POLÍTICA DE GESTÃO DE ACESSOS, SENHAS E CREDENCIAIS FÍSICAS

Versão: 1.0 | **Responsável:** TI / Segurança da Informação

Classificação: Interno

1. OBJETIVO

Estabelecer diretrizes claras e abrangentes para a criação, modificação, monitoramento e revogação de acessos lógicos e físicos, garantindo a segurança da informação, rastreabilidade completa das operações e conformidade com normas internacionais como ISO 27001, ISO 27002 e TISAX.

2. ESCOPO E APLICABILIDADE

Esta política se aplica a:

- Todos os colaboradores efetivos, estagiários, aprendizes e temporários;
- Terceiros, prestadores de serviço, consultores e parceiros de negócio;
- Visitantes com acesso temporário às instalações;
- Todos os sistemas corporativos, incluindo ERP, Active Directory (AD), e-mail corporativo, sistemas de gestão, aplicações web e redes locais;
- Acessos físicos controlados por crachá, biometria ou outros mecanismos de identificação.

3. PRINCÍPIOS FUNDAMENTAIS

A organização adota os seguintes princípios para gestão de acessos e credenciais:

Princípio	Descrição
Identidade individual	Cada usuário deve possuir credenciais únicas e intransferíveis, permitindo rastreamento completo de todas as ações realizadas.
Mínimo privilégio	Usuários devem receber apenas as permissões estritamente necessárias para o desempenho de suas funções.
Segregação de funções	Evitar concentração de privilégios críticos em uma única pessoa, prevenindo fraudes e erros operacionais.
Rastreabilidade completa	Todas as ações de criação, modificação e exclusão de acessos devem ser registradas via chamados, com data, hora, responsável e justificativa.
Autorização formal	Nenhum acesso deve ser concedido sem aprovação formal e documentada do gestor direto ou liderança imediata.

4. RESPONSABILIDADES

4.1 Setor de TI / Segurança da Informação

- Gerenciar e executar todas as ações de concessão, modificação e revogação de acessos conforme esta política;
- Bloquear imediatamente acessos ou credenciais em caso de violação de segurança;
- Garantir conformidade com práticas recomendadas de ISO 27001 e TISAX;
- Realizar auditorias periódicas de acessos ativos e permissões concedidas;
- Notificar gestores sobre qualquer irregularidade identificada.

4.2 Gestores e Líderes de Equipe

- Solicitar acessos de acordo com a função e necessidade real do colaborador;
- Aprovar formalmente todas as solicitações via sistema de chamados;
- Notificar imediatamente a TI sobre desligamentos, férias prolongadas ou mudanças de função;
- Revisar periodicamente os acessos da equipe e solicitar ajustes quando necessário.

4.3 Usuários Finais

- Utilizar exclusivamente suas credenciais pessoais e mantê-las em absoluto sigilo;
- **Não compartilhar senhas, crachás ou tokens sob nenhuma circunstância;**
- Reportar imediatamente à TI qualquer situação suspeita, perda de credenciais ou tentativa de acesso não autorizado;
- Bloquear seu computador sempre que se ausentar da estação de trabalho.

5. GESTÃO DE ACESSOS LÓGICOS

5.1 Criação de Novo Acesso

1. Toda solicitação de acesso deve ser formalizada via sistema de chamados da empresa;
2. O gestor direto deve aprovar explicitamente a solicitação, especificando os sistemas e permissões necessários;
3. A TI aplicará as permissões conforme o princípio do mínimo privilégio, avaliando a real necessidade;
4. Todas as evidências (logs, prints, relatórios) devem ser registradas e arquivadas adequadamente.

5.2 Alteração de Acesso Existente

5. Exige abertura de novo chamado com aprovação formal do gestor;
6. A TI deve validar possíveis conflitos de segregação de funções antes de aplicar as modificações;
7. Todas as alterações devem ser documentadas com justificativa e evidências.

