



Norma Gestão de Acesso Lógico

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

SUMÁRIO

1. OBJETIVO	3
2. CAMPO DE APLICAÇÃO.....	3
3. DEFINIÇÕES	3
4. PAPÉIS E RESPONSABILIDADES.....	4
4.1. Gestor Imediato	4
4.2. Equipe de Infraestrutura de TI.....	4
4.3. Gerente de Infraestrutura de TI.....	4
4.4. Área de Gente e Gestão (Recursos Humanos).....	5
4.5. Colaborador.....	5
5. DESCRIÇÃO	5
5.1. Requisitos do negócio para controle de acesso	5
5.2. Gerenciamento de acesso do usuário	5
5.2.1. Registro e cancelamento de usuário.....	5
5.2.2. Gerenciamento dos direitos de acesso	7
5.2.3. Provisionamento de acesso para usuários	8
5.3. Procedimentos de entrada nos sistemas.....	8
5.3.1. Controles de entrada nos sistemas (login/logon)	9
5.3.2. Política de Senhas – Acesso comum	9
5.3.3. Política de Senhas – Acesso privilegiado	10
5.3.3.1 Termo de Responsabilidade.....	10
5.3.3.2 Critérios mínimos obrigatórios.....	10
5.3.3.3 Restrições adicionais de uso	10
5.3.3.4 Procedimentos em caso de incidente	10
5.3.3.5.1 Windows/Active Directory (contas privilegiadas)	12
5.3.3.5.2 Linux (PAM).....	12
5.3.3.5.3 Banco de Dados	13
5.4. Análise crítica dos direitos de acesso	13
6. EVIDÊNCIAS GERADAS	14
7. DOCUMENTOS DE REFERÊNCIA.....	14
8. REGISTRO DE ALTERAÇÕES.....	14
9. FORMALIZAÇÃO	15

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

1. OBJETIVO

Esta Norma estabelece as regras para a gestão e controle de acesso aos sistemas de informação gerenciados pela Equipe de Infraestrutura de TI, incluindo os requisitos definidos para controle dos acessos, a gestão do ciclo de vida dos acessos, as revisões periódicas, a análise crítica dos direitos de acesso, a política de senhas e os procedimentos de entrada nos sistemas.

2. CAMPO DE APLICAÇÃO

Aplicável a todos os colaboradores, próprios ou terceiros, que utilizam recursos de TI fornecidos pelo **Grupo Benner*** para o exercício de suas atividades.

* Denominação utilizada para designar as empresas: Benner Sistemas S.A., Benner Tecnologia e Sistemas em Saúde Ltda., Benner Tecnologia e Serviços em Saúde Ltda., Otto HX Tecnologia e Sistemas Ltda, Moderna Sistemas Ltda, Nexorede Tecnologia Ltda e Itecsa Tecnologia e Serviços S.A.

3. DEFINIÇÕES

- **Active Directory (AD):** Banco de dados com informações sobre o ambiente de rede (usuários, grupos de acesso, computadores, impressoras, servidores etc.), gerenciando as permissões de acesso entre esses diversos componentes por meio de Group Policy (GPO).
- **Credencial de acesso:** Login de usuário (User ID) e senha para acesso à rede e aos demais sistemas de informação utilizados na Empresa.
- **Diretiva de Grupo ou Group Policy (GPO):** Funcionalidade do Active Directory (AD) composta por um conjunto de regras que controlam o que os usuários podem ou não fazer em um sistema de computador. Permite o gerenciamento e configuração centralizados de sistemas operacionais, aplicativos e configurações dos usuários no ambiente de rede.

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

- **Organizational Unit (OU):** Unidade administrativa dentro de um domínio do Active Directory (AD), em que um administrador pode vincular objetos de Política de Grupo e atribuir permissões a outros usuários / grupos.
- **Siscon:** Sistema utilizado para registro e atendimento de chamados relativos à infraestrutura de TI do Grupo Benner. Acessível por meio do endereço: <https://siscon.benner.com.br/>. ou Minha Benner, <https://minhabenner.com.br/>, sistema para registro de chamados integrado ao siscon.

