

	GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Emissão 14/10/2024	Classificação Uso interno
		Versão 1.03	Aprovado por: P!nk Corp Administration.

1. Introdução

- 1.1. A Norma de Gestão de Identidade e Controle de Acesso complementa a Política Geral de Segurança da Informação da P!NK CORP, fornecedora de serviços de cartões de benefícios corporativos. Esta norma define diretrizes para garantir que o acesso aos sistemas e ativos de informação seja seguro e adequado às necessidades operacionais, protegendo dados e mantendo a integridade dos recursos computacionais.

2. Propósito

- 2.1. Estabelecer diretrizes para a gestão de identidade e controle de acesso, assegurando que o uso dos sistemas e ativos de informação seja realizado por usuários autorizados e de maneira segura.


3. Escopo

- 3.1. Esta norma se aplica a todos os colaboradores, terceiros e prestadores de serviço que possuam acesso aos sistemas e ativos de informação da P!NK CORP.

4. Diretrizes

4.1. Acesso a Ativos e Sistemas de Informação

- 4.1.1. **Concessão de Contas:** Cada usuário autorizado receberá uma conta de acesso pessoal e intransferível. Essas contas destinam-se exclusivamente ao uso profissional, sendo responsabilidade do usuário assegurar a confidencialidade de suas credenciais;
- 4.1.2. **Responsabilidade pelo Uso:** Os usuários são responsáveis pelo uso de suas contas e responderão por qualquer acesso ou ação realizada por meio de suas credenciais, inclusive atividades irregulares realizadas por terceiros;
- 4.1.3. **Medidas de Prevenção:** Os usuários devem: nunca compartilhar suas senhas e credenciais de acesso, não anotar ou armazenar senhas em locais desprotegidos e informar imediatamente qualquer falha de segurança à equipe de segurança da informação;

	GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Emissão 14/10/2024	Classificação Uso interno
		Versão 1.03	Aprovado por: P!nk Corp Administration.

4.2. Controle e Utilização de Senhas

4.2.1. **Política de Senhas:** As senhas devem ser pessoais e intransferíveis, seguindo os padrões de segurança definidos abaixo:

4.2.1.1. **Complexidade:** Senhas para contas não-administrativas devem ter no mínimo 8 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais. Senhas para contas administrativas devem ter pelo menos 15 caracteres;

4.2.1.2. **Validade e Expiração:** Senhas têm validade de 90 dias, e o sistema exigirá uma nova senha ao final desse período;

4.2.1.3. **Bloqueio de Tentativas:** Após cinco tentativas de login inválidas, a conta será bloqueada por 30 minutos;

4.2.1.4. **Histórico de Senhas:** O sistema manterá um histórico das últimas 12 senhas, impedindo sua reutilização;

4.2.1.5. **Restrições de Composição:** A senha não pode conter o nome do usuário, dados pessoais ou informações facilmente associadas ao titular da conta.


4.3. Acesso com Privilégios

4.3.1. **Contas Privilegiadas:** Usuários com permissões administrativas devem utilizar uma credencial específica para atividades de alto nível e outra conta comum para atividades diárias;

4.3.2. **Controle e Restrição de Privilégios:** Privilégios administrativos são concedidos apenas para funções que exigem acesso elevado, e seu uso deve ser monitorado e registrado para auditoria.

4.4. Autorização e Revogação de Acesso

4.4.1. **Gestão de Permissões:** O nível de acesso é determinado com base no perfil e nas necessidades do cargo do usuário, sendo periodicamente revisado pelos gestores de informação e equipe de TI;

	GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Emissão 14/10/2024	Classificação Uso interno
Código N-SI-003		Versão 1.03	Aprovado por: P!nk Corp Administration.

4.4.2. **Solicitação e Aprovação:** A concessão e revogação de acessos são processadas mediante solicitação dos gestores e coordenadores. A revogação deve ser solicitada imediatamente após o desligamento do colaborador ou encerramento do contrato de terceiros.

4.5. Expectativa de Privacidade

4.5.1. **Armazenamento e Monitoramento de Dados:** Arquivos armazenados na infraestrutura corporativa ou na nuvem não têm expectativa de privacidade. A P!NK CORP reserva-se o direito de monitorar o acesso e uso desses dados para garantir a conformidade com as políticas internas.

5. Papéis e Responsabilidades

5.1. Gestor da Informação

5.1.1. Autoriza e revoga acessos, define o nível de privilégio adequado e realiza revisões periódicas das autorizações e credenciais;

5.2. Departamento de Recursos Humanos


5.2.1. Notifica a TI sobre desligamentos ou transferências de funcionários, assegurando que as credenciais de acesso sejam desativadas ou ajustadas de acordo com a mudança de função;

5.3. Gestores e Coordenadores

5.3.1. Solicitam concessão de acesso para novos colaboradores ou alterações para funções específicas. Também devem informar à TI sobre o término de contratos com terceiros que tenham acesso aos sistemas;

5.4. Gerência de Tecnologia da Informação

5.4.1. Processa solicitações de criação e remoção de contas, concede privilégios conforme solicitado e revisa periodicamente a validade das credenciais e níveis de acesso dos usuários.

	GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Emissão 14/10/2024	Classificação Uso interno
		Versão 1.03	Aprovado por: P!nk Corp Administration.

6. Sanções e Punições

- 6.1. Qualquer violação das diretrizes de gestão de identidade e controle de acesso será tratada como incidente de segurança, estando sujeita às sanções previstas na Política Geral de Segurança da Informação. As punições variam de advertências e suspensão até a rescisão do contrato, conforme a gravidade da infração.

7. Revisões

- 7.1. Esta norma é revisada anualmente ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

- 8.1. A norma **N-SI-003** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da P!NK CORP.
- 8.2. A presente norma foi aprovada no dia 14/10/2024