

POLÍTICA DE GESTÃO DE ACESSOS

1. Objetivo

Esta Política tem por objetivo estabelecer diretrizes para a concessão, utilização, alteração e revogação de acessos aos recursos tecnológicos utilizados pela TGV Tecnologia, bem como aos ambientes disponibilizados por seus clientes, visando proteger as informações corporativas, reduzir o risco de acessos não autorizados e apoiar a prestação segura dos serviços.

2. Abrangência

Esta Política aplica-se a todos os colaboradores, sócios, estagiários, prestadores de serviços e terceiros que utilizem recursos tecnológicos da TGV ou tenham acesso aos ambientes tecnológicos dos clientes durante a execução de suas atividades.

3. Princípios

A gestão de acessos deverá observar os seguintes princípios:

- necessidade de uso;
- menor privilégio;
- responsabilidade individual;
- confidencialidade das credenciais;
- conformidade com as políticas da TGV e dos clientes.

Os acessos deverão ser concedidos apenas quando necessários para o desempenho das atividades profissionais.

4. Concessão de Acessos

Os acessos aos recursos tecnológicos da TGV serão concedidos conforme a necessidade das atividades desempenhadas.

Os acessos aos ambientes tecnológicos dos clientes dependerão da autorização e dos procedimentos definidos pelo respectivo contratante.

Sempre que possível, os acessos deverão estar associados a usuários individualmente identificados, permitindo sua rastreabilidade.

5. Utilização das Credenciais

As credenciais de acesso são pessoais, individuais e intransferíveis.

É proibido:

- compartilhar senhas ou credenciais;

- utilizar contas de outros usuários;
- permitir que terceiros utilizem sua identificação de acesso;
- registrar senhas em locais de fácil acesso ou divulgação.

Os colaboradores deverão manter suas credenciais sob sigilo e comunicar imediatamente qualquer suspeita de comprometimento.

6. Autenticação

Sempre que disponível e compatível com os recursos tecnológicos utilizados, recomenda-se a utilização de mecanismos adicionais de autenticação para reforçar a proteção dos acessos.

Quando os clientes exigirem métodos específicos de autenticação, estes deverão ser integralmente observados pelos colaboradores da TGV durante a utilização de seus ambientes.

7. Utilização dos Acessos

Os acessos concedidos deverão ser utilizados exclusivamente para execução das atividades profissionais autorizadas.

É vedada a utilização dos acessos para:

- atividades particulares;
- obtenção de informações sem necessidade profissional;
- qualquer finalidade não autorizada pela empresa ou pelo cliente.

8. Acessos Privilegiados

Os acessos com privilégios administrativos ou elevados deverão ser concedidos apenas quando necessários para execução das atividades contratadas.

Sempre que possível, esses acessos deverão permanecer ativos somente pelo período necessário à realização das atividades e observar os controles definidos pelo cliente ou pela TGV, conforme aplicável.

9. Ambientes dos Clientes

Durante a utilização dos ambientes tecnológicos dos clientes, os colaboradores deverão observar integralmente:

- as políticas de segurança estabelecidas pelo cliente;
- os controles de acesso definidos pelo cliente;
- as restrições de utilização dos sistemas;
- os procedimentos operacionais comunicados pelo cliente.

Quando exigido contratualmente, deverão ser utilizados equipamentos, métodos de autenticação ou demais mecanismos de segurança definidos pelo contratante.

10. Alteração e Revogação dos Acessos

Os acessos deverão ser alterados ou revogados sempre que ocorrer:

- desligamento do colaborador;
- alteração de função;
- encerramento das atividades que justificaram a concessão do acesso;
- solicitação do cliente;
- identificação de utilização inadequada.

Sempre que possível, a revogação deverá ocorrer tempestivamente após a perda da necessidade de utilização do acesso.

11. Responsabilidades dos Colaboradores

São responsabilidades dos colaboradores:

- utilizar os acessos exclusivamente para fins profissionais;
- manter o sigilo das credenciais;
- bloquear a estação de trabalho sempre que se ausentarem;
- comunicar imediatamente qualquer suspeita de uso indevido ou comprometimento das credenciais;
- observar as políticas de segurança da TGV e dos clientes.

12. Registro e Monitoramento

Os registros relacionados aos acessos poderão ser mantidos pelos recursos tecnológicos utilizados pela TGV ou pelos próprios clientes, conforme seus respectivos mecanismos de controle.

Esses registros poderão ser utilizados para fins de auditoria, investigação de incidentes, atendimento a requisitos legais ou comprovação das atividades executadas.

13. Responsabilidades Compartilhadas

Considerando o modelo de atuação da TGV, a gestão dos acessos aos ambientes dos clientes constitui responsabilidade compartilhada.

Compete aos clientes, quando aplicável:

- definir os perfis de acesso;
- conceder e revogar credenciais sob sua administração;
- estabelecer seus mecanismos de autenticação;

- administrar seus ambientes tecnológicos.

Compete à TGV:

- solicitar apenas os acessos necessários para execução dos serviços;
- utilizar corretamente os acessos concedidos;
- comunicar quando determinado acesso deixar de ser necessário;
- orientar seus colaboradores quanto ao cumprimento desta Política e das políticas de segurança estabelecidas pelos clientes.

14. Descumprimento

O descumprimento desta Política poderá resultar na adoção das medidas administrativas, disciplinares, civis ou legais cabíveis, conforme a gravidade da ocorrência.

15. Vigência

Esta Política entra em vigor na data de sua aprovação e permanecerá válida até sua revisão ou substituição.

Aprovado por:

Jefferson Alencar da Silva

Diretor de Serviços

Brasília, 27 de janeiro de 2026