Outros termos e definições utilizados no contexto da Segurança da Informação podem ser consultados no MSI - Manual de Segurança da Informação.

4. PAPÉIS E RESPONSABILIDADES

4.1. Gestor Imediato

Assegurar que os colaboradores sob sua responsabilidade conheçam e compreendam os papéis e responsabilidades em segurança da informação; registrar e/ou aprovar no sistema Siscon as solicitações de criação, modificação e exclusão de acesso à rede e aos sistemas de informação para os Usuários de TI sob sua responsabilidade; revisar periodicamente as permissões de acesso dos Colaboradores em sua área/departamento e reportar as atualizações necessárias à Equipe de Infraestrutura de TI.

4.2. Equipe de Infraestrutura de TI

Atender as solicitações de criação, modificação e exclusão de credenciais de acesso à rede e demais sistemas de informação sob sua responsabilidade, observando os requisitos de negócio e as normas existentes; realizar periodicamente a revisão de Acesso Lógico; manter os registros e os controles atualizados.

4.3. Gerente de Infraestrutura de TI

Avaliar e emitir parecer (aprovado / reprovado) relativo às solicitações de acesso privilegiado; revisar periodicamente e aprovar a lista de usuários com acesso privilegiado à rede e demais sistemas de informação gerenciados pela Equipe de Infraestrutura de TI.

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

4.4. Área de Gente e Gestão (Recursos Humanos)

Atualizar os eventos de ausência temporária dos Colaboradores próprios (tais como férias, licenças, desligamento etc.) no sistema BENNER RH.

4.5. Colaborador

Manter a guarda segura das credenciais de acesso à rede e aos sistemas de informação utilizados; seguir todas as recomendações de segurança, as políticas, normas e procedimentos e controle de acesso estabelecidos pela Empresa; notificar à Equipe de Infraestrutura de TI por meio da abertura de um chamado no sistema Siscon, caso seja identificada qualquer anormalidade no uso dos sistemas a que tem acesso.

Outras definições de papéis, atividades e responsabilidades no contexto de segurança da informação estão detalhadas na Seção 6 da PSI - Política de Segurança da Informação.

5. DESCRIÇÃO

5.1. Requisitos do negócio para controle de acesso

Os acessos aos recursos de rede e às aplicações utilizadas na Empresa devem ser concedidos observando o princípio de mínimo privilégio, que equivale a conceder somente os acessos necessários ao desempenho das atividades para os quais os colaboradores foram designados. Além disso, os acessos só serão liberados para os usuários que tiverem sido treinados no conteúdo que compõe a Política de Segurança da Informação. Sendo assim, o TCOM (termo de compromisso) assinado é um pré-requisito importante para assegurar que os colaboradores conheçam as regras, diretrizes, melhores práticas e restrições que foram estabelecidas pela Empresa para o uso aceitável dos ativos de TI.

5.2. Gerenciamento de acesso do usuário

5.2.1. Registro e cancelamento de usuário

A criação de credenciais de acesso à rede corporativa é iniciada exclusivamente a partir de solicitação formal da área de Recursos Humanos, como parte do processo de admissão de novos colaboradores. Essa solicitação contém os dados cadastrais, o perfil de acesso, o líder

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

imediatamente e as ferramentas necessárias para o desempenho da função, e é direcionada à Equipe de Infraestrutura de TI para execução das providências.

Cada credencial é única, intransferível e rastreável, permitindo a autenticação do usuário nos sistemas corporativos e o monitoramento das atividades realizadas. Todas as criações de usuários são registradas por meio do sistema de chamados, sob responsabilidade da Equipe de Infraestrutura de TI.

Sistemas corporativos hospedados em nuvem podem ser acessados remotamente, desde que observadas as medidas de segurança definidas na Política de Segurança da Informação (PSI), como autenticação multifator (MFA), VPN e restrições de perfil, conforme aplicável.

