

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Objetivo

Esta Política de Segurança da Informação tem por objetivo estabelecer diretrizes para proteger as informações corporativas da TGV Tecnologia e as informações às quais seus colaboradores tenham acesso durante a prestação de serviços aos clientes, preservando sua confidencialidade, integridade e disponibilidade, garantindo a integridade das operações e prevenindo incidentes de segurança.

Considerando que a TGV atua predominantemente como empresa de consultoria, implantação, suporte e licenciamento de soluções tecnológicas, a presente política estabelece os princípios de segurança aplicáveis às atividades da empresa, observando também as políticas e controles de segurança definidos pelos clientes em seus respectivos ambientes.

2. Abrangência

Esta política aplica-se a todos os colaboradores, sócios, estagiários, prestadores de serviços e terceiros que atuem em nome da TGV Tecnologia, independentemente do vínculo contratual, bem como, no que couber, aos visitantes.

3. Revisão da Política

Esta política deverá ser revisada, no mínimo, anualmente ou sempre que houver alterações relevantes na legislação, nos processos internos, nos riscos de segurança ou no modelo de atuação da empresa.

As revisões deverão ser aprovadas pela direção da empresa e comunicadas aos colaboradores.

4. Responsabilidades

É responsabilidade de todos os colaboradores:

- cumprir esta Política de Segurança da Informação;
- proteger as informações da empresa e dos clientes;
- comunicar situações que possam representar riscos à segurança das informações;
- utilizar adequadamente os recursos tecnológicos disponibilizados pela empresa;

- observar as políticas de segurança estabelecidas pelos clientes durante a execução dos serviços.

A direção da empresa é responsável por promover a manutenção desta política e apoiar sua implementação.

5. Gestão dos Ativos

Os ativos de informação disponibilizados pela empresa deverão ser utilizados exclusivamente para fins profissionais.

Cada colaborador é responsável pela guarda, utilização adequada e preservação dos equipamentos, documentos e demais ativos sob sua responsabilidade.

O inventário dos ativos de informação da TGV deverá ser realizado e mantido atualizado sempre que necessário e, obrigatoriamente, no mínimo, a cada 2 (dois) anos.

Os colaboradores deverão respeitar os termos de responsabilidade e de confidencialidade relativos aos ativos de informação, conforme estabelecido no contrato de admissão ou no instrumento contratual aplicável.

No desligamento ou encerramento do vínculo, o colaborador, prestador de serviço ou terceiro deverá devolver todos os ativos sob sua responsabilidade. A TGV deverá revogar, bloquear ou solicitar a revogação dos respectivos acessos, credenciais e autorizações imediatamente ou dentro do prazo definido no processo de desligamento.

6. Confidencialidade das Informações

Todas as informações corporativas da TGV e as informações dos clientes obtidas durante a execução dos serviços deverão ser tratadas como confidenciais, salvo quando houver autorização expressa para sua divulgação.

Os colaboradores deverão utilizar essas informações exclusivamente para a execução das atividades profissionais relacionadas ao contrato vigente.

É vedada a utilização ou divulgação de informações para finalidade diversa daquela autorizada.

7. Acordos de Confidencialidade

Colaboradores, parceiros e terceiros deverão observar os termos de responsabilidade e os acordos de confidencialidade firmados entre as partes. A formalização de acordo de confidencialidade (Non-Disclosure Agreement — NDA) será obrigatória sempre que houver necessidade de acesso a informações ou dados de clientes para execução de provas de conceito ou de valor (POC ou POV).

As obrigações de confidencialidade permanecem válidas mesmo após o encerramento do vínculo contratual.

8. Utilização de Informações dos Clientes

Quando houver necessidade de utilização de informações disponibilizadas pelos clientes para execução de projetos, provas de conceito, atividades de suporte ou demais serviços contratados, essas informações deverão ser utilizadas exclusivamente para a finalidade prevista. É terminantemente proibida a utilização ou o armazenamento de dados pessoais sensíveis de clientes em provas de conceito ou de valor (POC ou POV).

Ao término das atividades, todas as informações e todos os dados de clientes utilizados em provas de conceito ou de valor (POC ou POV), inclusive eventuais cópias, deverão ser eliminados de forma segura. Nas demais atividades, as informações deverão ser devolvidas ou eliminadas conforme estabelecido contratualmente ou segundo orientação formal do cliente.

