

1. INTRODUÇÃO

A Trucks Control reconhece a segurança da informação como pilar estratégico da continuidade e da confiabilidade de suas operações. Esta política estabelece as diretrizes adotadas pela organização para proteger as informações próprias e de terceiros sob sua responsabilidade contra acesso, uso, divulgação, modificação ou destruição não autorizada.

Esta é a versão pública da Política de Segurança da Informação, alinhada aos requisitos da **ISO/IEC 27001:2022**, às boas práticas da **ISO/IEC 27002:2022** e a normas correlatas (ISO/IEC 27035, ISO/IEC 27701 e ISO 22301). As regras operacionais, os procedimentos e os controles que a sustentam constam de normas internas de circulação restrita.

2. OBJETIVOS DE SEGURANÇA DA INFORMAÇÃO

A Trucks Control está comprometida em implementar e monitorar seus controles de segurança da informação para garantir a confidencialidade, a integridade e a disponibilidade de todo ativo de informação, atendendo aos requisitos legais e contratuais das partes interessadas, sempre buscando a melhoria contínua de seus processos e serviços.

Do compromisso assumido decorrem:

- **Controles implementados e monitorados:** manter os controles de segurança da informação operantes e sob monitoramento contínuo, e não apenas formalmente documentados.
- **Conformidade legal e contratual:** observar a legislação aplicável, com destaque para a Lei Geral de Proteção de Dados Pessoais, e os requisitos contratuais assumidos perante clientes, parceiros e demais partes interessadas.
- **Melhoria contínua:** aperfeiçoar de forma permanente os processos, os serviços e o Sistema de Gestão de Segurança da Informação, com base em indicadores, auditorias, análises críticas e lições aprendidas.

As metas e os indicadores associados são acompanhados pelo Comitê de Segurança da Informação e submetidos à análise crítica da Direção.

3. ABRANGÊNCIA

Esta política aplica-se a todos os colaboradores, prestadores de serviço, parceiros, fornecedores, consultores e terceiros que tenham acesso, direto ou indireto, às informações ou aos sistemas sob responsabilidade da Trucks Control.

Alcança todos os tipos de informação, independentemente do meio (digital, físico, verbal ou visual) e da forma de armazenamento, processamento ou transmissão.

4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

- **Confidencialidade:** garantir que as informações sejam acessíveis apenas a pessoas devidamente autorizadas;
- **Integridade:** assegurar a exatidão e a completude das informações e sistemas, protegendo-os contra alterações indevidas;
- **Disponibilidade:** garantir que as informações e sistemas estejam acessíveis a usuários autorizados sempre que necessário;
- **Autenticidade:** confirmar a identidade de usuários, sistemas e fontes de informação;
- **Responsabilidade:** assegurar que todas as ações relacionadas ao uso de informações sejam rastreáveis e atribuíveis.

5. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

5.1. Governança e Responsabilidades

- A Alta Direção aprova, apoia e provê os recursos necessários à implementação desta política;
- O Comitê de Segurança da Informação é responsável por supervisionar o Sistema de Gestão de Segurança da Informação, aprovar planos de ação e acompanhar indicadores;
- A área de Segurança da Informação implementa controles, conduz a gestão de incidentes, realiza auditorias e zela pela conformidade com esta política;
- Todos os colaboradores e terceiros devem cumprir as diretrizes desta política, participar dos treinamentos aplicáveis e reportar incidentes.

5.2. Gestão de Riscos

- A Trucks Control adota metodologia formal de avaliação e tratamento de riscos de segurança da informação, considerando impacto e probabilidade;
- Os resultados das avaliações são revisados periodicamente ou sempre que houver mudanças significativas no ambiente de negócio ou tecnológico.

5.3. Classificação e Tratamento da Informação

As informações são classificadas conforme o seu grau de sensibilidade:

- **Pública:** acesso irrestrito;
- **Interna:** acesso restrito a colaboradores;
- **Confidencial:** acesso limitado a grupos autorizados;
- **Restrita:** acesso limitado à alta gestão ou funções críticas.

Cada nível de classificação possui regras específicas de armazenamento, compartilhamento, transmissão e descarte seguro.

5.4. Controle de Acesso

- O acesso a sistemas e informações segue o princípio do menor privilégio e é revisado periodicamente;
- As contas de usuários são únicas, autenticadas e rastreáveis;
- A autenticação multifator é exigida para acessos administrativos e remotos.