Os eventos de ausência temporária (como férias e licenças) ou definitiva (como desligamento) de colaboradores próprios são atualizados no sistema BENNER RH pela área de Recursos Humanos. Com base nessas informações, é executada automaticamente uma rotina de verificação e tratamento de acessos, agendada para ocorrer de segunda a sexta-feira, às 6h.

Essa rotina consulta o status do colaborador por meio de atributos personalizados no Active Directory e executa as ações conforme os seguintes critérios:

Status	Ação aplicada
Trabalhando	Acesso mantido
Afastado	Acesso bloqueado temporariamente
Demitido (ou status equivalente)	Acesso revogado definitivamente

Tabela 1 – Critérios de tratamento de acessos conforme o status do colaborador

A autenticação dessa rotina é realizada por certificado digital, garantindo segurança no processo. Todas as ações são registradas em log com data, usuário, tipo de ação e mensagem de status.

Além disso, cabe ao Gestor Imediato registrar no sistema de abertura de chamados corporativo vigente as atualizações decorrentes de movimentações internas (como

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

transferências) ou alterações contratuais envolvendo Provedores Externos de Serviço, assegurando a consistência entre função e acessos concedidos.

Prazos para revogação de acesso (quando não cobertos pela rotina automática):

- a) Colaboradores próprios com acessos privilegiados: revogação em até 4 (quatro) horas úteis após ciência formal do evento pelo RH ou Gestor Imediato;
- b) Demais acessos de colaboradores próprios: revogação em até 1 (um) dia útil após ciência formal;
- c) Provedores Externos de Serviço (terceiros): o Gestor do Contrato deve abrir solicitação no **sistema de abertura de chamados corporativo vigente** imediatamente após o término do vínculo ou mudança contratual. Prazos: 4 (quatro) horas úteis para credenciais privilegiadas e 1 (um) dia útil para credenciais comuns.

Todas as revogações manuais devem gerar evidência com “antes/depois” (capturas de tela e/ou extrações do diretório/sistema-alvo) anexadas ao chamado no **sistema de abertura de chamados corporativo vigente**, contendo: identificação do usuário/conta, data/hora, ativo/sistema, ação aplicada e responsável pela execução/validação.

5.2.2. Gerenciamento dos direitos de acesso

Existem dois tipos de acesso que podem ser concedidos aos usuários:

- **Acesso comum:** concedido a todos os usuários que executam atividades no ambiente Produtivo dos sistemas, de acordo com a rotina do departamento.
- **Acesso privilegiado:** concedido a usuários que possuem funções diferenciadas dentro dos sistemas de informação, tais como: administrador de domínio de rede, administrador de sistema operacional, administrador de banco de dados, desenvolvedor, homologador (usuário-chave), equipes de suporte, usuário de programas utilitários etc.

Os acessos definidos como privilegiados devem ser restritos e controlados. Por isso, as credenciais de acesso serão concedidas mediante assinatura do Colaborador no Termo de Responsabilidade de Acesso Privilegiado. Para possibilitar o rastreamento e auditoria das atividades realizadas, os logs de auditoria devem ser ativados para estes usuários. Tal

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

controle se faz necessário, uma vez que os acessos privilegiados podem ser capazes de sobrepor outros controles de segurança existentes nos sistemas utilizados na Empresa.

Toda solicitação de acesso privilegiado deve ser avaliada e aprovada pelo Gerente de Infraestrutura de TI, que poderá consultar outros gestores, quando necessário. Além da identificação da função que requer acesso privilegiado, é importante verificar em quais ambientes o acesso privilegiado deverá ser concedido, respeitando as diretrizes de segregação de funções entre os ambientes de Produção, Homologação, Desenvolvimento, Testes, Treinamento e outros eventualmente existentes nos sistemas de informação.

5.2.3. Provisionamento de acesso para usuários

Cabe ao Gestor Imediato a definição dos perfis de acesso à rede e aos sistemas para os colaboradores sob sua responsabilidade, levando em conta o princípio de mínimo privilégio, os requisitos de proteção de dados e a disponibilidade dos recursos necessários.

