutura é responsável pela criação, suspensão e exclusão das contas, mediante solicitações e autorizações formais do gestor da informação ou por processos de RH (contratação, movimentação, suspensão e desligamento).

4.2. Contratação de colaboradores

A equipe de TI Interno (service-desk) deve realizar os seguintes procedimentos no ciclo de contratação dos profissionais definidos na Norma de Gestão de RH, e as tarefas abaixo descritas:

- Criação de credencial de acesso à VPN administrativa, onde o acesso é necessário à sua competência e responsabilidade.
- Criação de credencial de acesso ao console de administração do provedor do serviço em nuvem, onde o acesso é necessário à sua competência e responsabilidade;
- Disponibilização das credenciais de acesso, conforme direcionado no chamado de contratação aberto pelo time de HX.

4.3. Identidades de Acesso

É altamente recomendado que as identidades atribuídas e destinadas às pessoas com acesso as soluções Plusoft sejam nominais e identificáveis.

A atribuição de identidades a entidades não humanas, devem estar especificadas em um documento de controle (Controle de Credenciais Não Nominais) com os seguintes requisitos especificados:

- Identificação da Credencial
- Finalidade de Uso
- Tipo de Acesso
- Dono da Credencial

As identidades atribuídas a várias pessoas (não-nominais) só são permitidas quando forem necessárias e por razões de negócios ou operacionais, e estão sujeitas à aprovação e documentação dedicada, contendo:

- Identificação da Credencial
- Finalidade de Uso
- Tipo de Acesso
- Dono da Credencial

4.4. Informações de autenticação

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

As senhas devem ser criadas evitando o uso de combinações de fácil dedução, e considerando os aspectos a seguir para a sua composição:

- As senhas devem ter um tamanho mínimo de 8 caracteres;
- Devem ser formadas a partir da combinação de caracteres alfabéticos, maiúsculos e minúsculos, numéricos e especiais (%, #, $, @, &, entre outros);
- Não devem ser usadas palavras encontradas em dicionários de qualquer idioma;
- Não devem ser usados números ou letras repetidas, em sequência ou formando séries óbvias, como, por exemplo, “aaaabbbb”, “12345678”, “asdfghjk”;
- Senhas triviais, por serem de fácil identificação, não devem ser utilizadas. Itens que não devem fazer parte da senha: meses do ano, dias da semana ou qualquer outro dado relativo a datas, nomes de familiares, iniciais, placas de carro, nomes comuns à instituição, números de telefone, identificação do usuário (username), nome do usuário, grupo do usuário, sequência numérica com mais de dois caracteres idênticos consecutivos, etc;
- Não sendo permitido o uso de senhas totalmente alfabéticas.

Não deve ser feita a reutilização de senhas.

A senha deve ser alterada a cada 60 dias, ou a qualquer momento que houver indicação ou suspeita de que houve seu comprometimento.

Na criação da primeira senha do usuário, a mesma deve ser enviada ao solicitante através do e-mail (enviado no ticket de admissão conforme diretrizes da Norma de RH) e deve ser trocado no primeiro acesso.

O acesso deverá preferencialmente usar a verificação de dois fatores, ou seja, além do uso de senha "forte" acima, a utilização de um autenticador seguro e confiável.

O acesso à VPN administrativa e/ou ao console de administração do provedor de serviço em nuvem deve ser realizado através autenticação centralizada (SSO) e MFA, garantindo assim um ponto único de controle. Somente o perfil de superadministrador, considerado abaixo como "Acesso privilegiado" não segue essa regra.

Em qualquer local que tenha autenticação, a senha deve estar mascarada como default.

O provedor do serviço em nuvem deve fornecer as diretrizes de gerenciamento de senhas informadas nesse item.

4.5. Bloqueio de acesso

A equipe de TI-Interno (Service-desk), sob gestão da área de infraestrutura deve bloquear o acesso dos administradores ao ambiente de produção nos seguintes cenários descritos abaixo:

- Afastamentos;
- Desligamento.

As permissões de acesso atribuídas às contas devem ser revogadas quando ocorrer alguma das seguintes situações:

a) Nos casos de afastamentos por períodos de ausência do colaborador superiores a 15 dias conforme diretriz 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. Neste caso, as permissões de acesso correntes devem ser revogadas devendo ser atribuídas novos acessos.

Após 5 (cinco) tentativas consecutivas e mal sucedidas de identificação do usuário, ocorrerá o bloqueio do login. Essa configuração é feita diretamente nas configurações do SSO.