5.5. Segurança em Recursos Tecnológicos

- Os dispositivos corporativos contam com proteção contra código malicioso, criptografia e controle de atualizações;
- A rede corporativa é segmentada e monitorada, com uso de mecanismos de proteção de perímetro, acesso remoto seguro e registros de auditoria;
- O uso de mídias removíveis é controlado e monitorado;
- As cópias de segurança são realizadas com regularidade e testadas periodicamente quanto à restauração.

5.6. Proteção de Dados e Privacidade

- O tratamento de dados pessoais observa os princípios e as bases legais da Lei Geral de Proteção de Dados Pessoais;
- Dados pessoais sensíveis são protegidos por criptografia, controle de acesso e registro de auditoria;
- A coleta e o uso de dados pessoais têm finalidade legítima, específica e informada, com base legal adequada e registro documental;
- As condições de tratamento, os direitos dos titulares e os canais de atendimento são detalhados na Política Externa de Privacidade e Proteção de Dados Pessoais do Grupo Trucks Control.

5.7. Segurança em Fornecedores e Terceiros

- Fornecedores que processam, armazenam ou acessam informações da Trucks Control são avaliados quanto à conformidade em segurança da informação e privacidade, conforme as diretrizes desta política;
- Os contratos contemplam cláusulas específicas de confidencialidade, notificação de incidentes e responsabilidade por violações.

5.8. Gestão de Incidentes de Segurança

- Os incidentes de segurança da informação devem ser reportados imediatamente ao canal oficial csi@tcsat.com.br
- O tratamento observa o Plano de Resposta a Incidentes, alinhado à ISO/IEC 27035, contemplando as fases de identificação, contenção, erradicação, recuperação e lições aprendidas;
- São mantidos registros dos incidentes e das ações corretivas adotadas;
- Nas hipóteses previstas em lei, a comunicação a titulares de dados pessoais e à Autoridade Nacional de Proteção de Dados é realizada nos prazos e nas condições aplicáveis.

5.9. Continuidade de Negócios e Recuperação de Desastres

A Trucks Control mantém Sistema de Gestão de Continuidade de Negócios integrado ao Sistema de Gestão de Segurança da Informação, assegurando abordagem unificada de resiliência organizacional.

O Plano de Continuidade de Negócios, alinhado aos princípios da ISO 22301, define estratégias, procedimentos e responsabilidades para a manutenção das operações críticas em situações de interrupção.

Testes de prontidão e simulações periódicas são conduzidos para avaliar a eficácia dos planos, identificar oportunidades de melhoria e fortalecer os controles preventivos e de recuperação.

5.10. Uso Aceitável dos Recursos

- Os recursos tecnológicos da organização são de uso corporativo e devem ser utilizados com responsabilidade e ética;
- É vedado o uso de sistemas corporativos para atividades ilícitas, para finalidades pessoais em caráter excessivo ou que representem risco à imagem da empresa;
- O tráfego de rede pode ser monitorado para fins de conformidade e segurança, nos limites da legislação aplicável.

5.11. Treinamento e Conscientização

- Os colaboradores participam de treinamentos periódicos sobre boas práticas de segurança, engenharia social, phishing e proteção de dados.
- A conscientização é reforçada por campanhas internas, comunicações e simulações de incidentes.

5.12. Conformidade, Auditoria e Penalidades

- O cumprimento desta política é verificado por auditorias internas e externas regulares;
- Violações praticadas por colaboradores podem resultar em medidas disciplinares, conforme a gravidade e a legislação aplicável;
- A não conformidade contratual por parte de terceiros pode resultar na aplicação das penalidades previstas em contrato, inclusive a rescisão.

6. COMUNICAÇÃO E DIVULGAÇÃO

Esta política é divulgada a colaboradores, terceiros, fornecedores e partes externas relevantes, sendo publicada nos canais corporativos internos e no site da Trucks Control.

O canal oficial para dúvidas e comunicação de incidentes de segurança da informação é o endereço csi@tcsat.com.br. As solicitações relativas a dados pessoais e ao exercício de direitos dos titulares devem ser encaminhadas ao endereço lgpd@tcsat.com.br.

Alterações significativas são formalmente comunicadas e submetidas à aprovação do Comitê de Segurança da Informação e da Diretoria.

7. CONTROLE DE ALTERAÇÕES

Data	Versão	Alteração	Elaboração	Aprovação
04/11/2025	1	Emissão da Política de Segurança da Informação (uso interno).	Marco Antônio, Gerência de Infraestrutura	Augusto Carvalho, Diretor de Tecnologia
04/09/2026	1.0 P	Emissão da versão pública, derivada da política interna, com inclusão dos objetivos de segurança da informação aprovados pela Diretoria e atualização dos canais oficiais de contato.	Segurança da Informação	Diretoria de Tecnologia