Sempre que houver necessidade de criação, alteração ou exclusão de acesso à rede e demais sistemas de informação, o Gestor Imediato deve registrar uma solicitação no **sistema de abertura de chamados corporativo vigente**.

Cabe à Equipe de Infraestrutura de TI atender as solicitações, considerando os recursos disponíveis e os requisitos definidos pelas áreas de negócio. Se necessário, a Equipe poderá acionar o suporte de provedores de serviços externos à organização.

Em caso de restrições ou divergências, a Equipe de Infraestrutura de TI deve verificar os ajustes necessários junto ao Gerente de Infraestrutura de TI e/ou Gestor Imediato do usuário.

5.3. Procedimentos de entrada nos sistemas

As políticas vigentes de logon e senha estão registradas na aba [Política Logon Senha] da planilha NAL RAL - Registros de Acesso Lógico, diferenciando as regras aplicáveis de acordo com o tipo de acesso: comum e privilegiado.

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

5.3.1. Controles de entrada nos sistemas (login/logon)

Os usuários devem efetuar logon nos sistemas utilizando suas próprias credenciais de acesso. Usuários com permissão de acesso privilegiado devem utilizar estas credenciais específicas somente para realizar as intervenções devidamente registradas e aprovadas. É proibida a utilização das credenciais de acesso privilegiado para realizar as atividades relacionadas ao acesso comum.

Caso haja bloqueio da conta de usuário por exceder o número máximo de tentativas de logon, o usuário deve aguardar o período necessário para o desbloqueio automático ou abrir um chamado no **sistema de abertura de chamados corporativo vigente** para que a Equipe de Infraestrutura de TI possa efetuar o desbloqueio.

É vedada a utilização de usuários genéricos e/ou compartilhados entre os departamentos. Eventuais exceções devem ser registradas pelo Gestor Imediato com as devidas justificativas, para que possam ser avaliadas pelo Gerente de Infraestrutura de TI.

Observação: para contas com acesso privilegiado, não se aplica o desbloqueio automático. Nesses casos, o procedimento deve ser realizado exclusivamente pela Equipe de Infraestrutura de TI, mediante validação e registro **no sistema de abertura de chamados corporativo vigente**, conforme critérios estabelecidos nas seções 5.3.3.

5.3.2. Política de Senhas – Acesso comum

Ao receber um chamado para criação de credenciais de acesso à rede corporativa, a equipe de TI gera uma senha temporária, que é impressa e entregue ao Colaborador.

A senha temporária deve ser alterada no primeiro logon do usuário, obedecendo os requisitos de tamanho e complexidade configurados nos sistemas e descritos na aba [Política Logon Senha] da planilha NAL RAL - Registros de Acesso Lógico.

É de responsabilidade de cada usuário a guarda segura de suas credenciais de acesso à rede e aos demais sistemas de informação utilizados. Caso seja identificada qualquer anormalidade, a Equipe de Infraestrutura de TI deve ser notificada por meio da abertura de um chamado no **sistema de abertura de chamados corporativo vigente**.

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

5.3.3. Política de Senhas – Acesso privilegiado

As credenciais de acesso privilegiado apresentam risco elevado à organização e, por isso, estão sujeitas a regras mais rigorosas de controle.

5.3.3.1 Termo de Responsabilidade

- O usuário deve assinar previamente um **Termo de Responsabilidade** específico, reconhecendo as obrigações associadas ao uso de credenciais privilegiadas.

5.3.3.2 Critérios mínimos obrigatórios

Requisito	Valor mínimo/obrigatório
Tentativas até bloqueio	3 tentativas consecutivas de login inválido
Desbloqueio automático	Não permitido — desbloqueio manual pela Equipe de Infraestrutura de TI mediante validação
Bloqueio por inatividade	Sessão bloqueada após 4 minutos de inatividade
Tamanho mínimo da senha	12 caracteres
Complexidade mínima	4 dos 4 requisitos: letra maiúscula, letra minúscula, número e caractere especial
Restrições	Proibido o uso de partes do nome da empresa
Validade da senha	60 dias
Histórico de senhas	Bloqueio de reutilização das últimas 24 senhas
Duração mínima da senha	Não definida

5.3.3.3 Restrições adicionais de uso

- O uso de credenciais privilegiadas deve se restringir estritamente às atividades para as quais foram atribuídas.
- É **proibido** utilizar credenciais privilegiadas para funções operacionais cotidianas.