9. Controle de Acesso aos Ambientes dos Clientes

O acesso aos ambientes tecnológicos dos clientes deverá ocorrer exclusivamente quando necessário para execução dos serviços contratados.

Os colaboradores deverão observar integralmente:

- as políticas de segurança do cliente;
- os controles de acesso estabelecidos pelo cliente;
- as restrições de utilização dos ambientes disponibilizados;
- as orientações fornecidas pelos responsáveis do cliente.

Sempre que exigido contratualmente, deverão ser utilizados equipamentos, credenciais ou mecanismos de autenticação definidos pelo próprio cliente.

10. Utilização de Serviços Corporativos

Os documentos e informações corporativas deverão ser armazenados preferencialmente nos repositórios corporativos disponibilizados pela empresa.

Os colaboradores deverão evitar o armazenamento permanente de informações corporativas exclusivamente em equipamentos locais ou em serviços não autorizados pela empresa.

11. Proteção e Recuperação das Informações

A TGV adota como estratégia de armazenamento a utilização de serviços corporativos disponibilizados por fornecedores especializados, buscando garantir disponibilidade e recuperação das informações corporativas.

Sempre que possível, os documentos deverão permanecer armazenados nos repositórios corporativos disponibilizados pela empresa.

Considerando o modelo de atuação da TGV, os ambientes produtivos, bases de dados e aplicações dos clientes permanecem sob responsabilidade dos respectivos contratantes, inclusive quanto aos procedimentos de backup e recuperação, salvo disposição contratual específica em contrário.

12. Utilização de Dispositivos de Armazenamento

Não é permitida a utilização de mídias ou dispositivos removíveis para armazenamento ou transferência de informações corporativas ou de clientes por parte dos colaboradores.

13. Gestão de Incidentes

Situações que possam comprometer a segurança das informações, a continuidade dos serviços ou o atendimento aos clientes deverão ser registradas por meio dos canais corporativos definidos pela empresa.

Os incidentes deverão ser acompanhados até sua conclusão, buscando minimizar impactos e registrar as ações adotadas.

Quando envolverem ambientes ou informações dos clientes, deverão ser observados também os procedimentos definidos pelo respectivo contratante.

14. Conscientização

A TGV promoverá ações e comunicados periódicos de conscientização sobre Segurança da Informação, visando orientar seus colaboradores quanto às boas práticas de proteção das informações, à utilização adequada dos recursos tecnológicos e às ameaças de segurança atuais.

15. Política de Mesa Limpa

Todos os colaboradores deverão observar as diretrizes estabelecidas na Política de Mesa Limpa da TGV, mantendo documentos e equipamentos protegidos contra acesso não autorizado.

A Política de Mesa Limpa complementa as diretrizes estabelecidas neste documento.

16. Controle de Acesso Físico

O acesso às dependências físicas da empresa deverá ser controlado por meio de biometria digital e pelos demais controles estabelecidos pela TGV.

Pessoas que não integrem o quadro de colaboradores somente poderão acessar as dependências físicas da empresa quando autorizadas e acompanhadas, durante toda a permanência, por colaborador devidamente autorizado.

17. Responsabilidades Compartilhadas

Considerando o modelo de negócio da TGV, parte dos controles de segurança relacionados aos ambientes tecnológicos utilizados na prestação dos serviços permanece sob responsabilidade dos respectivos clientes.

Entre esses controles podem estar incluídos, conforme cada contrato:

- administração da infraestrutura tecnológica;
- segurança de redes;
- gestão de vulnerabilidades;
- gestão de logs;
- administração de identidades e acessos aos ambientes do cliente;
- backup e recuperação dos ambientes produtivos;
- monitoramento de segurança.

Compete à TGV cumprir as políticas estabelecidas pelos clientes durante a utilização desses ambientes, proteger as informações às quais tiver acesso e manter controles internos compatíveis com sua atuação.

18. Descumprimento

O descumprimento desta política poderá resultar, conforme a gravidade da ocorrência, em medidas administrativas, disciplinares, civis ou legais cabíveis, incluindo advertência, suspensão temporária, rescisão do vínculo de trabalho ou contratual e adoção das medidas legais apropriadas.

19. Vigência

Esta política entra em vigor na data de sua aprovação, permanecendo válida até sua revisão ou substituição.

Aprovado por:

Jefferson Alencar da Silva
Diretor de Serviços

Brasília, 12 de janeiro de 2026