Para o desbloqueio o colaborador deve avisar seu gestor para que seja aberto um ticket no portal para análise.

4.6. Desligamento de colaboradores

Independente se o colaborador solicitou desligamento ou foi desligado por parte da empresa a área de infraestrutura e/ou a área de Segurança da Informação deverá ser avisada em imediato para prover o devido bloqueio dos acessos, através da criação da tarefa no sistema interno, ou presencialmente, devido a criticidade do processo.

Todos os acessos desde à VPN administrativa, acesso aos servidores, console de administração do provedor de serviço em nuvem e demais outros acessos deverão ser cancelados até 2 horas úteis após a abertura do chamado.

Deverão ser seguidos os processos de Desligamento descritos 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 feito através da VPN Pfsense e caso ocorra algum incidente que cause indisponibilidade, é ativado o acesso através da VPN Sophos.

---

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

Apenas os administradores do ambiente de infraestrutura devem ter acessos privilegiados para o acesso ao ambiente hospedado no provedor de serviços em nuvem.

Toda a solicitação de concessão de acesso privilegiado deve ter a ciência formal do dono da informação e a segurança da informação deve acompanhar o processo de concessão de acesso.

Os membros da área de infraestrutura da Plusoft apenas terão os acessos privilegiados para a administração do ambiente concedido após a assinatura dos seguintes termos descritos abaixo:

- Termo de Compromisso, Sigilo e Confidencialidade
- Termo de Aceite da PSI
- Termo de responsabilidade pela guarda e uso do equipamento de trabalho

Os devidos termos acima devem estar devidamente assinados pelos colaboradores, membros da área de infraestrutura, onde uma (01) cópia deverá estar sob custódia do RH, armazenado na área do colaborador.

Usuários de acesso privilegiados deverão usar os mesmos somente para realização de tarefas administrativas, usando no seu dia a dia suas identidades de rede normal.

---

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 presentes no ambiente e certificar junto ao gestor da informação a veracidade dos acessos. Caso seja identificado qualquer desvio o acesso é removido em imediato após aprovação do Gestor da informação.

Todo processo deve ser documentado pelo Gestor da Informação e verificado pelo Security Officer que é responsável por solicitar o ajuste dos acessos e manter sob custódia todas 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	[redacted]	Versão final.
2.0	04/09 /2017	[redacted]	Mudança de modelo.
3.0	06/11 /2017	[redacted]	Inclusão controles ISO27017.
4.0	06/11 /2017	[redacted]	Revisão do Documento.
5.0	04/09 /2019	[redacted]	Revisão do documento e atualização do item 8. APROVAÇÃO DO DOCUMENTO
5.1	25/11 /2019	[redacted]	Inclusão do item de 6. Segregação de funções para melhor esclarecimento, apontado na Auditoria Interna de 2019. Alteração da sequência a partir desse item 6.
5.2	07/08 /2020	[redacted]	Atualização do item 9. APROVAÇÃO DO DOCUMENTO
5.3	20/08 /2020	[redacted]	Adequação para Grupo Plusoft.
5.4	23/09 /2020	[redacted]	Revisão do documento.
6.0	05/10 /2020	[redacted]	Revisão do documento.
6.1	01/06 /2021	[redacted]	Revisão do documento.
7.0	14/09 /2021	[redacted]	Revisão, adequação ao novo layout
8.0	20/09 /2021	[redacted]	Atualização de índice/ sumário, hiperlinks e item 8 (aprovações)
8.1	10/11 /2021	[redacted]	Atualização do item 4,3 sobre a identificação das credenciais de acesso.
9.0	07/10 /2022	[redacted]	Revisão do documento.
9.1	23/11 /2022	[redacted]	Correção do texto do item 4.4
9.2	14/08 /2023	[redacted]	Adequação a ISO27001/2022.
9.3	14/08 /2023	[redacted]	Revisão das adequações acima.
9.4	12/09 /2023	[redacted]	Adicionado documento de onboarding no item 4.2 Contratação de colaboradores
9.5	29/09 /2023	[redacted]	Aprovação 2023
9.6	05/09 /2024	[redacted]	Revisão 2024
9.7	04/10 /2024	[redacted]	Aprovação 2024
9.8	21/04 /2025	[redacted]	Mudança para classificação = pública e revisão para essa mudança

9.9	24/09 /2025	[redacted]	Revisão 2025
10.0	03/10 /2025	Comitê de SI	Aprovação 2025