5.3.3.4 Procedimentos em caso de incidente

- Caso haja qualquer indício de comprometimento, a senha deve ser alterada **imediatamente**.
- O incidente deve ser reportado à **Equipe de Infraestrutura de TI** por meio do **sistema de abertura de chamados corporativo vigente**.

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

Nota de hierarquia e prevalência:

Como funciona a relação entre os itens:

- *Os critérios mínimos obrigatórios definidos em 5.3.3.2 valem para todas as plataformas e tecnologias.*
- *O detalhamento técnico em 5.3.3.5 mostra como esses critérios mínimos são implementados em cada sistema (Windows, Linux, Banco de Dados).*
- *Se algum parâmetro técnico for mais rigoroso que o mínimo, aplica-se o mais rigoroso.*
- *Se a tecnologia não permitir aplicar exatamente o mínimo, deve ser adotado um controle equivalente, aprovado pela área de TI e registrado no sistema de chamados.*
- *Em caso de dúvida, sempre prevalece a regra mais restritiva.*

RESUMO PARA CLIENTE/AUDITOR (INFORMATIVO – NÃO NORMATIVO)

- 5.3.3 = O que é obrigatório para todos.
- 5.3.3.5 = Como aplicar isso em cada tecnologia.
- Sempre vale o mais restritivo
- Se não for possível, registre e compense.

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

5.3.3.5 Critérios mínimos por plataforma (acessos privilegiados)

Os parâmetros abaixo mostram como os critérios mínimos obrigatórios definidos em 5.3.3 são aplicados tecnicamente em cada plataforma. Sempre que possível, utilize o parâmetro mais restritivo. Limitações técnicas devem ser tratadas conforme orientação da área de TI e registradas formalmente.

5.3.3.5.1 Windows/Active Directory (contas privilegiadas)

Requisito	Parâmetro	Valor mínimo/obrigatório
Tentativas até bloqueio	<i>Account lockout threshold</i>	3
Desbloqueio automático	<i>Account lockout duration</i>	Desabilitado (0 – somente administrador desbloqueia)
Reset do contador de falhas	<i>Reset account lockout counter</i>	≥ 15 minutos
Senha	Complexidade e tamanho	≥ 12 caracteres; complexidade habilitada
Histórico de senha	<i>Enforce password history</i>	≥ 24
Validade de senha	<i>Maximum password age</i>	60 dias

5.3.3.5.2 Linux (PAM)

Requisito	Parâmetro	Valor mínimo/obrigatório	Significado
Complexidade	<i>pam_pwquality</i>	<i>retry=3</i>	Permite até 3 tentativas antes de falhar
		<i>minlen=12</i>	Senha deve ter no mínimo 12 caracteres
		<i>dcredit=-1</i>	Requer pelo menos 1 dígito
		<i>ucredit=-1</i>	Requer pelo menos 1 letra maiúscula
		<i>lcredit=-1</i>	Requer pelo menos 1 letra minúscula
		<i>ocredit=-1</i>	Requer pelo menos 1 caractere especial
		<i>difok=24</i>	Diferentes da senha anterior
Validade de senha	<i>enforce_for_root</i>		Aplicar ao usuário root
	<i>PASS_MAX_DAYS 60</i>	60	Validade máxima da senha
	<i>PASS_MIN_DAYS 0</i>	0	Validade mínima da senha
	<i>PASS_WARN_AGE 14</i>	14	Dias para aviso de expiração