5.3 Remoção e Bloqueio de Acesso

A remoção de acesso deve ocorrer imediatamente nas seguintes situações:

- **Desligamento ou término de contrato;**
- Mudança de função ou transferência de área;
- Detecção de acesso indevido ou não autorizado;
- **Compartilhamento de credenciais (senha ou crachá);**

Importante: No caso de desligamento, o bloqueio deve ocorrer no momento da comunicação oficial ao RH, mesmo que a data de saída seja futura.

6. GESTÃO DE SENHAS

6.1 Requisitos de Segurança

- **As senhas são pessoais, individuais e intransferíveis;**
- Devem seguir a política de complexidade definida no Active Directory via GPO (Group Policy Object);
- Requisitos mínimos: 8 caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais;
- **É expressamente proibido o compartilhamento sob qualquer circunstância;**
- Senhas devem ser alteradas a cada 90 dias ou imediatamente em caso de suspeita de comprometimento.

6.2 Tratamento de Violações

Em caso de senha compartilhada, as seguintes ações serão tomadas imediatamente:

8. A conta é bloqueada imediatamente;
9. Um incidente de segurança é registrado formalmente;
10. O gestor direto é notificado para as devidas providências;
11. A senha é redefinida após análise e autorização;
12. Medidas disciplinares podem ser aplicadas conforme políticas internas de RH.

7. GESTÃO DE CREDENCIAIS FÍSICAS (CRACHÁS)

7.1 Diretrizes de Uso

- **Crachás são pessoais e intransferíveis;**
- Devem ser portados de forma visível durante toda a permanência nas instalações;
- Não podem ser emprestados, compartilhados ou utilizados por terceiros;
- Perda ou extravio deve ser comunicada imediatamente ao RH.

7.2 Tratamento de Violações

- TI/RH deve bloquear imediatamente crachás identificados como compartilhados;
- Toda ação de bloqueio deve ser registrada formalmente como incidente de segurança;
- O gestor deve ser notificado para providências cabíveis.

8. EVIDÊNCIAS E DOCUMENTAÇÃO

Todos os acessos criados, alterados ou removidos devem ser formalizados para fins de auditoria e conformidade

- .

9. TRATAMENTO DE INCIDENTES E VIOLAÇÕES

9.1 Situações que Exigem Bloqueio Imediato

- **Senhas compartilhadas ou divulgadas;**
- **Crachás utilizados por terceiros;**
- Acessos concedidos sem autorização formal;
- Múltiplas tentativas de login com falha (possível ataque);
- Acesso a sistemas fora do horário habitual sem justificativa.

9.2 Fluxo de Tratamento

13. **Bloqueio imediato** da conta ou credencial comprometida;
14. **Registro formal do incidente** com data, hora, tipo de violação e ações tomadas;
15. **Notificação imediata ao gestor** e ao setor de RH, se aplicável;
16. **Investigação do incidente** para identificar extensão do problema;

10. REVISÃO PERIÓDICA DE ACESSOS

Para garantir conformidade contínua e identificar acessos desnecessários ou obsoletos, as seguintes ações devem ser realizadas:

- **Revisão trimestral** dos acessos ativos por parte dos gestores;
- **Auditoria semestral** pela TI/Segurança da Informação para validar conformidade;
- Revisão de acessos administrativos e privilegiados mensalmente;

11. REVISÃO E ATUALIZAÇÃO DA POLÍTICA

Esta política deve ser revisada periodicamente para garantir sua eficácia e conformidade com as melhores práticas e normas vigentes.

11.1 Periodicidade de Revisão

- **Revisão ordinária:** a cada 12 meses;
- **Revisão extraordinária:** sempre que houver alteração estrutural significativa na organização;
- **Revisão emergencial:** após incidente de segurança relevante ou mudança regulatória.

11.2 Aprovação e Divulgação

As revisões devem ser:

- Aprovadas pela Diretoria/Alta Administração;
- Comunicadas a todos os colaboradores e terceiros;

12. DISPOSIÇÕES FINAIS

O não cumprimento desta política poderá resultar em medidas disciplinares conforme regulamento interno da empresa, incluindo advertências, suspensões e, em casos graves, desligamento por justa causa.