POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

04/11/2025

1. INTRODUÇÃO

A Trucks Control reconhece a segurança da informação como um pilar estratégico para garantir a continuidade e a confiabilidade de suas operações. A proteção de informações e ativos críticos é essencial para a manutenção da confiança de clientes, parceiros e colaboradores, bem como para o cumprimento de obrigações legais e contratuais.

Esta Política de Segurança da Informação (PSI) estabelece diretrizes para proteger a **confidencialidade, integridade e disponibilidade** das informações, alinhando-se aos requisitos da **ISO/IEC 27001:2022**, boas práticas da **ISO/IEC 27002:2022** e normas correlatas (ISO 27035, 27701 e 22301).

2. OBJETIVO

Assegurar que todas as informações tratadas pela **Trucks Control** — próprias ou de terceiros — sejam protegidas contra acesso, uso, divulgação, modificação ou destruição não autorizada.

3. ABRANGÊNCIA

Aplica-se a todos os colaboradores, prestadores de serviço, parceiros, fornecedores, consultores e terceiros que tenham acesso, direto ou indireto, às informações ou sistemas sob responsabilidade da Trucks Control.
Abrange 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 deve aprovar, apoiar e prover recursos para a implementação desta política.
- O Comitê de Segurança da Informação (CSI) é responsável por supervisionar o SGSI, aprovar planos de ação e acompanhar indicadores.
- A área de Segurança da Informação deve implementar controles, gerir incidentes, realizar auditorias e garantir conformidade com esta política.
- Todos os colaboradores e terceiros devem cumprir as diretrizes desta política, participar dos treinamentos 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 devem ser revisados periodicamente ou quando houver mudanças significativas no ambiente de negócio ou tecnológico.

5.3. Classificação e Tratamento da Informação

As informações devem ser classificadas conforme 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 deve possuir regras específicas para armazenamento, compartilhamento, transmissão e descarte seguro.

5.4. Controle de Acesso

- O acesso a sistemas e informações deve seguir o princípio do menor privilégio e ser revisado periodicamente.
- Contas de usuários devem ser únicas, autenticadas e rastreáveis.
- O uso de autenticação multifator (MFA) é obrigatório para acessos administrativos e remotos.

5.5. Segurança em Recursos Tecnológicos

- Todos os dispositivos (notebooks, servidores, smartphones, etc.) devem possuir antivírus atualizado, criptografia de disco e controle de atualizações.
- A rede corporativa deve ser segmentada e monitorada, com uso de firewall, VPN segura e logs de auditoria.
- O uso de mídias removíveis deve ser controlado e monitorado.
- Backups devem ser realizados regularmente e testados periodicamente quanto à restauração.

5.6. Proteção de Dados e Privacidade

- O tratamento de dados pessoais deve seguir os princípios da Lei Geral de Proteção de Dados (LGPD).
- Dados sensíveis devem ser protegidos com criptografia, controle de acesso e registro de auditoria.
- A coleta e o uso de dados pessoais devem ter finalidade legítima, consentimento e registro documental.

5.7. Segurança em Fornecedores e Terceiros

- Fornecedores que processam, armazenam ou acessam informações da Trucks Control devem ser avaliados regularmente quanto à conformidade em segurança e privacidade seguindo as diretrizes desta política.
- Cláusulas contratuais específicas devem garantir confidencialidade, notificação de incidentes e responsabilidade por violações.

5.8. Gestão de Incidentes de Segurança

- Todos os incidentes devem ser reportados imediatamente ao canal oficial de segurança: csi@truckscontrol.com.br
- A área responsável deve seguir o Plano de Resposta a Incidentes (PRI) conforme a ISO/IEC 27035, contendo fases de identificação, contenção, erradicação e lições aprendidas.
- Devem ser mantidos registros de incidentes e ações corretivas.

5.9. Continuidade de Negócios e Recuperação de Desastres

A Trucks Control implementou o Sistema de Gestão de Continuidade de Negócios (SGCN), de forma integrada ao Sistema de Gestão de Segurança da Informação (SGSI), assegurando uma abordagem unificada de resiliência organizacional.

O Plano de Continuidade de Negócios (PCN), 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.

Essas práticas visam garantir a continuidade dos serviços essenciais, mesmo diante de falhas graves, ataques cibernéticos, indisponibilidade de infraestrutura ou desastres naturais.

5.10. Uso Aceitável dos Recursos

- Os recursos tecnológicos da organização são de uso corporativo e devem ser utilizados com responsabilidade e ética.
- É proibido o uso de sistemas corporativos para atividades ilícitas, pessoais excessivos ou que representem riscos à imagem da empresa.

- O tráfego de rede pode ser monitorado para garantir conformidade e segurança.

5.11. Treinamento e Conscientização

- Todos os colaboradores devem participar de treinamentos periódicos sobre boas práticas de segurança, engenharia social, phishing e proteção de dados.
- A conscientização será reforçada por campanhas internas, comunicações e simulações de incidentes.

5.12. Conformidade, Auditoria e Penalidades

- O cumprimento desta política será verificado por auditorias internas e externas regulares.
- Violações podem resultar em medidas disciplinares, incluindo advertência, suspensão ou desligamento, conforme a gravidade.
- A não conformidade contratual poderá resultar em penalidades e rescisão de contratos.

6. COMUNICAÇÃO E DIVULGAÇÃO

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

O canal oficial para dúvidas e denúncias de incidentes é o e-mail csi@truckscontrol.com.br

Mudanças significativas serão comunicadas formalmente e aprovadas pelo Comitê de Segurança da Informação.

7. CONTROLE DE ALTERAÇÕES

Data	Versão	Alteração/Revisão	Cargo	Aprovação	Cargo
04/11/2025	V1	Marco Antônio	Gestor de TI	Augusto Carvalho	Diretor de TI