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

5.3.3.5.3 Banco de Dados

Plataforma	Requisito	Parâmetro	Valor mínimo/obrigatório
Oracle	Expiração de senha	PASSWORD_LIFE_TIME	60 dias
	Tentativas até bloqueio	FAILED_LOGIN_ATTEMPTS	3
	Complexidade	PASSWORD_VERIFY_FUNCTION	ORA12C_VERIFY_FUNCTION (ou equivalente, ≥12 car., 4 classes)
SQL Server	Política de senha	CHECK_POLICY / CHECK_EXPIRATION	Habilitados; herdar políticas do domínio

5.4. Análise crítica dos direitos de acesso

Trimestralmente, a Equipe de Infraestrutura de TI realiza a Revisão de Acesso Lógico. Para cada ativo crítico de TI:

- É extraída a lista de permissões de usuários vigente (“antes”) e enviada ao Gestor Imediato para validação;
- O Gestor Imediato deve responder em até 3 (três) dias corridos após o envio, aprovando ou solicitando ajustes;
- Ajustes solicitados devem ser formalizados via sistema de abertura de chamados corporativo vigente (ex.: Siscon);
- Acessos não revisados dentro do prazo serão removidos em até 2 (dois) dias após o término do SLA de resposta;
- Finalizada a revisão, é anexada evidência “antes/depois” ao chamado (incluindo query/listagem, data/hora, responsável e decisão do gestor).

Durante a revisão, os usuários desabilitados no período são movidos para a OU de Usuários Desligados no Active Directory, conforme rotina automatizada.

Todas as permissões de acesso dos usuários para cada ativo crítico de TI são listadas e enviadas para avaliação do Gestor Imediato. Caso sejam necessários ajustes, o Gestor Imediato deve abrir solicitação no sistema de abertura de chamados corporativo vigente, indicando as correções necessárias.

Todas as atividades realizadas pela Equipe de Infraestrutura de TI durante a Revisão de Acesso Lógico devem ser registradas no sistema de abertura de chamados corporativo vigente.

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

Quaisquer exceções nos procedimentos de entrada nos sistemas (regras de logon e senhas) devem estar documentadas e serão reavaliadas a cada Revisão de Acesso Lógico.

6. EVIDÊNCIAS GERADAS

- **Sistema de abertura de chamados corporativo vigente:** registro das solicitações de criação, alteração ou exclusão de acesso à rede e demais sistemas de informação sob a responsabilidade da Equipe de Infraestrutura de TI; agendamento e registro das revisões periódicas de acesso lógico.
- **BENNER RH:** Sistema utilizado para gestão de pessoal (Colaboradores próprios).
- **TCOM** - Termo de Compromisso e Responsabilidade assinado pelos Usuários de TI.
- **Termo de Responsabilidade** específico para usuários com Acesso Privilegiado.
- **Planilha NAL RAL** - Registros de Acesso Lógico: preenchida e assinada a cada ocorrência da Revisão de Acesso Lógico e anexada nos respectivos chamados gerados no **sistema de abertura de chamados corporativo vigente**.

7. DOCUMENTOS DE REFERÊNCIA

- BENNER. Política de Segurança da Informação (PSI). [S.I.]: Grupo Benner, 2024.
- BENNER. Manual de Segurança da Informação (MSI). [S.I.]: Grupo Benner, 2024.
- BENNER. Norma de Gestão de Acesso Físico (NAF). [S.I.]: Grupo Benner, 2024.

8. REGISTRO DE ALTERAÇÕES

Versão	Data	Etapa	Responsável
00	27/06/2022	Emissão do documento	Jane Glauce R. Coimbra
01	28/08/2024	Revisão	Jorge Espinhara (BENNER)
02	25/09/2025	Revisão	Jorge Espinhara (BENNER)

PSI.IE.001-2– Norma de Gestão de Acesso Lógico

9. FORMALIZAÇÃO

ELABORAÇÃO/REVISÃO		APROVAÇÃO	
Jorge Espinhara – Governança de TI		Severino Benner - CEO	
25/09/2025	<div>DocuSigned by: Jorge Luiz Carvalho Espinhara 40FC1E7A18DC49D...</div>	25/09/2025	<div>DocuSigned by: Severino Benner B5112A47CD594F7...</div>